INDUSFACE™ WAS

Vulnerability Assessment Report

Indusface

34.233.47.30

http://demo2.indussecure.com/

Confidential

Scan Date: 2023-10-06

INDUSFACE™

Scope

Vulnerability Assessment for IP Address 34.233.47.30.

Limitations

1. The entire test was carried out with no prior knowledge of the systems and applications.
2. All test were carried out without any known credentials to systems and applications.
3. Indusface WAS does not carry out any DoS attacks or to run any exploits which can affect systems availability.

Confidentiality

This document contains sensitive and/or confidential information, do not distribute, email, fax or transfer via any electronic mechanism without proper authorization. Information contained with in this document should be handled with appropriate caution. While reasonable attempts have been made to confirm the accuracy of the data contained herein, Indusface WAS, assumes no liability for the completeness, use of, or conclusions drawn from such data.

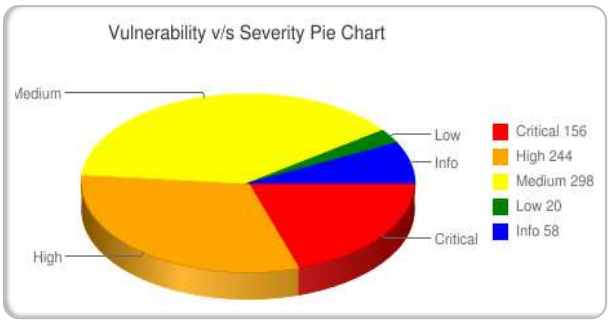
Disclaimer

This, or any other, Security Audit cannot and does not guarantee security. Indusface WAS makes no warranty or claim of any kind, whatsoever, about the accuracy or usefulness of any information provided herein. By using this information you agree that Indusface WAS shall be held harmless in any event. Indusface WAS makes this information available solely under its Terms of Service Agreement published at was.indusface.com.

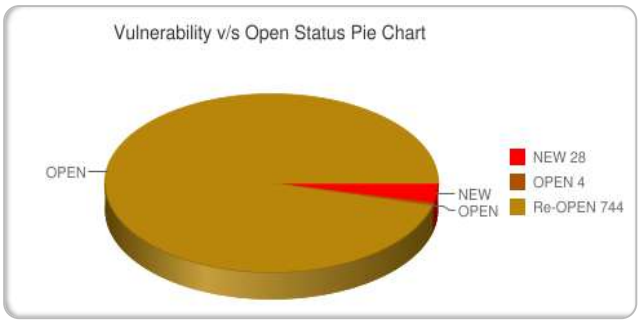
Executive Summary

Total number of vulnerabilities identified for 34.233.47.30 is 776

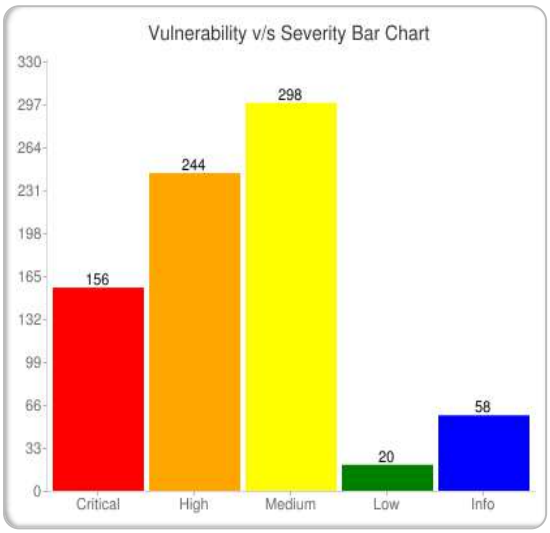
Vulnerability v/s Severity Pie Chart



Vulnerability v/s Open Status Pie Chart



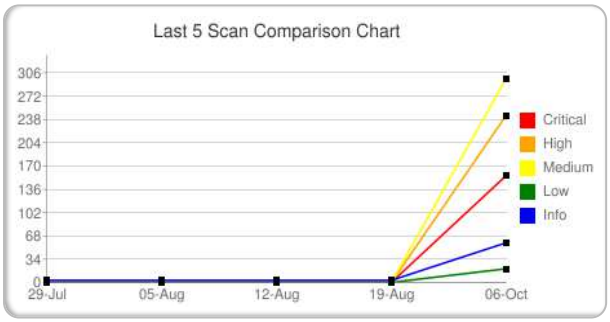
Vulnerability v/s Severity Bar Chart



Vulnerability Summary

Severity	Total
Critical	156
High	244
Medium	298
Low	20
Info	58

Comparison Chart



Comparison Summary

Severity	29 Jul	05 Aug	12 Aug	19 Aug	06 Oct
Critical	0	0	0	0	156
High	0	0	0	0	244
Medium	0	0	0	0	298
Low	0	0	0	0	20
Info	3	3	3	3	58

Vulnerability Details

Title	Total
Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities (Linux)	4
Apache HTTP Server 2.4.0 - 2.4.46 Multiple Vulnerabilities - Linux	4
Apache HTTP Server 2.4.0 - 2.4.55 HTTP Request Smuggling Vulnerability (Linux)	4
Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Linux	4
Apache HTTP Server < 2.4.54 Multiple Vulnerabilities - Linux	4
Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Linux	4
Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Linux	4
Apache HTTP Server Multiple Vulnerabilities June17 (Linux)	4
OpenBSD OpenSSH < 9.3p2 RCE Vulnerability	2
OpenSSH X11 Forwarding Security Bypass Vulnerability (Linux)	2
OpenSSL End of Life (EOL) Detection (Linux)	4
OpenSSL: c_rehash script allows command injection (CVE-2022-1292) - Linux	4
OpenSSL: The c_rehash script allows command injection (CVE-2022-2068) - Linux	4
PHP 'CVE-2019-11043' FPM Remote Code Execution Vulnerability (Version Check)	4
PHP 'CVE-2019-13224' Use-After-Free Vulnerability (Linux)	4
PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16 (Linux)	4
PHP 'type confusion' Denial of Service Vulnerability (Linux)	4
PHP 'var_unserializer' Denial of Service Vulnerability (Linux)	4
PHP < 5.6.29, 7.0.x < 7.0.14 DoS Vulnerability - Linux	4
PHP < 7.0.12 RCE / DoS Vulnerability - Linux	4
PHP < 7.2.27, 7.3.x < 7.3.14, 7.4.x < 7.4.2 Multiple Vulnerabilities - Jan20 (Linux)	4
PHP < 7.4.28, 8.0.x < 8.0.16, 8.1.x < 8.1.3 Security Update (Feb 2022) - Linux	4
PHP < 7.4.33, 8.0.x < 8.0.25, 8.1.x < 8.1.12 Security Update - Linux	4
PHP < 8.0.30, 8.1.x < 8.1.22, 8.2.x < 8.2.9 Security Update - Linux	4

PHP <= 5.6.27 / 7.0.x <= 7.0.12 DoS Vulnerability	4
PHP <= 7.1.5 Multiple DoS Vulnerabilities	4
PHP Arbitrary Code Execution Vulnerability - Aug16 (Linux)	4
PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Linux)	4
PHP Denial of Service Vulnerability - 02 - Aug16 (Linux)	4
PHP End Of Life Detection (Linux)	4
PHP Multiple DoS Vulnerabilities (Oct 2016) - Linux	4
PHP Multiple Vulnerabilities (Jul 2017 - 01) - Linux	4
PHP Multiple Vulnerabilities (Jun/Aug 2014) - Linux	4
PHP Multiple Vulnerabilities - 01 - Apr16 (Linux)	4
PHP Multiple Vulnerabilities - 02 - Aug16 (Linux)	4
PHP Multiple Vulnerabilities - 03 - Jul16 (Linux)	4
PHP Multiple Vulnerabilities - 04 - Jul16 (Linux)	4
PHP Out of Bounds Read Memory Corruption Vulnerability - 01 - Mar16 (Linux)	4
PHP Stack Buffer Overflow Vulnerability Mar18 (Linux)	4
PHP XML Entity Expansion And XML External Entity Vulnerabilities (Linux)	4
Apache HTTP Server 'mod_auth_digest' DoS Vulnerability (Linux)	4
Apache HTTP Server 'Whitespace Defects' Multiple Vulnerabilities	4
Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Linux)	4
Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerability (Linux)	4
Apache HTTP Server < 2.4.48 NULL Pointer Dereference Vulnerability - Linux	4
Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Linux)	4
Apache HTTP Server Man-in-the-Middle Attack Vulnerability - July16 (Linux)	4
Apache HTTP Server mod_session_crypto Vulnerability (Dec 2016) - Linux	4
Apache HTTP Server OPTIONS Memory Leak Vulnerability (Optionsbleed) - Version Check	4
Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater)	2

Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)	2
OpenBSD OpenSSH <= 8.6 Command Injection Vulnerability	2
OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability	2
OpenSSH Client Information Leak	2
OpenSSH Multiple Vulnerabilities	2
OpenSSH Multiple Vulnerabilities Jan17 (Linux)	2
OpenSSH Privilege Escalation Vulnerability - May16	2
OpenSSL 1.0.2 < 1.0.2zg, 1.1.1 < 1.1.1t, 3.0 < 3.0.8 Multiple Vulnerabilities - Linux	4
OpenSSL: Infinite loop in BN_mod_sqrt() reachable when parsing certificates (CVE-2022-0778) - Linux	4
OpenSSL: Integer overflow in CipherUpdate (CVE-2021-23840) - Linux	4
OpenSSL: Read Buffer Overruns Processing ASN.1 Strings (20210824) - Linux	4
PHP 'CVE-2017-7189' Improper Input Validation Vulnerability (Linux)	4
PHP 'CVE-2018-19935' - 'imap_mail' Denial of Service Vulnerability (Linux)	4
PHP 'FastCGI Process Manager' Privilege Escalation Vulnerability	4
PHP 'make_http_soap_request' DoS / Information Disclosure Vulnerability - Linux	4
PHP 'serialize_function_call' Function Type Confusion Vulnerability - Mar16 (Linux)	4
PHP 'stream_get_meta_data' Privilege Escalation Vulnerability (Linux)	4
PHP 'timelib_meridian' Heap Based Buffer Overflow Vulnerability (Linux)	4
PHP 'WDDX Deserialization' Denial of Service Vulnerability - (Linux)	4
PHP 5.3.7 - 7.3.31, 7.4.x < 7.4.25, 8.0.x < 8.0.12 Security Update (Oct 2021) - Linux	4
PHP < 7.2.30, 7.3 < 7.3.17, 7.4 < 7.4.5 DoS Vulnerability - Apr20 (Linux)	4
PHP < 7.3.27, 7.4.x < 7.4.15, 8.0.x < 8.0.2 NULL Deference Vulnerability (Feb 2021) - Linux	4
PHP < 7.4.30, 8.0.x < 8.0.20, 8.1.x < 8.1.7 Security Update (Jun 2022) - Linux	4
PHP < 8.0.22, 8.1.x < 8.1.9 Security Update - Linux	4
PHP < 8.0.27, 8.1.x < 8.1.14, 8.2.x < 8.2.1 Security Update - Linux	4
PHP < 8.0.28, 8.1.x < 8.1.16, 8.2.x < 8.2.3 Security Update - Linux	4

PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Linux)	4
PHP Denial of Service Vulnerability Jul17 (Linux)	4
PHP Directory Traversal Vulnerability - Jul16 (Linux)	4
PHP Fileinfo Component Denial of Service Vulnerability (Linux)	4
PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Linux)	4
PHP Multiple Denial of Service Vulnerabilities (Linux)	4
PHP Multiple Double Free Vulnerabilities - Jan15	4
PHP Multiple Heap Buffer Overflow and Information Disclosure Vulnerabilities (Linux)	4
PHP Multiple Remote Code Execution Vulnerabilities - Jul15 (Linux)	4
PHP Multiple Vulnerabilities (Feb 2019) - Linux	4
PHP Multiple Vulnerabilities (Jan 2017 - 02) - Linux	4
PHP Multiple Vulnerabilities (Jul 2016 - 05) - Linux	4
PHP Multiple Vulnerabilities (Nov 2016) - Linux	4
PHP Multiple Vulnerabilities - 01 - Aug16 (Linux)	4
PHP Multiple Vulnerabilities - 01 - Feb15	4
PHP Multiple Vulnerabilities - 01 - Jan15	4
PHP Multiple Vulnerabilities - 01 - Jul16 (Linux)	4
PHP Multiple Vulnerabilities - 01 - Jun15 (Linux)	4
PHP Multiple Vulnerabilities - 01 - Mar16 (Linux)	4
PHP Multiple Vulnerabilities - 02 - Jan15	4
PHP Multiple Vulnerabilities - 02 - Jun15 (Linux)	4
PHP Multiple Vulnerabilities - 02 - Sep16 (Linux)	4
PHP Multiple Vulnerabilities - 03 - Aug16 (Linux)	4
PHP Multiple Vulnerabilities - 03 - Sep16 (Linux)	4
PHP Multiple Vulnerabilities - 04 - Aug16 (Linux)	4
PHP Multiple Vulnerabilities - Dec18 (Linux)	4
PHP Out of Bounds Read Multiple Vulnerabilities - Jan15	4

PHP Remote Code Execution and Denial of Service Vulnerabilities - Dec13	4
PHP Use-After-Free Remote Code EXecution Vulnerability - Jan15	4
Apache HTTP Server 'mod_cache' Denial of Service Vulnerability -01 May15	4
Apache HTTP Server 'mod_cache' Denial of Service Vulnerability May15	4
Apache HTTP Server 'mod_lua' Denial of Service Vulnerability -01 May15	4
Apache HTTP Server 'mod_lua' Denial of Service Vulnerability May15	4
Apache HTTP Server 2.4.0 - 2.4.40 Multiple Vulnerabilities (Linux)	4
Apache HTTP Server 2.4.0 < 2.4.42 Multiple Vulnerabilities (Linux)	4
Apache HTTP Server 2.4.1 < 2.4.24 IP Spoofing Vulnerability (Linux)	4
Apache HTTP Server 2.4.6 - 2.4.46 Tunneling Misconfiguration Vulnerability - Linux	4
Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Linux)	4
Apache HTTP Server < 2.4.55 Multiple Vulnerabilities (Linux)	4
Apache HTTP Server CRLF Injection Vulnerability (Dec 2016) - Linux	4
Apache HTTP Server DoS Vulnerability (Sep 2014) - Linux	4
Apache HTTP Server Multiple Vulnerabilities (Mar 2014) - Linux	4
Apache HTTP Server Multiple Vulnerabilities (Sep 2014) - Linux	4
Apache HTTP Server Multiple Vulnerabilities Apr18 (Linux)	4
Apache HTTP Server Multiple Vulnerabilities August15 (Linux)	4
Apache HTTP Server Multiple Vulnerabilities May15	4
Missing 'HttpOnly' Cookie Attribute (HTTP)	2
OpenBSD OpenSSH < 9.1 Multiple Vulnerabilities	2
OpenBSD OpenSSH < 9.2 Unspecified Vulnerability	2
OpenBSD OpenSSH < 9.3 Unspecified Vulnerability	2
OpenBSD OpenSSH <= 7.9 Multiple Vulnerabilities	2
OpenBSD OpenSSH Information Disclosure Vulnerability (CVE-2020-14145)	2
OpenSSH 'auth2-gss.c' User Enumeration Vulnerability - Linux	2

OpenSSH 'sftp-server' Security Bypass Vulnerability (Linux)	2
OpenSSH < 7.8 User Enumeration Vulnerability - Linux	2
OpenSSH <= 7.2p1 - Xauth Injection	2
OpenSSH Denial of Service And User Enumeration Vulnerabilities (Linux)	2
OpenSSH Denial of Service Vulnerability - Jan16	2
OpenSSH Information Disclosure Vulnerability (CVE-2016-20012)	2
OpenSSH Security Bypass Vulnerability	2
OpenSSL 'OOB read' Security Bypass Vulnerability (Linux)	4
OpenSSL DoS Vulnerability (20180327) - Linux	4
OpenSSL DoS Vulnerability (20230719) - Linux	4
OpenSSL DoS Vulnerability (20230731) - Linux	4
OpenSSL Information Disclosure Vulnerability (20191206) - Linux	4
OpenSSL Multiple Vulnerabilities (20230322, 20230328, 20230530) - Linux	4
OpenSSL Multiple Vulnerabilities - Nov 2017 (Linux)	4
OpenSSL Overflow Vulnerability (20171207, 20180327) - Linux	4
OpenSSL Security Bypass Vulnerability - DEC 2017 (Linux)	4
OpenSSL: 0-byte record padding oracle (CVE-2019-1559) (Linux)	4
OpenSSL: 1.0.2 < 1.0.2p / 1.1.0 < 1.1.0i Multiple Vulnerabilities (Linux)	4
OpenSSL: BN_mod_exp may produce incorrect results on MIPS (CVE-2021-4160) - Linux	4
OpenSSL: EDIPARTYNAME NULL Pointer De-reference Vulnerability (CVE-2020-1971) (Linux)	4
OpenSSL: Microarchitecture timing vulnerability in ECC scalar multiplication (CVE-2018-5407) (Linux)	4
OpenSSL: Null pointer deref in X509_issuer_and_serial_hash() (CVE-2021-23841) - Linux	4
OpenSSL: Timing vulnerability in DSA signature generation (CVE-2018-0734) (Linux)	4
PHP 'donate' function Denial of Service Vulnerability - Nov14	4
PHP 'LibGD' Denial of Service Vulnerability	4

PHP 'open_basedir' Security Bypass Vulnerability	4
PHP 'PHAR' Error Page Reflected XSS And DoS Vulnerabilities (Linux)	4
PHP 'PHP-FPM' Denial of Service Vulnerability (Linux)	4
PHP 'php_parserr' Heap Based Buffer Overflow Vulnerability (Linux)	4
PHP < 7.2.26 Multiple Vulnerabilities - Dec19 (Linux)	4
PHP < 7.2.28 Multiple Vulnerabilities - Feb20 (Linux)	4
PHP < 7.2.29 Multiple Vulnerabilities - Mar20 (Linux)	4
PHP < 7.2.31, 7.3 < 7.3.18, 7.4 < 7.4.6 Multiple DoS Vulnerabilities - May20 (Linux)	4
PHP < 7.2.34, 7.3 < 7.3.23, 7.4 < 7.4.11 Multiple Vulnerabilities - October20 (Linux)	4
PHP < 7.3.26, 7.4.x < 7.4.14, 8.0.x < 8.0.1 Filter Vulnerability (Jan 2021) - Linux	4
PHP < 7.3.28, 7.4.x < 7.4.18 IMAP Header Injection Vulnerability (Apr 2021) - Linux	4
PHP < 7.3.29 Multiple Vulnerabilities (Jul 2021) - Linux	4
PHP < 7.3.30, 7.4.x < 7.4.23, 8.0.x < 8.0.10 Security Update (Aug 2021) - Linux	4
PHP < 7.3.31, 7.4.x < 7.4.24, 8.0.x < 8.0.11 Security Update (Sep 2021) - Linux	4
PHP < 7.3.33, 7.4.x < 7.4.26, 8.0.x < 8.0.13 Security Update (Nov 2021) - Linux	4
PHP < 7.4.31, 8.0.x < 8.0.24, 8.1.x < 8.1.11 Security Update - Linux	4
PHP < 8.0.29, 8.1.x < 8.1.20, 8.2.x < 8.2.7 Security Update - Linux	4
PHP CDF File Parsing Denial of Service Vulnerabilities - 01 - Jun14	4
PHP Cross-Site Scripting Vulnerability - Aug16 (Linux)	4
PHP Denial of Service Vulnerability - 01 - Jul16 (Linux)	4
PHP Heap Use-After-Free Vulnerability - Sep19 (Linux)	4
PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Linux)	4
PHP Multiple Vulnerabilities - 01 - Aug14	4
PHP Multiple Vulnerabilities - 03 - Jun15 (Linux)	4
PHP Multiple Vulnerabilities - 04 - Jun15 (Linux)	4
PHP Multiple Vulnerabilities - 05 - Aug16 (Linux)	4
PHP Multiple Vulnerabilities - Sep19 (Linux)	4

PHP Multiple Vulnerabilities May18 (Linux)	4
PHP Security Bypass Vulnerability May18 (Linux)	4
PHP Sessions Subsystem Session Fixation Vulnerability (Aug 2013)	4
SSL/TLS: Certificate Expired	2
SSL/TLS: Certificate In Chain Expired	2
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	2
Weak Encryption Algorithm(s) Supported (SSH)	2
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	2
OpenSSL 1.0.2, 1.1.0, 1.1.1 Multiple Vulnerabilities - Linux	4
OpenSSL: Raccoon Attack (CVE-2020-1968) (Linux)	4
PHP < 7.2.33, 7.3 < 7.3.21, 7.4 < 7.4.9 DoS Vulnerability - August20 (Linux)	4
PHP <= 5.6.0 'PEAR' Symlink Attack Vulnerability	4
TCP Timestamps Information Disclosure	2
Weak MAC Algorithm(s) Supported (SSH)	2
Apache HTTP Server Detection Consolidation	2
CGI Scanning Consolidation	4
HTTP Security Headers Detection	4
HTTP Server type and version	4
MariaDB / Oracle MySQL Detection (MySQL Protocol)	2
OpenSSH Detection Consolidation	2
OpenSSL Detection Consolidation	2
OS Detection Consolidation and Reporting	2
PHP Detection (HTTP)	4
Services	8
SSH Protocol Algorithms Supported	2
SSH Protocol Versions Supported	2
SSH Server type and version	2
SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN	2
SSL/TLS: Collect and Report Certificate Details	2
SSL/TLS: Report Medium Cipher Suites	2
SSL/TLS: Report Non Weak Cipher Suites	2
SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites	2
SSL/TLS: Report Supported Cipher Suites	2
SSL/TLS: Safe/Secure Renegotiation Support Status	2
SSL/TLS: Version Detection	2

Traceroute	2

Vulnerabilities

Unique Alert ID: 607306 Found on: 2023-10-06 Severity: Critical

OpenSSL End of Life (EOL) Detection (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-12-18
Cvss Base: 10.0
Cvss Score: 10.0

Description:

The OpenSSL version on the remote host has reached the end of life and should not be used anymore. An EOL version of OpenSSL is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:

VendorFix Update the OpenSSL version on the remote host to a still supported version.

Result:

The "OpenSSL" version on the remote host has reached the end of life. CPE: cpe:/a:openssl:openssl:1.0.2k Installed version: 1.0.2k Location/URL: 443/tcp EOL version: 1.0.2 EOL date: 2019-12-31

Unique Alert ID: 539065 Found on: 2023-10-06 Severity: Critical

OpenSSL End of Life (EOL) Detection (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 10.0
Cvss Score: 10.0

Description:

The OpenSSL version on the remote host has reached the end of life and should not be used anymore. An EOL version of OpenSSL is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:

VendorFix Update the OpenSSL version on the remote host to a still supported version.

Result:

The "OpenSSL" version on the remote host has reached the end of life. CPE: cpe:/a:openssl:openssl:1.0.2k Installed version: 1.0.2k Location/URL: 80/tcp EOL version: 1.0.2 EOL date: 2019-12-31

Unique Alert ID: 539060 Found on: 2023-10-06 Severity: Critical

PHP End Of Life Detection (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 10.0
Cvss Score: 10.0

Description:

The PHP version on the remote host has reached the end of life and should not be used anymore. Each release branch of PHP is fully supported for two years from its initial stable release. During this period, bugs and security issues that have b

een reported are fixed and are released in regular point releases. After this two year period of active support, each bran ch is then supported for an additional year for critical security issues only. Releases during this period are made on an as -needed basis: there may be multiple point releases, or none, depending on the number of reports. Once the three years of support are completed, the branch reaches its end of life and is no longer supported. An end of life version of PHP is n ot receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to c ompromise the security of this host.

Solution:

VendorFix Update the PHP version on the remote host to a still supported version.

Result:

The "PHP" version on the remote host has reached the end of life. CPE: cpe:/a:php:php:5.4.16 Installed version: 5.4.16 EOL version: 5.4 EOL date: 2015-09-03

References:

- https://secure.php.net/supported-versions.php,https://secure.php.net/eol.php

Unique Alert ID: 539069 Found on: 2023-10-06 Severity: Critical

PHP End Of Life Detection (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 10.0
Cvss Score: 10.0

Description:

The PHP version on the remote host has reached the end of life and should not be used anymore. Each release branch of PHP is fully supported for two years from its initial stable release. During this period, bugs and security issues that have b een reported are fixed and are released in regular point releases. After this two year period of active support, each bran ch is then supported for an additional year for critical security issues only. Releases during this period are made on an as -needed basis: there may be multiple point releases, or none, depending on the number of reports. Once the three years of support are completed, the branch reaches its end of life and is no longer supported. An end of life version of PHP is n ot receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to c ompromise the security of this host.

Solution:

VendorFix Update the PHP version on the remote host to a still supported version.

Result:

The "PHP" version on the remote host has reached the end of life. CPE: cpe:/a:php:php:5.4.16 Installed version: 5.4.16 EOL version: 5.4 EOL date: 2015-09-03

References:

- https://secure.php.net/supported-versions.php,https://secure.php.net/eol.php

Unique Alert ID: 919527 Found on: 2023-10-06 Severity: Critical

PHP <= 7.1.5 Multiple DoS Vulnerabilities (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2017-8923,CVE-2017-9119
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to multiple denial of service (DoS) vulnerabilities. The following flaws exist: - CVE-2017-8923: The zend_stri ng_extend function in Zend/zend_string.h does not prevent changes to string objects that result in a negative length, whi ch allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by l everaging a script's use of .

Solution:

WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Result:

Installed version: 5.4.16 Fixed version: None Installation path / port: 443/tcp

References:

- https://bugs.php.net/bug.php?id=73122,https://bugs.php.net/bug.php?id=74310,https://bugs.php.net/bug.php?id=74577,https://bugs.php.net/bug.php?id=74593

Unique Alert ID: 919535 Found on: 2023-10-06 Severity: Critical

PHP < 5.6.29, 7.0.x < 7.0.14 DoS Vulnerability - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2016-9935	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to a denial of service (DoS) vulnerability. The php_wddx_push_element function in ext/wddx/wddx.c allows remote attackers to cause a denial of service (out-of-bounds read and memory corruption) or possibly have unspecified other impact via an empty boolean element in a wddxPacket XML document.

Solution:

VendorFix Update to version 5.6.29, 7.0.14 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.29 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.0.14,https://www.php.net/ChangeLog-5.php#5.6.29,https://bugs.php.net/bug.php?id=73631

Unique Alert ID: 539098 Found on: 2023-10-06 Severity: Critical

PHP 'CVE-2019-11043' FPM Remote Code Execution Vulnerability (Version Check) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2019-11043	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to a remote code execution vulnerability in certain nginx + php-fpm configurations. The file sapi/fpm/fpm/fpm_main.c contains pointer arithmetic that assumes that env_path_info has a prefix equal to the path to the php script. However, the code does not check this assumption is satisfied. The absence of the check can lead to an invalid pointer in the 'path_info' variable. Such conditions can be achieved in a pretty standard Nginx configuration. The regexp in `fastcgi_split_path_info` directive can be broken using the newline character (in encoded form, %0a). Broken regexp leads to empty PATH_INFO, which triggers the bug. Successful exploitation would allow an unauthenticated remote attacker to execute arbitrary code on the target machine.

Solution:

VendorFix Update to version 7.1.33, 7.2.24, 7.3.11 or later. As an alternative a workaround to update the nginx configuration to mitigate this vulnerability is described at the PHP.net bugtracker linked in the references.

Result:

Installed version: 5.4.16 Fixed version: 7.1.33 Installation path / port: 80/tcp

References:

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog,https://bugs.php.net/bug.php?id=78599,https://www.php.net/ChangeLog-7.php#7.3.11,https://www.php.net/ChangeLog-7.php#7.2.24,https://www.php.net/ChangeLog-7.php#7.1.33,https://github.com/neex/phuip-fpizdam

Unique Alert ID: 919536 Found on: 2023-10-06 Severity: Critical

PHP <= 5.6.27 / 7.0.x <= 7.0.12 DoS Vulnerability (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2016-9138
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. PHP mishandles property modification during __wakeup processing, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data, as demonstrated by Exception::__toString with DateInterval::__wakeup.

Solution:

WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Result:

Installed version: 5.4.16 Fixed version: None Installation path / port: 80/tcp

References:

- https://bugs.php.net/bug.php?id=73147

Unique Alert ID: 919526 Found on: 2023-10-06 Severity: Critical

PHP <= 7.1.5 Multiple DoS Vulnerabilities (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2017-8923,CVE-2017-9119
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to multiple denial of service (DoS) vulnerabilities. The following flaws exist: - CVE-2017-8923: The zend_string_extend function in Zend/zend_string.h does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .

Solution:

WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Result:

Installed version: 5.4.16 Fixed version: None Installation path / port: 80/tcp

References:

- https://bugs.php.net/bug.php?id=73122,https://bugs.php.net/bug.php?id=74310,https://bugs.php.net/bug.php?id=7

4577,https://bugs.php.net/bug.php?id=74593

Unique Alert ID: 919525 Found on: 2023-10-06 Severity: Critical

PHP <= 5.6.27 / 7.0.x <= 7.0.12 DoS Vulnerability (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2016-9138
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. PHP mishandles property modification during __wakeup processin g, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted seriali zed data, as demonstrated by Exception::__toString with DateInterval::__wakeup.

Solution:

WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Result:

Installed version: 5.4.16 Fixed version: None Installation path / port: 443/tcp

References:

- https://bugs.php.net/bug.php?id=73147

Unique Alert ID: 539105 Found on: 2023-10-06 Severity: Critical

PHP Stack Buffer Overflow Vulnerability Mar18 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-7584
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to a stack buffer overflow vulnerability. The flaw exists because php fails to adequately bounds-check user-supplied data before copying it into an insufficiently sized buffer. Successful exploitation will allow an attacker to execute arbitrary code in the context of the affected application. Failed exploit attempts will result in denial-of-service conditions.

Solution:

VendorFix Update to version 7.2.3, 7.0.28, 5.6.34, 7.1.15 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.34 Installation path / port: 80/tcp

References:

- http://php.net/ChangeLog-7.php,https://bugs.php.net/bug.php?id=75981

Unique Alert ID: 919530 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2021-34798,CVE-2021-39275,CVE-2021-40438	
Cvss Base:	9.0	
Cvss Score:	9.0	
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H	

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2021-34798: NULL pointer dereference in httpd core - CVE-2021-39275: ap_escape_quotes buffer overflow - CVE-2021-40438: mod_proxy SSRF

Solution:

VendorFix Update to version 2.4.49 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.49 Installation path / port: 80/tcp

References:

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog,https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 919531 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2021-34798,CVE-2021-39275,CVE-2021-40438	
Cvss Base:	9.0	
Cvss Score:	9.0	
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H	

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2021-34798: NULL pointer dereference in httpd core - CVE-2021-39275: ap_escape_quotes buffer overflow - CVE-2021-40438: mod_proxy SSRF

Solution:

VendorFix Update to version 2.4.49 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.49 Installation path / port: 443/tcp

References:

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog,https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 1010819 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server < 2.4.54 Multiple Vulnerabilities - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2022-08-27
CVE ID:	CVE-2022-26377,CVE-2022-28614,CVE-2022-28615,CVE-2022-29404,CVE-2022-30556,CVE-2022-31813	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2022-26377: mod_proxy_ajp: Possible request smuggling - CVE-2022-28614: Read beyond bounds via ap_rwrite() - CVE-2022-28615: Read beyond bounds in ap_strcmp_match() - CVE-2022-29404: Denial of service in mod_lua r:parsebody - CVE-2022-30556: Information disclosure in mod_lua with websockets - CVE-2022-31813: mod_proxy X-Forwarded-For dropped by hop-by-hop mechanism

Solution:

VendorFix Update to version 2.4.54 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.54 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html#2.4.54

Unique Alert ID: 1010818 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server < 2.4.54 Multiple Vulnerabilities - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2022-08-27
CVE ID:	CVE-2022-26377,CVE-2022-28614,CVE-2022-28615,CVE-2022-29404,CVE-2022-30556,CVE-2022-31813	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2022-26377: mod_proxy_ajp: Possible request smuggling - CVE-2022-28614: Read beyond bounds via ap_rwrite() - CVE-2022-28615: Read beyond bounds in ap_strcmp_match() - CVE-2022-29404: Denial of service in mod_lua r:parsebody - CVE-2022-30556: Information disclosure in mod_lua with websockets - CVE-2022-31813: mod_proxy X-Forwarded-For dropped by hop-by-hop mechanism

Solution:

VendorFix Update to version 2.4.54 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.54 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html#2.4.54

Unique Alert ID: 539054 Found on: 2023-10-06 Severity: Critical

PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-4342,CVE-2016-2554
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to denial of service and unspecified vulnerabilities. The flaw is due an improper handling of zero-length uncompressed data in 'ext/phar/phar_object.c' script. Successfully exploiting this issue allow remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.5.32, or 5.6.18, or 7.0.3, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.32

References:

- http://www.php.net/ChangeLog-7.php,http://www.openwall.com/lists/oss-security/2016/04/28/2

Unique Alert ID: 539056 Found on: 2023-10-06 Severity: Critical

PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-4342,CVE-2016-2554
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to denial of service and unspecified vulnerabilities. The flaw is due an improper handling of zero-length uncompressed data in 'ext/phar/phar_object.c' script. Successfully exploiting this issue allow remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.5.32, or 5.6.18, or 7.0.3, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.32

References:

- http://www.php.net/ChangeLog-7.php,http://www.openwall.com/lists/oss-security/2016/04/28/2

Unique Alert ID: 539159 Found on: 2023-10-06 Severity: Critical

PHP Arbitrary Code Execution Vulnerability - Aug16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-4116
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to an arbitrary code execution vulnerability. The flaw is due to Use-after-free vulnerability in the 'spl_ptr_heap_insert' function in 'ext/spl/spl_heap.c'. Successfully exploiting this issue allow remote attackers to execute arbitrary code by triggering a failed SplMinHeap::compare operation.

Solution:

VendorFix Update to PHP version 5.5.27, or 5.6.11, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.27

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539160 Found on: 2023-10-06 Severity: Critical

PHP Arbitrary Code Execution Vulnerability - Aug16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2015-4116	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to an arbitrary code execution vulnerability. The flaw is due to Use-after-free vulnerability in the 'spl_ptr_heap_insert' function in 'ext/spl/spl_heap.c'. Successfully exploiting this issue allow remote attackers to execute arbitrary code by triggering a failed SplMinHeap::compare operation.

Solution:

VendorFix Update to PHP version 5.5.27, or 5.6.11, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.27

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 1010812 Found on: 2023-10-06 Severity: Critical

PHP < 7.4.28, 8.0.x < 8.0.16, 8.1.x < 8.1.3 Security Update (Feb 2022) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2022-08-27
CVE ID:	CVE-2021-21708	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP released new versions which include a security fix. Fix #81708: UAF due to php_filter_float() failing for ints.

Solution:

VendorFix Update to version 7.4.28, 8.0.16, 8.1.3 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.4.28 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.4.28,https://www.php.net/ChangeLog-8.php#8.0.16,https://www.php.net/ChangeLog-8.php#8.1.3,https://bugs.php.net/bug.php?id=81708

Unique Alert ID: 1010814 Found on: 2023-10-06 Severity: Critical

PHP < 7.4.28, 8.0.x < 8.0.16, 8.1.x < 8.1.3 Security Update (Feb 2022) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-08-27
CVE ID:	CVE-2021-21708		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP released new versions which include a security fix. Fix #81708: UAF due to php_filter_float() failing for ints.

Solution:

VendorFix Update to version 7.4.28, 8.0.16, 8.1.3 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.4.28 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.4.28,https://www.php.net/ChangeLog-8.php#8.0.16,https://www.php.net/ChangeLog-8.php#8.1.3,https://bugs.php.net/bug.php?id=81708

Unique Alert ID: 539117 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities - 04 - Jul16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-8867,CVE-2015-8876,CVE-2015-8873,CVE-2015-8835		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws exist due to: - An improper validation of certain Exception objects in 'Zend/zend_exceptions.c' script. - The 'openssl_random_pseudo_bytes' function in 'ext/openssl/openssl.c' incorrectly relies on the deprecated 'RAND_pseudo_bytes' function. Successfully exploiting this issue allow remote attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger unintended method execution to defeat cryptographic protection mechanisms.

Solution:

VendorFix Update to PHP version 5.4.44, or 5.5.28, or 5.6.12, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.44

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 919523 Found on: 2023-10-06 Severity: Critical

PHP < 7.0.12 RCE / DoS Vulnerability - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2016-7480		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to a remote code execution (RCE) or denial of service (DoS) vulnerability. The SplObjectStorage unserialize implementation in ext/spl/spl_observer.c does not verify that a key is an object, which allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized memory access) via crafted serialized data.

Solution:

VendorFix Update to version 7.0.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.0.12 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.0.12,https://bugs.php.net/bug.php?id=73257,http://blog.checkpoint.com/2016/12/27/check-point-discovers-three-zero-day-vulnerabilities-web-programming-language-php-7

Unique Alert ID: 919524 Found on: 2023-10-06 Severity: Critical

PHP < 7.0.12 RCE / DoS Vulnerability - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2016-7480	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to a remote code execution (RCE) or denial of service (DoS) vulnerability. The SplObjectStorage unserialize implementation in ext/spl/spl_observer.c does not verify that a key is an object, which allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized memory access) via crafted serialized data.

Solution:

VendorFix Update to version 7.0.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.0.12 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.0.12,https://bugs.php.net/bug.php?id=73257,http://blog.checkpoint.com/2016/12/27/check-point-discovers-three-zero-day-vulnerabilities-web-programming-language-php-7

Unique Alert ID: 539099 Found on: 2023-10-06 Severity: Critical

PHP 'var_unserializer' Denial of Service Vulnerability (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-7411	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to improper handling of object-deserialization failures in 'ext/standard/var_unserializer.re' script. Successfully exploiting this issue allow remote attackers to cause a denial of service.

Solution:

VendorFix Update to PHP version 5.6.26, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.26

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539104 Found on: 2023-10-06 Severity: Critical

PHP Stack Buffer Overflow Vulnerability Mar18 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2018-7584	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to a stack buffer overflow vulnerability. The flaw exists because php fails to adequately bounds-check user-supplied data before copying it into an insufficiently sized buffer. Successful exploitation will allow an attacker to execute arbitrary code in the context of the affected application. Failed exploit attempts will result in denial-of-service conditions.

Solution:

VendorFix Update to version 7.2.3, 7.0.28, 5.6.34, 7.1.15 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.34 Installation path / port: 443/tcp

References:

- http://php.net/ChangeLog-7.php,https://bugs.php.net/bug.php?id=75981

Unique Alert ID: 539100 Found on: 2023-10-06 Severity: Critical

PHP 'var_unserializer' Denial of Service Vulnerability (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-7411	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to improper handling of object-deserialization failures in 'ext/standard/var_unserializer.re' script. Successfully exploiting this issue allow remote attackers to cause a denial of service.

Solution:

VendorFix Update to PHP version 5.6.26, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.26

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539058 Found on: 2023-10-06 Severity: Critical

PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-5590,CVE-2015-8838,CVE-2015-5589		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to a stack buffer overflow vulnerability. Multiple flaws are due to - Inadequate boundary checks on user-supplied input by 'phar_fix_filepath' function in 'ext/phar/phar.c' script. - Improper validation of file pointer in the 'phar_convert_to_other' function in 'ext/phar/phar_object.c' script. Successfully exploiting this issue allow remote attackers to execute arbitrary code in the context of the PHP process. Failed exploit attempts will likely crash the webserver.

Solution:

VendorFix Update to PHP version 5.4.43, or 5.5.27, or 5.6.11 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.43

References:

- http://www.php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=69923

Unique Alert ID: 919532 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2021-44790		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

Apache HTTP Server is prone to a buffer overflow vulnerability. A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts).

Solution:

VendorFix Update to version 2.4.52 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.52 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 919533 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2021-44790		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

Apache HTTP Server is prone to a buffer overflow vulnerability. A carefully crafted request body can cause a buffer overf low in the mod_lua multipart parser (r:parsebody() called from Lua scripts).

Solution:

VendorFix Update to version 2.4.52 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.52 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 1010817 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-08-27
CVE ID:	CVE-2022-22719,CVE-2022-22720,CVE-2022-22721,CVE-2022-23943		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2022-22719: mod_lua U se of uninitialized value of in r:parsebody - CVE-2022-22720: HTTP request smuggling vulnerability - CVE-2022-22721: P ossible buffer overflow with very large or unlimited LimitXMLRequestBody - CVE-2022-23943: mod_sed: Read/write beyo nd bounds

Solution:

VendorFix Update to version 2.4.53 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.53 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html#2.4.53

Unique Alert ID: 1010816 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2022-08-27
CVE ID:	CVE-2022-22719,CVE-2022-22720,CVE-2022-22721,CVE-2022-23943	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2022-22719: mod_lua Use of uninitialized value of in r:parsebody - CVE-2022-22720: HTTP request smuggling vulnerability - CVE-2022-22721: Possible buffer overflow with very large or unlimited LimitXMLRequestBody - CVE-2022-23943: mod_sed: Read/write beyond bounds

Solution:

VendorFix Update to version 2.4.53 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.53 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html#2.4.53

Unique Alert ID: 539067 Found on: 2023-10-06 Severity: Critical

PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2015-5590,CVE-2015-8838,CVE-2015-5589	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to a stack buffer overflow vulnerability. Multiple flaws are due to - Inadequate boundary checks on user-supplied input by 'phar_fix_filepath' function in 'ext/phar/phar.c' script. - Improper validation of file pointer in the 'phar_convert_to_other' function in 'ext/phar/phar_object.c' script. Successfully exploiting this issue allow remote attackers to execute arbitrary code in the context of the PHP process. Failed exploit attempts will likely crash the webserver.

Solution:

VendorFix Update to PHP version 5.4.43, or 5.5.27, or 5.6.11 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.43

References:

- http://www.php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=69923

Unique Alert ID: 539092 Found on: 2023-10-06 Severity: Critical

PHP 'CVE-2019-13224' Use-After-Free Vulnerability (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2019-13224
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to a use-after-free vulnerability in a used third-pary library. The flaw exists due to a use-after-free in onig_new_deluxe() in regext.c of the third-party library Oniguruma 6.9.2 which is used by PHP. The attacker provides a pair of a regex pattern and a string, with a multi-byte encoding that gets handled by onig_new_deluxe(). This flaw allows attackers to potentially cause information disclosure, denial of service, or possibly code execution by providing a crafted regular expression.

Solution:

VendorFix Update to version 7.1.32, 7.3.9 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.1.32 Installation path / port: 443/tcp

References:

- http://bugs.php.net/78380,https://www.php.net/ChangeLog-7.php#7.3.9,https://www.php.net/ChangeLog-7.php#7.1.32

Unique Alert ID: 539094 Found on: 2023-10-06 Severity: Critical

PHP 'CVE-2019-13224' Use-After-Free Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2019-13224
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to a use-after-free vulnerability in a used third-pary library. The flaw exists due to a use-after-free in onig_new_deluxe() in regext.c of the third-party library Oniguruma 6.9.2 which is used by PHP. The attacker provides a pair of a regex pattern and a string, with a multi-byte encoding that gets handled by onig_new_deluxe(). This flaw allows attackers to potentially cause information disclosure, denial of service, or possibly code execution by providing a crafted regular expression.

Solution:

VendorFix Update to version 7.1.32, 7.3.9 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.1.32 Installation path / port: 80/tcp

References:

- http://bugs.php.net/78380,https://www.php.net/ChangeLog-7.php#7.3.9,https://www.php.net/ChangeLog-7.php#7.1.32

Unique Alert ID: 539119 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities - 04 - Jul16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2015-8867,CVE-2015-8876,CVE-2015-8873,CVE-2015-8835	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws exist due to: - An improper validation of certain Exception objects i n 'Zend/zend_exceptions.c' script. - The 'openssl_random_pseudo_bytes' function in 'ext/openssl/openssl.c' incorrectly re lies on the deprecated 'RAND_pseudo_bytes' function. Successfully exploiting this issue allow remote attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger unintended method execution to defeat crypt ographic protection mechanisms.

Solution:

VendorFix Update to PHP version 5.4.44, or 5.5.28, or 5.6.12, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.44

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539063 Found on: 2023-10-06 Severity: Critical

PHP 'type confusion' Denial of Service Vulnerability (Linux) (tcp/80)

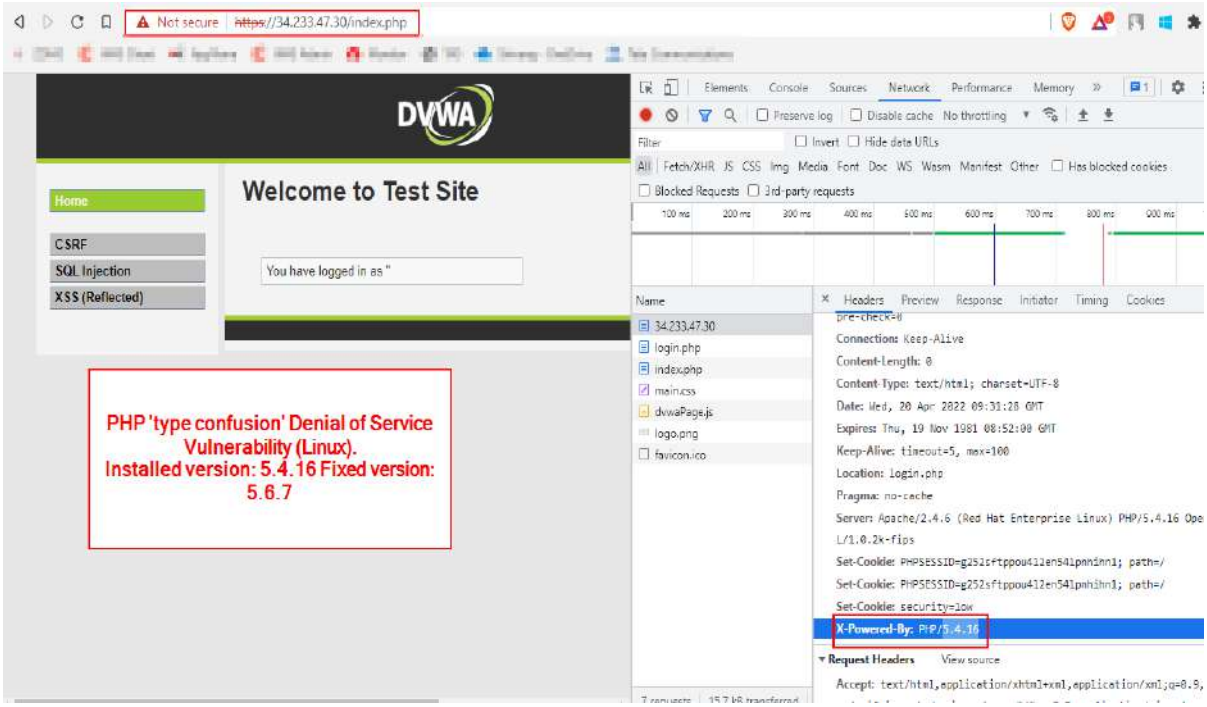
Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2015-4601	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to 'type confusion' issues in 'ext/soap/php_encodin g.c', 'ext/soap/php_http.c', and 'ext/soap/soap.c' scripts. Successfully exploiting this issue allow remote attackers to caus e a denial of service.

Proof of Concept:

POC 1: PHP 'type confusion' Denial of Service Vulnerability (Linux).Installed version: 5.4.16 Fixed version: 5.6.7



Solution:

VendorFix Update to PHP version 5.6.7 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.7

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539062 Found on: 2023-10-06 Severity: Critical

PHP 'type confusion' Denial of Service Vulnerability (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-4601		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to 'type confusion' issues in 'ext/soap/php_encoding.c', 'ext/soap/php_http.c', and 'ext/soap/soap.c' scripts. Successfully exploiting this issue allow remote attackers to cause a denial of service.

Solution:

VendorFix Update to PHP version 5.6.7 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.7

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 919534 Found on: 2023-10-06 Severity: Critical

PHP < 5.6.29, 7.0.x < 7.0.14 DoS Vulnerability - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2016-9935	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to a denial of service (DoS) vulnerability. The php_wddx_push_element function in ext/wddx/wddx.c allows remote attackers to cause a denial of service (out-of-bounds read and memory corruption) or possibly have unspecified other impact via an empty boolean element in a wddxPacket XML document.

Solution:

VendorFix Update to version 5.6.29, 7.0.14 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.29 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.0.14,https://www.php.net/ChangeLog-5.php#5.6.29,https://bugs.php.net/bug.php?id=73631

Unique Alert ID: 539096 Found on: 2023-10-06 Severity: Critical

PHP 'CVE-2019-11043' FPM Remote Code Execution Vulnerability (Version Check) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2019-11043	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to a remote code execution vulnerability in certain nginx + php-fpm configurations. The file sapi/fpm/fpm/fpm_main.c contains pointer arithmetic that assumes that env_path_info has a prefix equal to the path to the php script. However, the code does not check this assumption is satisfied. The absence of the check can lead to an invalid pointer in the 'path_info' variable. Such conditions can be achieved in a pretty standard Nginx configuration. The regexp in `fastcgi_split_path_info` directive can be broken using the newline character (in encoded form, %0a). Broken regexp leads to empty PATH_INFO, which triggers the bug. Successful exploitation would allow an unauthenticated remote attacker to execute arbitrary code on the target machine.

Solution:

VendorFix Update to version 7.1.33, 7.2.24, 7.3.11 or later. As an alternative a workaround to update the nginx configuration to mitigate this vulnerability is described at the PHP.net bugtracker linked in the references.

Result:

Installed version: 5.4.16 Fixed version: 7.1.33 Installation path / port: 443/tcp

References:

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog,https://bugs.php.net/bug.php?id=78599,https://www.php.net/ChangeLog-7.php#7.3.11,https://www.php.net/ChangeLog-7.php#7.2.24,https://www.php.net/ChangeLog-7.php#7.1.33,https://github.com/neex/phuip-fpizdam

Unique Alert ID: 1010820 Found on: 2023-10-06 Severity: Critical

OpenSSL: c_rehash script allows command injection (CVE-2022-1292) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-08-27
CVE ID: CVE-2022-1292
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

OpenSSL is prone to a command injection vulnerability. The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script.

Solution:

VendorFix Update to version 1.0.2ze, 1.1.1o or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2ze Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20220503.txt

Unique Alert ID: 1010821 Found on: 2023-10-06 Severity: Critical

OpenSSL: c_rehash script allows command injection (CVE-2022-1292) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-08-27
CVE ID: CVE-2022-1292
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

OpenSSL is prone to a command injection vulnerability. The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script.

Solution:

VendorFix Update to version 1.0.2ze, 1.1.1o or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2ze Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20220503.txt

Unique Alert ID: 1010822 Found on: 2023-10-06 Severity: Critical

OpenSSL: The c_rehash script allows command injection (CVE-2022-2068) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-08-27
CVE ID:	CVE-2022-2068		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

OpenSSL is prone to a command injection vulnerability. In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prev ent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command exec uted through the shell. This script is distributed by some operating systems in a manner where it is automatically execute d. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool.

Solution:

VendorFix Update to version 1.0.2zf, 1.1.1p, 3.0.4 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2zf Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20220621.txt

Unique Alert ID: 1010823 Found on: 2023-10-06 Severity: Critical

OpenSSL: The c_rehash script allows command injection (CVE-2022-2068) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-08-27
CVE ID:	CVE-2022-2068		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

OpenSSL is prone to a command injection vulnerability. In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prev ent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command exec uted through the shell. This script is distributed by some operating systems in a manner where it is automatically execute d. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool.

Solution:

VendorFix Update to version 1.0.2zf, 1.1.1p, 3.0.4 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2zf Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20220621.txt

Unique Alert ID: 539158 Found on: 2023-10-06 Severity: Critical

OpenSSH X11 Forwarding Security Bypass Vulnerability (Linux) (tcp/22)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-1908	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

openssh is prone to a security bypass vulnerability. An access flaw was discovered in OpenSSH, It did not correctly handl e failures to generate authentication cookies for untrusted X11 forwarding. A malicious or compromised remote X applica tion could possibly use this flaw to establish a trusted connection to the local X server, even if only untrusted X11 forward ing was requested. Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.

Solution:

VendorFix Upgrade to OpenSSH version 7.2 or later.

Result:

Installed version: 6.6.1 Fixed version: 7.2 Installation path / port: 22/tcp

References:

- http://openwall.com/lists/oss-security/2016/01/15/13,https://bugzilla.redhat.com/show_bug.cgi?id=1298741#c4,htt p://www.openssh.com/txt/release-7.2,https://anongit.mindrot.org/openssh.git/commit/?id=ed4ce82dbfa8a3a3c8ea6 fa0db113c71e234416c,https://bugzilla.redhat.com/show_bug.cgi?id=1298741

Unique Alert ID: 539103 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server Multiple Vulnerabilities June17 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2017-7679,CVE-2017-3169,CVE-2017-3167	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Multiple flaws exist as, - The mod_mime can read one byte past t he end of a buffer when sending a malicious Content-Type response header. - The mod_ssl may dereference a NULL poin ter when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port. - An use of th e ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication require ments being bypassed. Successful exploitation will allow remote attackers to bypass authentication and perform unauthor ized actions, cause a denial-of-service condition and gain access to potentially sensitive information.

Solution:

VendorFix Update to Apache HTTP Server 2.2.33 or 2.4.26 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.26 Installation path / port: 443/tcp

References:

- http://seclists.org/oss-sec/2017/q2/509,http://httpd.apache.org/security/vulnerabilities_24.html,http://httpd.apache .org/security/vulnerabilities_22.html

Unique Alert ID: 539087 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server Multiple Vulnerabilities June17 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2017-7679,CVE-2017-3169,CVE-2017-3167		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Multiple flaws exist as, - The mod_mime can read one byte past t he end of a buffer when sending a malicious Content-Type response header. - The mod_ssl may dereference a NULL poin ter when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port. - An use of th e ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication require ments being bypassed. Successful exploitation will allow remote attackers to bypass authentication and perform unauthor ized actions, cause a denial-of-service condition and gain access to potentially sensitive information.

Solution:

VendorFix Update to Apache HTTP Server 2.2.33 or 2.4.26 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.26 Installation path / port: 80/tcp

References:

- http://seclists.org/oss-sec/2017/q2/509,http://httpd.apache.org/security/vulnerabilities_24.html,http://httpd.apache .org/security/vulnerabilities_22.html

Unique Alert ID: 539124 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities - 03 - Jul16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-4537,CVE-2016-4538,CVE-2016-4539,CVE-2016-4540,CVE-2016-4541,CVE-2016-4542,CVE-2016-4543,CVE-2016-4544		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws exist due to: - An improper validation of TIFF start data in 'exif_pro cess_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An improper validation of IFD sizes in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An improper construction of spprintf arguments, in 'exif_process_TIFF_in_JPEG' functio n in 'ext/exif/exif.c' script. - An error in 'grapheme_strpos function' in 'ext/intl/grapheme/grapheme_string.c'. - An error i n 'xml_parse_into_struct' function in 'ext/xml/xml.c' script. - The 'bcpowmod' function in 'ext/bcmath/bcmath.c' improperl y modifies certain data structures. - An improper validation of input passed to 'bcpowmod' function in 'ext/bcmath/bcmat h.c' script. - An error in 'grapheme_strpos' function in ext/intl/grapheme/grapheme_string.c script. Successfully exploitin g this issue allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other i mpact.

Solution:

VendorFix Update to PHP version 5.5.35, or 5.6.21, or 7.0.6, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.35

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539127 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities - 03 - Jul16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-4537,CVE-2016-4538,CVE-2016-4539,CVE-2016-4540,CVE-2016-4541,CVE-2016-4542,CVE-2016-4543,CVE-2016-4544	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws exist due to: - An improper validation of TIFF start data in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An improper validation of IFD sizes in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An improper construction of spprintf arguments, in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An error in 'grapheme_strpos function' in 'ext/intl/grapheme/grapheme_string.c'. - An error in 'xml_parse_into_struct' function in 'ext/xml/xml.c' script. - The 'bcpowmod' function in 'ext/bcmath/bcmath.c' improperly modifies certain data structures. - An improper validation of input passed to 'bcpowmod' function in 'ext/bcmath/bcmath.c' script. - An error in 'grapheme_strpos' function in ext/intl/grapheme/grapheme_string.c script. Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.5.35, or 5.6.21, or 7.0.6, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.35

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539085 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities - 02 - Aug16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-5771,CVE-2016-5770	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - The 'spl_array.c' in the SPL extension improperly interacts with the unserialize implementation and garbage collection. - The integer overflow in the 'SplFileObject::fread' function in 'spl_directory.c' in the SPL extension. Successfully exploiting this issue allow remote attackers to cause a denial of service (use-after-free and application crash) or possibly execute arbitrary code or possibly have unspecified other impact via a large integer argument.

Solution:

VendorFix Update to PHP version 5.5.37, or 5.6.23, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.37

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539149 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities - 01 - Apr16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-3142,CVE-2016-3141	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - A use-after-free error in wddx.c script in the WDDX ex tension in PHP - An error in the phar_parse_zipfile function in zip.c script in the PHAR extension in PHP. Successfully expl oiting this issue allow remote attackers to gain access to potentially sensitive information and conduct a denial of service (memory corruption and application crash).

Solution:

VendorFix Update to PHP version 5.5.33 or 5.6.19 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.33

References:

- https://bugs.php.net/bug.php?id=71587,https://bugs.php.net/bug.php?id=71498,https://secure.php.net/ChangeLog-5.php

Unique Alert ID: 919528 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server 2.4.0 - 2.4.46 Multiple Vulnerabilities - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2020-35452,CVE-2021-26690,CVE-2021-26691	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2020-35452: mod_auth _digest possible stack overflow by one null byte - CVE-2021-26690: mod_session NULL pointer dereference - CVE-2021-26691: mod_session response handling heap overflow - CVE-2020-35452: A specially crafted Digest nonce can cause a s tack overflow in mod_auth_digest. - CVE-2021-26690: A specially crafted Cookie header handled by mod_session can ca use a NULL pointer dereference and crash, leading to a possible Denial Of Service. - CVE-2021-26691: A specially crafted SessionHeader sent by an origin server could cause a heap overflow.

Solution:

VendorFix Update to version 2.4.48 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.48 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539150 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities - 01 - Apr16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-3142,CVE-2016-3141		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - A use-after-free error in wddx.c script in the WDDX extension in PHP - An error in the phar_parse_zipfile function in zip.c script in the PHAR extension in PHP. Successfully exploiting this issue allow remote attackers to gain access to potentially sensitive information and conduct a denial of service (memory corruption and application crash).

Solution:

VendorFix Update to PHP version 5.5.33 or 5.6.19 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.33

References:

- https://bugs.php.net/bug.php?id=71587,https://bugs.php.net/bug.php?id=71498,https://secure.php.net/ChangeLog-5.php

Unique Alert ID: 539245 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities (Jul 2017 - 01) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2017-7890,CVE-2017-9224,CVE-2017-9225,CVE-2017-9226,CVE-2017-9227,CVE-2017-9228,CVE-2017-9229,CVE-2017-11144,CVE-2017-11145,CVE-2017-11628,CVE-2017-12933		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - An ext/date/lib/parse_date.c out-of-bounds read affecting the php_parse_date function. - The openssl extension PEM sealing code did not check the return value of the OpenSSL sealing function. - lack of bounds checks in the date extension's timelib_meridian parsing code. - A stack-based buffer overflow in the zend_ini_do_op() function in the 'Zend/zend_ini_parser.c' script. - The GIF decoding function gdImageCreateFromGifCtx in gd_gif_in.c in the GD Graphics Library (aka libgd) does not zero colorMap arrays before use. - Heap buffer overread (READ: 1) finish_nested_data from unserialize - Add oniguruma upstream fix Successfully exploiting this issue allow remote attackers to leak information from the interpreter, crash PHP interpreter and also disclose sensitive information.

Solution:

VendorFix Update to version 5.6.31, 7.0.21, 7.1.7 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.31 Installation path / port: 443/tcp

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539246 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities (Jul 2017 - 01) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2017-7890,CVE-2017-9224,CVE-2017-9225,CVE-2017-9226,CVE-2017-9227,CVE-2017-9228,CVE-2017-9229,CVE-2017-11144,CVE-2017-11145,CVE-2017-11628,CVE-2017-12933	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - An ext/date/lib/parse_date.c out-of-bounds read affec ting the php_parse_date function. - The openssl extension PEM sealing code did not check the return value of the OpenSS L sealing function. - lack of bounds checks in the date extension's timelib_meridian parsing code. - A stack-based buffer overflow in the zend_ini_do_op() function in the 'Zend/zend_ini_parser.c' script. - The GIF decoding function gdImageCre ateFromGifCtx in gd_gif_in.c in the GD Graphics Library (aka libgd) does not zero colorMap arrays before use. - Heap buf fer overread (READ: 1) finish_nested_data from unserialize - Add oniguruma upstream fix Successfully exploiting this iss ue allow remote attackers to leak information from the interpreter, crash PHP interpreter and also disclose sensitive infor mation.

Solution:

VendorFix Update to version 5.6.31, 7.0.21, 7.1.7 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.31 Installation path / port: 80/tcp

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 919529 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server 2.4.0 - 2.4.46 Multiple Vulnerabilities - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2020-35452,CVE-2021-26690,CVE-2021-26691	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2020-35452: mod_auth _digest possible stack overflow by one null byte - CVE-2021-26690: mod_session NULL pointer dereference - CVE-2021-26691: mod_session response handling heap overflow - CVE-2020-35452: A specially crafted Digest nonce can cause a s tack overflow in mod_auth_digest. - CVE-2021-26690: A specially crafted Cookie header handled by mod_session can ca use a NULL pointer dereference and crash, leading to a possible Denial Of Service. - CVE-2021-26691: A specially crafted SessionHeader sent by an origin server could cause a heap overflow.

Solution:

VendorFix Update to version 2.4.48 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.48 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539155 Found on: 2023-10-06 Severity: Critical

PHP Multiple DoS Vulnerabilities (Oct 2016) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-7568,CVE-2016-9137		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple denial of service (DoS) vulnerabilities. - Fixed bug #73003 (Integer Overflow in gdImageWebpCtx of gd_webp.c). - Fixed bug #73147 (Use After Free in PHP7 unserialize()). Successfully exploiting this issue allows a remote attacker to cause a DoS, or possibly have unspecified other impact.

Solution:

VendorFix Update to version 5.6.27, 7.0.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.27 Installation path / port: 443/tcp

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php,http://seclists.org/oss-sec/2016/q3/639,https://bugs.php.net/bug.php?id=73003,https://bugs.php.net/bug.php?id=73147

Unique Alert ID: 539156 Found on: 2023-10-06 Severity: Critical

PHP Multiple DoS Vulnerabilities (Oct 2016) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-7568,CVE-2016-9137		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple denial of service (DoS) vulnerabilities. - Fixed bug #73003 (Integer Overflow in gdImageWebpCtx of gd_webp.c). - Fixed bug #73147 (Use After Free in PHP7 unserialize()). Successfully exploiting this issue allows a remote attacker to cause a DoS, or possibly have unspecified other impact.

Solution:

VendorFix Update to version 5.6.27, 7.0.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.27 Installation path / port: 80/tcp

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php,http://seclists.org/oss-sec/2016/q3/639,https://bugs.php.net/bug.php?id=73003,https://bugs.php.net/bug.php?id=73147

Unique Alert ID: 539134 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities - 02 - Aug16 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-5771,CVE-2016-5770
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - The 'spl_array.c' in the SPL extension improperly interacts with the unserialize implementation and garbage collection. - The integer overflow in the 'SplFileObject::fread' function in 'spl_directory.c' in the SPL extension. Successfully exploiting this issue allow remote attackers to cause a denial of service (use-after-free and application crash) or possibly execute arbitrary code or possibly have unspecified other impact via a large integer argument.

Solution:

VendorFix Update to PHP version 5.5.37, or 5.6.23, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.37

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539179 Found on: 2023-10-06 Severity: Critical

PHP XML Entity Expansion And XML External Entity Vulnerabilities (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-8866
Cvss Base: 9.6
Cvss Score: 9.6
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Description:

PHP is prone to XML entity expansion and XML external entity vulnerabilities. The flaw is due to script 'ext/libxml/libxml.c' does not isolate each thread from 'libxml_disable_entity_loader' when PHP-FPM is used. Successfully exploiting this issue allow remote attackers to conduct XML External Entity (XXE) and XML Entity Expansion (XEE) attacks.

Solution:

VendorFix Update to PHP version 5.5.22, or 5.6.6, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.22

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539178 Found on: 2023-10-06 Severity: Critical

PHP XML Entity Expansion And XML External Entity Vulnerabilities (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18

CVE ID: CVE-2015-8866
Cvss Base: 9.6
Cvss Score: 9.6
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Description:

PHP is prone to XML entity expansion and XML external entity vulnerabilities. The flaw is due to script 'ext/libxml/libxml.c' does not isolate each thread from 'libxml_disable_entity_loader' when PHP-FPM is used. Successfully exploiting this issue allow remote attackers to conduct XML External Entity (XXE) and XML Entity Expansion (XEE) attacks.

Solution:

VendorFix Update to PHP version 5.5.22, or 5.6.6, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.22

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539195 Found on: 2023-10-06 Severity: Critical

PHP < 7.2.27, 7.3.x < 7.3.14, 7.4.x < 7.4.2 Multiple Vulnerabilities - Jan20 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2020-7059,CVE-2020-7060
Cvss Base: 9.1
Cvss Score: 9.1
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Description:

PHP is prone to multiple vulnerabilities. PHP is prone to multiple vulnerabilities: - OOB read in php_strip_tags_ex (CVE-2020-7059) - Global buffer-overflow in 'mbfl_filt_conv_big5_wchar' (CVE-2020-7060)

Solution:

VendorFix Update to version 7.2.27, 7.3.14, 7.4.2 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.27 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.27,https://www.php.net/ChangeLog-7.php#7.3.14,https://www.php.net/ChangeLog-7.php#7.4.2

Unique Alert ID: 539204 Found on: 2023-10-06 Severity: Critical

PHP Out of Bounds Read Memory Corruption Vulnerability - 01 - Mar16 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-1903
Cvss Base: 9.1
Cvss Score: 9.1
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Description:

PHP is prone to an out-of-bounds read memory corruption vulnerability. The flaw is due to memory corruption vulnerabilit y via a large 'bgd_color' argument to the 'imagerotate' function in 'ext/gd/libgd/gd_interpolation.c' script. Successfully ex ploiting this issue allow remote attackers to obtain sensitive information or cause a denial-of-service condition.

Solution:

VendorFix Update to PHP version 5.5.31, or 5.6.17 or 7.0.2 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.31

References:

- https://bugs.php.net/bug.php?id=70976,http://www.openwall.com/lists/oss-security/2016/01/14/8

Unique Alert ID: 539203 Found on: 2023-10-06 Severity: Critical

PHP Out of Bounds Read Memory Corruption Vulnerability - 01 - Mar16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-1903
Cvss Base: 9.1
Cvss Score: 9.1
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Description:

PHP is prone to an out-of-bounds read memory corruption vulnerability. The flaw is due to memory corruption vulnerabilit y via a large 'bgd_color' argument to the 'imagerotate' function in 'ext/gd/libgd/gd_interpolation.c' script. Successfully ex ploiting this issue allow remote attackers to obtain sensitive information or cause a denial-of-service condition.

Solution:

VendorFix Update to PHP version 5.5.31, or 5.6.17 or 7.0.2 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.31

References:

- https://bugs.php.net/bug.php?id=70976,http://www.openwall.com/lists/oss-security/2016/01/14/8

Unique Alert ID: 539202 Found on: 2023-10-06 Severity: Critical

PHP Denial of Service Vulnerability - 02 - Aug16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-5114
Cvss Base: 9.1
Cvss Score: 9.1
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to the 'sapi/fpm/fpm/fpm_log.c' script misinterpret s the semantics of the snprintf return value. Successfully exploiting this issue allow attackers to obtain sensitive informati on from process memory or cause a denial of service (out-of-bounds read and buffer overflow) via a long string.

Solution:

VendorFix Update to PHP version 5.5.31, or 5.6.17, or 7.0.2, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.31

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539193 Found on: 2023-10-06 Severity: Critical

PHP < 7.2.27, 7.3.x < 7.3.14, 7.4.x < 7.4.2 Multiple Vulnerabilities - Jan20 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2020-7059,CVE-2020-7060	
Cvss Base:	9.1	
Cvss Score:	9.1	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H	

Description:

PHP is prone to multiple vulnerabilities. PHP is prone to multiple vulnerabilities: - OOB read in php_strip_tags_ex (CVE-2020-7059) - Global buffer-overflow in 'mbfl_filt_conv_big5_wchar' (CVE-2020-7060)

Solution:

VendorFix Update to version 7.2.27, 7.3.14, 7.4.2 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.27 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.27,https://www.php.net/ChangeLog-7.php#7.3.14,https://www.php.net/ChangeLog-7.php#7.4.2

Unique Alert ID: 539191 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2017-9788	
Cvss Base:	9.1	
Cvss Score:	9.1	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H	

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The flaw exists due to error in Apache 'mod_auth_digest' which does not properly initialize memory used to process 'Digest' type HTTP Authorization headers. Successful exploitation will allow remote attackers to cause the target service to crash. A remote user can obtain potentially sensitive information as well on the target system.

Solution:

VendorFix Update to Apache HTTP Server 2.2.34 or 2.4.27 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.27 Installation path / port: 80/tcp

References:

- http://www.securitytracker.com/id/1038906,http://httpd.apache.org/security/vulnerabilities_22.html,http://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539205 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2017-9788		
Cvss Base:	9.1		
Cvss Score:	9.1		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H		

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The flaw exists due to error in Apache 'mod_auth_digest' which d oes not properly initialize memory used to process 'Digest' type HTTP Authorization headers. Successful exploitation will allow remote attackers to cause the target service to crash. A remote user can obtain potentially sensitive information as well on the target system.

Solution:

VendorFix Update to Apache HTTP Server 2.2.34 or 2.4.27 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.27 Installation path / port: 443/tcp

References:

- http://www.securitytracker.com/id/1038906,http://httpd.apache.org/security/vulnerabilities_22.html,http://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539200 Found on: 2023-10-06 Severity: Critical

PHP Denial of Service Vulnerability - 02 - Aug16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-5114		
Cvss Base:	9.1		
Cvss Score:	9.1		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H		

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to the 'sapi/fpm/fpm/fpm_log.c' script misinterpret s the semantics of the snprintf return value. Successfully exploiting this issue allow attackers to obtain sensitive informati on from process memory or cause a denial of service (out-of-bounds read and buffer overflow) via a long string.

Solution:

VendorFix Update to PHP version 5.5.31, or 5.6.17, or 7.0.2, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.31

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 1533213 Found on: 2023-10-06 Severity: Critical

PHP < 8.0.30, 8.1.x < 8.1.22, 8.2.x < 8.2.9 Security Update - Linux (tcp/80)

Open Status: NEW **First Found:** 2023-10-06
CVE ID: CVE-2023-3823,CVE-2023-3824
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - CVE-2023-3823: Fixed bug GHSA-3qrf-m4j2-pcrr (Security issue with external entity loading in XML without enabling it) - CVE-2023-3824: Fixed bug GHSA-jqcx-ccgc-xwhv (Buffer mismanagement in phar_dir_read())

Solution:

VendorFix Update to version 8.0.30, 8.1.22, 8.2.9 or later.

Result:

Installed version: 5.4.16 Fixed version: 8.0.30 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-8.php#8.1.22,https://www.php.net/ChangeLog-8.php#8.0.30,https://www.php.net/ChangeLog-8.php#8.2.9,https://github.com/php/php-src/security/advisories/GHSA-3qrf-m4j2-pcrr,https://github.com/php/php-src/security/advisories/GHSA-jqcx-ccgc-xwhv

Unique Alert ID: 1533214 Found on: 2023-10-06 Severity: Critical

PHP < 8.0.30, 8.1.x < 8.1.22, 8.2.x < 8.2.9 Security Update - Linux (tcp/443)

Open Status: NEW **First Found:** 2023-10-06
CVE ID: CVE-2023-3823,CVE-2023-3824
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - CVE-2023-3823: Fixed bug GHSA-3qrf-m4j2-pcrr (Security issue with external entity loading in XML without enabling it) - CVE-2023-3824: Fixed bug GHSA-jqcx-ccgc-xwhv (Buffer mismanagement in phar_dir_read())

Solution:

VendorFix Update to version 8.0.30, 8.1.22, 8.2.9 or later.

Result:

Installed version: 5.4.16 Fixed version: 8.0.30 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-8.php#8.1.22,https://www.php.net/ChangeLog-8.php#8.0.30,https://www.php.net/ChangeLog-8.php#8.2.9,https://github.com/php/php-src/security/advisories/GHSA-3qrf-m4j2-pcrr,https://github.com/php/php-src/security/advisories/GHSA-jqcx-ccgc-xwhv

Unique Alert ID: 539309 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities (Jun/Aug 2014) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-3981,CVE-2014-4721,CVE-2014-0207,CVE-2014-3478,CVE-2014-3479,CVE-2014-3480,CVE-2014-3487,CVE-2014-4049,CVE-2014-3515,CVE-2014-9912		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. The following vulnerabilities exist: - Fixed bug #67390 (insecure temporary file use in the configure script). (CVE-2014-3981). - Fixed bug #67498 (phpinfo() Type Confusion Information Leak Vulnerability). (CVE-2014-4721). - Fixed bug #67326 (cdf_read_short_sector insufficient boundary check). (CVE-2014-0207). - Fixed bug #67410 (mconvert incorrect handling of truncated pascal string size). (CVE-2014-3478). - Fixed bug #67411 (cdf_check_stream_offset insufficient boundary check). (CVE-2014-3479). - Fixed bug #67412 (cdf_count_chain insufficient boundary check). (CVE-2014-3480). - Fixed bug #67413 (cdf_read_property_info insufficient boundary check). (CVE-2014-3487). - Fixed bug #67432 (Fix potential segfault in dns_get_record()). (CVE-2014-4049). - Fixed bug #67492 (unserialize() SPL ArrayObject / SPLObjectStorage Type Confusion). (CVE-2014-3515). - Fixed bug #67397 (Buffer overflow in locale_get_display_name and uloc_getDisplayName (libicu 4.8.1)). (CVE-2014-9912).

Solution:

VendorFix Update to version 5.3.29, 5.4.30, 5.5.14 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.30 Installation path / port: 80/tcp

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=67390,https://bugs.php.net/bug.php?id=67498,https://bugs.php.net/bug.php?id=67326,https://bugs.php.net/bug.php?id=67410,https://bugs.php.net/bug.php?id=67411,https://bugs.php.net/bug.php?id=67412,https://bugs.php.net/bug.php?id=67413,https://bugs.php.net/bug.php?id=67432,https://bugs.php.net/bug.php?id=67492,http://seclists.org/fulldisclosure/2014/Jun/21,https://www.sektioneins.de/en/blog/14-07-04-phpinfo-infoleak.html,http://secunia.com/advisories/59575

Unique Alert ID: 539308 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities (Jun/Aug 2014) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-3981,CVE-2014-4721,CVE-2014-0207,CVE-2014-3478,CVE-2014-3479,CVE-2014-3480,CVE-2014-3487,CVE-2014-4049,CVE-2014-3515,CVE-2014-9912		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. The following vulnerabilities exist: - Fixed bug #67390 (insecure temporary file use in the configure script). (CVE-2014-3981). - Fixed bug #67498 (phpinfo() Type Confusion Information Leak Vulnerability). (CVE-2014-4721). - Fixed bug #67326 (cdf_read_short_sector insufficient boundary check). (CVE-2014-0207). - Fixed bug #67410 (mconvert incorrect handling of truncated pascal string size). (CVE-2014-3478). - Fixed bug #67411 (cdf_ch

eck_stream_offset insufficient boundary check). (CVE-2014-3479). - Fixed bug #67412 (cdf_count_chain insufficient boundary check). (CVE-2014-3480). - Fixed bug #67413 (cdf_read_property_info insufficient boundary check). (CVE-2014-3487). - Fixed bug #67432 (Fix potential segfault in dns_get_record()). (CVE-2014-4049). - Fixed bug #67492 (unserialize() SPL ArrayObject / SPLObjectStorage Type Confusion). (CVE-2014-3515). - Fixed bug #67397 (Buffer overflow in locale_get_display_name and uloc_getDisplayName (libicu 4.8.1)). (CVE-2014-9912).

Solution:

VendorFix Update to version 5.3.29, 5.4.30, 5.5.14 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.30 Installation path / port: 443/tcp

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=67390,https://bugs.php.net/bug.php?id=67498,https://bugs.php.net/bug.php?id=67326,https://bugs.php.net/bug.php?id=67410,https://bugs.php.net/bug.php?id=67411,https://bugs.php.net/bug.php?id=67412,https://bugs.php.net/bug.php?id=67413,https://bugs.php.net/bug.php?id=67432,https://bugs.php.net/bug.php?id=67492,http://seclists.org/fulldisclosure/2014/Jun/21,https://www.sektioneins.de/en/blog/14-07-04-phpinfo-infoleak.html,http://secunia.com/advisories/59575

Unique Alert ID: 1533217 Found on: 2023-10-06 Severity: Critical

OpenBSD OpenSSH < 9.3p2 RCE Vulnerability (tcp/22)

Open Status:	NEW	**First Found:**	2023-10-06
CVE ID:	CVE-2023-38408		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

OpenBSD OpenSSH is prone to a remote code execution (RCE) vulnerability in OpenSSH's forwarded ssh-agent. A condition where specific libraries loaded via ssh-agent(1)'s PKCS#11 support could be abused to achieve remote code execution via a forwarded agent socket.

Solution:

VendorFix Update to version 9.3p2 or later.

Result:

Installed version: 6.6.1 Fixed version: 9.3p2 Installation path / port: 22/tcp

References:

- https://www.openssh.com/releasenotes.html#9.3p2,https://www.qualys.com/2023/07/19/cve-2023-38408/rce-openssh-forwarded-ssh-agent.txt

Unique Alert ID: 1533222 Found on: 2023-10-06 Severity: Critical

PHP < 7.4.33, 8.0.x < 8.0.25, 8.1.x < 8.1.12 Security Update - Linux (tcp/80)

Open Status:	NEW	**First Found:**	2023-10-06
CVE ID:	CVE-2022-31630,CVE-2022-37454		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2022-31630: OOB read due to insufficient input validation in imageloadfont() - CVE-2022-37454: Buffer overflow in hash_update() on long parameter

Solution:

VendorFix Update to version 7.4.33, 8.0.25, 8.1.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.4.33 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.4.33,https://www.php.net/ChangeLog-8.php#8.0.25,https://www.php.net/ChangeLog-8.php#8.1.12

Unique Alert ID: 1533223 Found on: 2023-10-06 Severity: Critical

PHP < 7.4.33, 8.0.x < 8.0.25, 8.1.x < 8.1.12 Security Update - Linux (tcp/443)

Open Status:	NEW	**First Found:** 2023-10-06
CVE ID:	CVE-2022-31630,CVE-2022-37454	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2022-31630: OOB read due to insufficien t input validation in imageloadfont() - CVE-2022-37454: Buffer overflow in hash_update() on long parameter

Solution:

VendorFix Update to version 7.4.33, 8.0.25, 8.1.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.4.33 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.4.33,https://www.php.net/ChangeLog-8.php#8.0.25,https://www.php.net/ChangeLog-8.php#8.1.12

Unique Alert ID: 1533228 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server 2.4.0 - 2.4.55 HTTP Request Smuggling Vulnerability (Linux) (tcp/443)

Open Status:	NEW	**First Found:** 2023-10-06
CVE ID:	CVE-2023-25690	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

Apache HTTP Server is prone to a HTTP request smuggling vulnerability. Some mod_proxy configurations allow a HTTP R equest Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule o r ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data an d is then re-inserted into the proxied request-target using variable substitution. Request splitting/smuggling could result i n bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisonin g.

Solution:

VendorFix Update to version 2.4.56 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.56 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 1533229 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server 2.4.0 - 2.4.55 HTTP Request Smuggling Vulnerability (Linux) (tcp/80)

Open Status: NEW **First Found:** 2023-10-06
CVE ID: CVE-2023-25690
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

Apache HTTP Server is prone to a HTTP request smuggling vulnerability. Some mod_proxy configurations allow a HTTP R equest Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule o r ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data an d is then re-inserted into the proxied request-target using variable substitution. Request splitting/smuggling could result i n bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisonin g.

Solution:

VendorFix Update to version 2.4.56 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.56 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 607306 Found on: 2023-10-06 Severity: Critical

OpenSSL End of Life (EOL) Detection (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-12-18
Cvss Base: 10.0
Cvss Score: 10.0

Description:

The OpenSSL version on the remote host has reached the end of life and should not be used anymore. An EOL version of OpenSSL is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:

VendorFix Update the OpenSSL version on the remote host to a still supported version.

Result:

The "OpenSSL" version on the remote host has reached the end of life. CPE: cpe:/a:openssl:openssl:1.0.2k Installed version: 1.0.2k Location/URL: 443/tcp EOL version: 1.0.2 EOL date: 2019-12-31

Unique Alert ID: 539065 Found on: 2023-10-06 Severity: Critical

OpenSSL End of Life (EOL) Detection (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 10.0
Cvss Score: 10.0

Description:

The OpenSSL version on the remote host has reached the end of life and should not be used anymore. An EOL version of OpenSSL is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:

VendorFix Update the OpenSSL version on the remote host to a still supported version.

Result:

The "OpenSSL" version on the remote host has reached the end of life. CPE: cpe:/a:openssl:openssl:1.0.2k Installed version: 1.0.2k Location/URL: 80/tcp EOL version: 1.0.2 EOL date: 2019-12-31

Unique Alert ID: 539060 Found on: 2023-10-06 Severity: Critical

PHP End Of Life Detection (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 10.0
Cvss Score: 10.0

Description:

The PHP version on the remote host has reached the end of life and should not be used anymore. Each release branch of PHP is fully supported for two years from its initial stable release. During this period, bugs and security issues that have b een reported are fixed and are released in regular point releases. After this two year period of active support, each bran ch is then supported for an additional year for critical security issues only. Releases during this period are made on an as -needed basis: there may be multiple point releases, or none, depending on the number of reports. Once the three years of support are completed, the branch reaches its end of life and is no longer supported. An end of life version of PHP is n ot receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to c ompromise the security of this host.

Solution:

VendorFix Update the PHP version on the remote host to a still supported version.

Result:

The "PHP" version on the remote host has reached the end of life. CPE: cpe:/a:php:php:5.4.16 Installed version: 5.4.16 EOL version: 5.4 EOL date: 2015-09-03

References:

- https://secure.php.net/supported-versions.php,https://secure.php.net/eol.php

Unique Alert ID: 539069 Found on: 2023-10-06 Severity: Critical

PHP End Of Life Detection (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 10.0
Cvss Score: 10.0

Description:

The PHP version on the remote host has reached the end of life and should not be used anymore. Each release branch of PHP is fully supported for two years from its initial stable release. During this period, bugs and security issues that have b een reported are fixed and are released in regular point releases. After this two year period of active support, each bran ch is then supported for an additional year for critical security issues only. Releases during this period are made on an as -needed basis: there may be multiple point releases, or none, depending on the number of reports. Once the three years of support are completed, the branch reaches its end of life and is no longer supported. An end of life version of PHP is n ot receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to c ompromise the security of this host.

Solution:

VendorFix Update the PHP version on the remote host to a still supported version.

Result:

The "PHP" version on the remote host has reached the end of life. CPE: cpe:/a:php:php:5.4.16 Installed version: 5.4.16 EOL version: 5.4 EOL date: 2015-09-03

References:

- https://secure.php.net/supported-versions.php,https://secure.php.net/eol.php

Unique Alert ID: 919527 Found on: 2023-10-06 Severity: Critical

PHP <= 7.1.5 Multiple DoS Vulnerabilities (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2017-8923,CVE-2017-9119
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to multiple denial of service (DoS) vulnerabilities. The following flaws exist: - CVE-2017-8923: The zend_string_extend function in Zend/zend_string.h does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .

Solution:

WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Result:

Installed version: 5.4.16 Fixed version: None Installation path / port: 443/tcp

References:

- https://bugs.php.net/bug.php?id=73122,https://bugs.php.net/bug.php?id=74310,https://bugs.php.net/bug.php?id=74577,https://bugs.php.net/bug.php?id=74593

Unique Alert ID: 919535 Found on: 2023-10-06 Severity: Critical

PHP < 5.6.29, 7.0.x < 7.0.14 DoS Vulnerability - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2016-9935
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The php_wddx_push_element function in ext/wddx/wddx.c allows remote attackers to cause a denial of service (out-of-bounds read and memory corruption) or possibly have unspecified other impact via an empty boolean element in a wddxPacket XML document.

Solution:

VendorFix Update to version 5.6.29, 7.0.14 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.29 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.0.14,https://www.php.net/ChangeLog-5.php#5.6.29,https://bugs.php.net/bug.php?id=73631

Unique Alert ID: 539098 Found on: 2023-10-06 Severity: Critical

PHP 'CVE-2019-11043' FPM Remote Code Execution Vulnerability (Version Check) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2019-11043		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to a remote code execution vulnerability in certain nginx + php-fpm configurations. The file sapi/fpm/fpm/fpm_main.c contains pointer arithmetic that assumes that env_path_info has a prefix equal to the path to the php script. However, the code does not check this assumption is satisfied. The absence of the check can lead to an invalid pointer in the 'path_info' variable. Such conditions can be achieved in a pretty standard Nginx configuration. The regexp in `fastcgi_split_path_info` directive can be broken using the newline character (in encoded form, %0a). Broken regexp leads to empty PATH_INFO, which triggers the bug. Successful exploitation would allow an unauthenticated remote attacker to execute arbitrary code on the target machine.

Solution:

VendorFix Update to version 7.1.33, 7.2.24, 7.3.11 or later. As an alternative a workaround to update the nginx configuration to mitigate this vulnerability is described at the PHP.net bugtracker linked in the references.

Result:

Installed version: 5.4.16 Fixed version: 7.1.33 Installation path / port: 80/tcp

References:

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog,https://bugs.php.net/bug.php?id=78599,https://www.php.net/ChangeLog-7.php#7.3.11,https://www.php.net/ChangeLog-7.php#7.2.24,https://www.php.net/ChangeLog-7.php#7.1.33,https://github.com/neex/phuip-fpizdam

Unique Alert ID: 919536 Found on: 2023-10-06 Severity: Critical

PHP <= 5.6.27 / 7.0.x <= 7.0.12 DoS Vulnerability (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2016-9138		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to a denial of service (DoS) vulnerability. PHP mishandles property modification during __wakeup processing, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data, as demonstrated by Exception::__toString with DateInterval::__wakeup.

Solution:

WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Result:

Installed version: 5.4.16 Fixed version: None Installation path / port: 80/tcp

References:

- https://bugs.php.net/bug.php?id=73147

Unique Alert ID: 919526 Found on: 2023-10-06 Severity: Critical

PHP <= 7.1.5 Multiple DoS Vulnerabilities (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2017-8923,CVE-2017-9119
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to multiple denial of service (DoS) vulnerabilities. The following flaws exist: - CVE-2017-8923: The zend_string_extend function in Zend/zend_string.h does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .

Solution:

WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Result:

Installed version: 5.4.16 Fixed version: None Installation path / port: 80/tcp

References:

- https://bugs.php.net/bug.php?id=73122,https://bugs.php.net/bug.php?id=74310,https://bugs.php.net/bug.php?id=74577,https://bugs.php.net/bug.php?id=74593

Unique Alert ID: 919525 Found on: 2023-10-06 Severity: Critical

PHP <= 5.6.27 / 7.0.x <= 7.0.12 DoS Vulnerability (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2016-9138
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. PHP mishandles property modification during __wakeup processing, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data, as demonstrated by Exception::__toString with DateInterval::__wakeup.

Solution:

WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Result:

Installed version: 5.4.16 Fixed version: None Installation path / port: 443/tcp

References:

- https://bugs.php.net/bug.php?id=73147

Unique Alert ID: 539105 Found on: 2023-10-06 Severity: Critical

PHP Stack Buffer Overflow Vulnerability Mar18 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-7584
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to a stack buffer overflow vulnerability. The flaw exists because php fails to adequately bounds-check user-supplied data before copying it into an insufficiently sized buffer. Successful exploitation will allow an attacker to execute arbitrary code in the context of the affected application. Failed exploit attempts will result in denial-of-service conditions.

Solution:

VendorFix Update to version 7.2.3, 7.0.28, 5.6.34, 7.1.15 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.34 Installation path / port: 80/tcp

References:

- http://php.net/ChangeLog-7.php,https://bugs.php.net/bug.php?id=75981

Unique Alert ID: 919530 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-34798,CVE-2021-39275,CVE-2021-40438
Cvss Base: 9.0
Cvss Score: 9.0
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2021-34798: NULL pointer dereference in httpd core - CVE-2021-39275: ap_escape_quotes buffer overflow - CVE-2021-40438: mod_proxy SSRF

Solution:

VendorFix Update to version 2.4.49 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.49 Installation path / port: 80/tcp

References:

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog,https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 919531 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server < 2.4.49 Multiple Vulnerabilities - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2021-34798,CVE-2021-39275,CVE-2021-40438	
Cvss Base:	9.0	
Cvss Score:	9.0	
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H	

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2021-34798: NULL pointer dereference in httpd core - CVE-2021-39275: ap_escape_quotes buffer overflow - CVE-2021-40438: mod_proxy SSRF

Solution:

VendorFix Update to version 2.4.49 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.49 Installation path / port: 443/tcp

References:

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog,https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 1010819 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server < 2.4.54 Multiple Vulnerabilities - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2022-08-27
CVE ID:	CVE-2022-26377,CVE-2022-28614,CVE-2022-28615,CVE-2022-29404,CVE-2022-30556,CVE-2022-31813	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2022-26377: mod_proxy_ajp: Possible request smuggling - CVE-2022-28614: Read beyond bounds via ap_rwrite() - CVE-2022-28615: Read beyond bounds in ap_strcmp_match() - CVE-2022-29404: Denial of service in mod_lua r:parsebody - CVE-2022-30556: Information disclosure in mod_lua with websockets - CVE-2022-31813: mod_proxy X-Forwarded-For dropped by hop-by-hop mechanism

Solution:

VendorFix Update to version 2.4.54 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.54 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html#2.4.54

Unique Alert ID: 1010818 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server < 2.4.54 Multiple Vulnerabilities - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2022-08-27
CVE ID:	CVE-2022-26377,CVE-2022-28614,CVE-2022-28615,CVE-2022-29404,CVE-2022-30556,CVE-2022-31813	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2022-26377: mod_proxy_ajp: Possible request smuggling - CVE-2022-28614: Read beyond bounds via ap_rwrite() - CVE-2022-28615: Read beyond bounds in ap_strcmp_match() - CVE-2022-29404: Denial of service in mod_lua r:parsebody - CVE-2022-30556: Information disclosure in mod_lua with websockets - CVE-2022-31813: mod_proxy X-Forwarded-For dropped by hop-by-hop mechanism

Solution:

VendorFix Update to version 2.4.54 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.54 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html#2.4.54

Unique Alert ID: 539054 Found on: 2023-10-06 Severity: Critical

PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-4342,CVE-2016-2554	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to denial of service and unspecified vulnerabilities. The flaw is due an improper handling of zero-length uncompressed data in 'ext/phar/phar_object.c' script. Successfully exploiting this issue allow remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.5.32, or 5.6.18, or 7.0.3, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.32

References:

- http://www.php.net/ChangeLog-7.php,http://www.openwall.com/lists/oss-security/2016/04/28/2

Unique Alert ID: 539056 Found on: 2023-10-06 Severity: Critical

PHP Denial of Service And Unspecified Vulnerabilities - 01 - Jul16 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-4342,CVE-2016-2554
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to denial of service and unspecified vulnerabilities. The flaw is due an improper handling of zero-length uncompressed data in 'ext/phar/phar_object.c' script. Successfully exploiting this issue allow remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.5.32, or 5.6.18, or 7.0.3, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.32

References:

- http://www.php.net/ChangeLog-7.php,http://www.openwall.com/lists/oss-security/2016/04/28/2

Unique Alert ID: 539159 Found on: 2023-10-06 Severity: Critical

PHP Arbitrary Code Execution Vulnerability - Aug16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-4116
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to an arbitrary code execution vulnerability. The flaw is due to Use-after-free vulnerability in the 'spl_ptr_heap_insert' function in 'ext/spl/spl_heap.c'. Successfully exploiting this issue allow remote attackers to execute arbitrary code by triggering a failed SplMinHeap::compare operation.

Solution:

VendorFix Update to PHP version 5.5.27, or 5.6.11, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.27

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539160 Found on: 2023-10-06 Severity: Critical

PHP Arbitrary Code Execution Vulnerability - Aug16 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-4116
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to an arbitrary code execution vulnerability. The flaw is due to Use-after-free vulnerability in the 'spl_ptr_heap_insert' function in 'ext/spl/spl_heap.c'. Successfully exploiting this issue allow remote attackers to execute arbitrary code by triggering a failed SplMinHeap::compare operation.

Solution:

VendorFix Update to PHP version 5.5.27, or 5.6.11, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.27

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 1010812 Found on: 2023-10-06 Severity: Critical

PHP < 7.4.28, 8.0.x < 8.0.16, 8.1.x < 8.1.3 Security Update (Feb 2022) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-08-27
CVE ID: CVE-2021-21708
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP released new versions which include a security fix. Fix #81708: UAF due to php_filter_float() failing for ints.

Solution:

VendorFix Update to version 7.4.28, 8.0.16, 8.1.3 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.4.28 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.4.28,https://www.php.net/ChangeLog-8.php#8.0.16,https://www.php.net/ChangeLog-8.php#8.1.3,https://bugs.php.net/bug.php?id=81708

Unique Alert ID: 1010814 Found on: 2023-10-06 Severity: Critical

PHP < 7.4.28, 8.0.x < 8.0.16, 8.1.x < 8.1.3 Security Update (Feb 2022) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-08-27
CVE ID:	CVE-2021-21708		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP released new versions which include a security fix. Fix #81708: UAF due to php_filter_float() failing for ints.

Solution:

VendorFix Update to version 7.4.28, 8.0.16, 8.1.3 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.4.28 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.4.28,https://www.php.net/ChangeLog-8.php#8.0.16,https://www.php.net/ChangeLog-8.php#8.1.3,https://bugs.php.net/bug.php?id=81708

Unique Alert ID: 539117 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities - 04 - Jul16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-8867,CVE-2015-8876,CVE-2015-8873,CVE-2015-8835		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws exist due to: - An improper validation of certain Exception objects in 'Zend/zend_exceptions.c' script. - The 'openssl_random_pseudo_bytes' function in 'ext/openssl/openssl.c' incorrectly relies on the deprecated 'RAND_pseudo_bytes' function. Successfully exploiting this issue allow remote attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger unintended method execution to defeat cryptographic protection mechanisms.

Solution:

VendorFix Update to PHP version 5.4.44, or 5.5.28, or 5.6.12, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.44

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 919523 Found on: 2023-10-06 Severity: Critical

PHP < 7.0.12 RCE / DoS Vulnerability - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2016-7480		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to a remote code execution (RCE) or denial of service (DoS) vulnerability. The SplObjectStorage unserialize implementation in ext/spl/spl_observer.c does not verify that a key is an object, which allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized memory access) via crafted serialized data.

Solution:

VendorFix Update to version 7.0.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.0.12 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.0.12,https://bugs.php.net/bug.php?id=73257,http://blog.checkpoint.com/2016/12/27/check-point-discovers-three-zero-day-vulnerabilities-web-programming-language-php-7

Unique Alert ID: 919524 Found on: 2023-10-06 Severity: Critical

PHP < 7.0.12 RCE / DoS Vulnerability - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2016-7480		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to a remote code execution (RCE) or denial of service (DoS) vulnerability. The SplObjectStorage unserialize implementation in ext/spl/spl_observer.c does not verify that a key is an object, which allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized memory access) via crafted serialized data.

Solution:

VendorFix Update to version 7.0.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.0.12 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.0.12,https://bugs.php.net/bug.php?id=73257,http://blog.checkpoint.com/2016/12/27/check-point-discovers-three-zero-day-vulnerabilities-web-programming-language-php-7

Unique Alert ID: 539099 Found on: 2023-10-06 Severity: Critical

PHP 'var_unserializer' Denial of Service Vulnerability (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-7411		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to improper handling of object-deserialization failu res in 'ext/standard/var_unserializer.re' script. Successfully exploiting this issue allow remote attackers to cause a denial of service.

Solution:

VendorFix Update to PHP version 5.6.26, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.26

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539104 Found on: 2023-10-06 Severity: Critical

PHP Stack Buffer Overflow Vulnerability Mar18 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2018-7584		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to a stack buffer overflow vulnerability. The flaw exists because php fails to adequately bounds-check user-supplied data before copying it into an insufficiently sized buffer. Successful exploitation will allow an attacker to execute arbitrary code in the context of the affected application. Failed exploit attempts will result in denial-of-service conditions.

Solution:

VendorFix Update to version 7.2.3, 7.0.28, 5.6.34, 7.1.15 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.34 Installation path / port: 443/tcp

References:

- http://php.net/ChangeLog-7.php,https://bugs.php.net/bug.php?id=75981

Unique Alert ID: 539100 Found on: 2023-10-06 Severity: Critical

PHP 'var_unserializer' Denial of Service Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-7411

Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to improper handling of object-deserialization failures in 'ext/standard/var_unserializer.re' script. Successfully exploiting this issue allow remote attackers to cause a denial of service.

Solution:

VendorFix Update to PHP version 5.6.26, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.26

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539058 Found on: 2023-10-06 Severity: Critical

PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-5590,CVE-2015-8838,CVE-2015-5589
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to a stack buffer overflow vulnerability. Multiple flaws are due to - Inadequate boundary checks on user-supplied input by 'phar_fix_filepath' function in 'ext/phar/phar.c' script. - Improper validation of file pointer in the 'phar_convert_to_other' function in 'ext/phar/phar_object.c' script. Successfully exploiting this issue allow remote attackers to execute arbitrary code in the context of the PHP process. Failed exploit attempts will likely crash the webserver.

Solution:

VendorFix Update to PHP version 5.4.43, or 5.5.27, or 5.6.11 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.43

References:

- http://www.php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=69923

Unique Alert ID: 919532 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-44790
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

Apache HTTP Server is prone to a buffer overflow vulnerability. A carefully crafted request body can cause a buffer overf low in the mod_lua multipart parser (r:parsebody() called from Lua scripts).

Solution:

VendorFix Update to version 2.4.52 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.52 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 919533 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server <= 2.4.51 Buffer Overflow Vulnerability - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-44790
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

Apache HTTP Server is prone to a buffer overflow vulnerability. A carefully crafted request body can cause a buffer overf low in the mod_lua multipart parser (r:parsebody() called from Lua scripts).

Solution:

VendorFix Update to version 2.4.52 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.52 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 1010817 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2022-08-27
CVE ID:	CVE-2022-22719,CVE-2022-22720,CVE-2022-22721,CVE-2022-23943	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2022-22719: mod_lua Use of uninitialized value of in r:parsebody - CVE-2022-22720: HTTP request smuggling vulnerability - CVE-2022-22721: Possible buffer overflow with very large or unlimited LimitXMLRequestBody - CVE-2022-23943: mod_sed: Read/write beyond bounds

Solution:

VendorFix Update to version 2.4.53 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.53 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html#2.4.53

Unique Alert ID: 1010816 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server <= 2.4.52 Multiple Vulnerabilities - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2022-08-27
CVE ID:	CVE-2022-22719,CVE-2022-22720,CVE-2022-22721,CVE-2022-23943	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2022-22719: mod_lua Use of uninitialized value of in r:parsebody - CVE-2022-22720: HTTP request smuggling vulnerability - CVE-2022-22721: Possible buffer overflow with very large or unlimited LimitXMLRequestBody - CVE-2022-23943: mod_sed: Read/write beyond bounds

Solution:

VendorFix Update to version 2.4.53 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.53 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html#2.4.53

Unique Alert ID: 539067 Found on: 2023-10-06 Severity: Critical

PHP 'phar_fix_filepath' Function Stack Buffer Overflow Vulnerability - Mar16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-5590,CVE-2015-8838,CVE-2015-5589		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to a stack buffer overflow vulnerability. Multiple flaws are due to - Inadequate boundary checks on user-supplied input by 'phar_fix_filepath' function in 'ext/phar/phar.c' script. - Improper validation of file pointer in the 'phar_convert_to_other' function in 'ext/phar/phar_object.c' script. Successfully exploiting this issue allow remote attackers to execute arbitrary code in the context of the PHP process. Failed exploit attempts will likely crash the webserver.

Solution:

VendorFix Update to PHP version 5.4.43, or 5.5.27, or 5.6.11 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.43

References:

- http://www.php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=69923

Unique Alert ID: 539092 Found on: 2023-10-06 Severity: Critical

PHP 'CVE-2019-13224' Use-After-Free Vulnerability (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2019-13224		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to a use-after-free vulnerability in a used third-pary library. The flaw exists due to a use-after-free in onig_new_deluxe() in regext.c of the third-party library Oniguruma 6.9.2 which is used by PHP. The attacker provides a pair of a regex pattern and a string, with a multi-byte encoding that gets handled by onig_new_deluxe(). This flaw allows attackers to potentially cause information disclosure, denial of service, or possibly code execution by providing a crafted regular expression.

Solution:

VendorFix Update to version 7.1.32, 7.3.9 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.1.32 Installation path / port: 443/tcp

References:

- http://bugs.php.net/78380,https://www.php.net/ChangeLog-7.php#7.3.9,https://www.php.net/ChangeLog-7.php#7.1.32

Unique Alert ID: 539094 Found on: 2023-10-06 Severity: Critical

PHP 'CVE-2019-13224' Use-After-Free Vulnerability (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2019-13224		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to a use-after-free vulnerability in a used third-pary library. The flaw exists due to a use-after-free in onig_new_deluxe() in regext.c of the third-party library Oniguruma 6.9.2 which is used by PHP. The attacker provides a pair of a regex pattern and a string, with a multi-byte encoding that gets handled by onig_new_deluxe(). This flaw allows attackers to potentially cause information disclosure, denial of service, or possibly code execution by providing a crafted regular expression.

Solution:

VendorFix Update to version 7.1.32, 7.3.9 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.1.32 Installation path / port: 80/tcp

References:

- http://bugs.php.net/78380,https://www.php.net/ChangeLog-7.php#7.3.9,https://www.php.net/ChangeLog-7.php#7.1.32

Unique Alert ID: 539119 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities - 04 - Jul16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-8867,CVE-2015-8876,CVE-2015-8873,CVE-2015-8835		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws exist due to: - An improper validation of certain Exception objects in 'Zend/zend_exceptions.c' script. - The 'openssl_random_pseudo_bytes' function in 'ext/openssl/openssl.c' incorrectly relies on the deprecated 'RAND_pseudo_bytes' function. Successfully exploiting this issue allow remote attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger unintended method execution to defeat cryptographic protection mechanisms.

Solution:

VendorFix Update to PHP version 5.4.44, or 5.5.28, or 5.6.12, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.44

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539063 Found on: 2023-10-06 Severity: Critical

PHP 'type confusion' Denial of Service Vulnerability (Linux) (tcp/80)

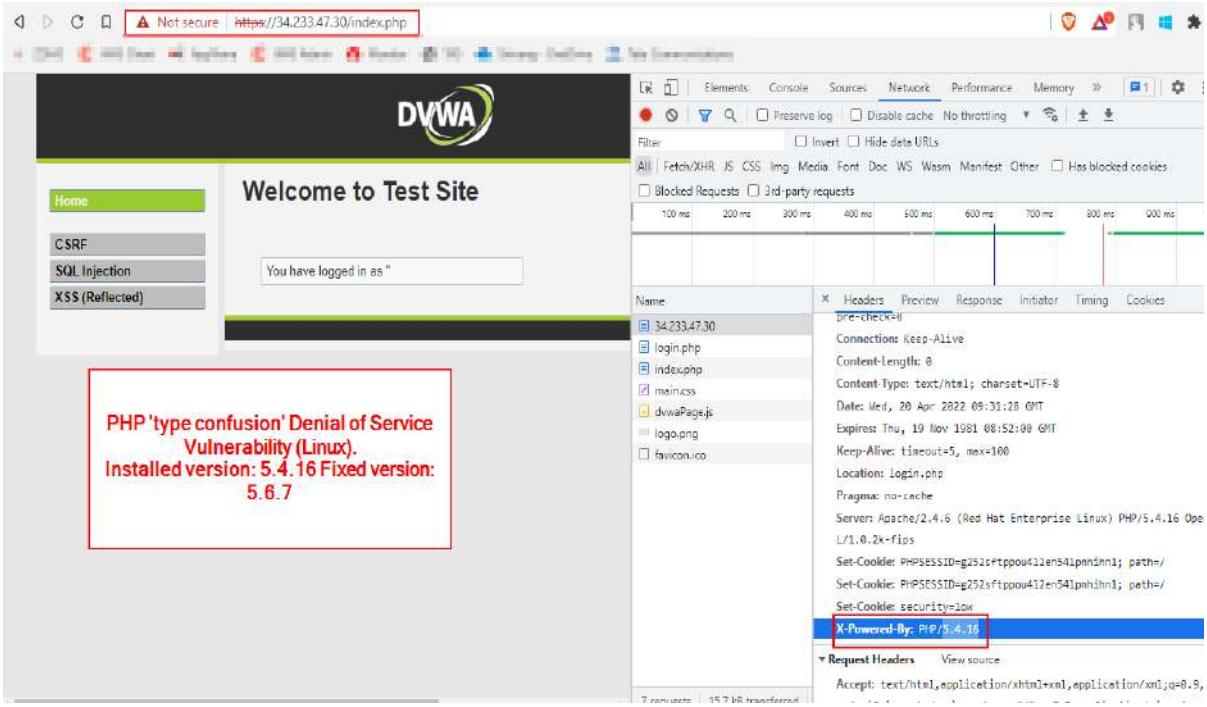
Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-4601
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to 'type confusion' issues in 'ext/soap/php_encoding.c', 'ext/soap/php_http.c', and 'ext/soap/soap.c' scripts. Successfully exploiting this issue allow remote attackers to cause a denial of service.

Proof of Concept:

POC 1: PHP 'type confusion' Denial of Service Vulnerability (Linux).Installed version: 5.4.16 Fixed version: 5.6.7



Solution:

VendorFix Update to PHP version 5.6.7 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.7

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539062 Found on: 2023-10-06 Severity: Critical

PHP 'type confusion' Denial of Service Vulnerability (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-4601		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to 'type confusion' issues in 'ext/soap/php_encoding.c', 'ext/soap/php_http.c', and 'ext/soap/soap.c' scripts. Successfully exploiting this issue allow remote attackers to cause a denial of service.

Solution:

VendorFix Update to PHP version 5.6.7 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.7

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 919534 Found on: 2023-10-06 Severity: Critical

PHP < 5.6.29, 7.0.x < 7.0.14 DoS Vulnerability - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2016-9935		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to a denial of service (DoS) vulnerability. The php_wddx_push_element function in ext/wddx/wddx.c allows remote attackers to cause a denial of service (out-of-bounds read and memory corruption) or possibly have unspecified other impact via an empty boolean element in a wddxPacket XML document.

Solution:

VendorFix Update to version 5.6.29, 7.0.14 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.29 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.0.14,https://www.php.net/ChangeLog-5.php#5.6.29,https://bugs.php.net/bug.php?id=73631

Unique Alert ID: 539096 Found on: 2023-10-06 Severity: Critical

PHP 'CVE-2019-11043' FPM Remote Code Execution Vulnerability (Version Check) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2019-11043		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to a remote code execution vulnerability in certain nginx + php-fpm configurations. The file sapi/fpm/fpm/fpm_main.c contains pointer arithmetic that assumes that env_path_info has a prefix equal to the path to the php script. However, the code does not check this assumption is satisfied. The absence of the check can lead to an invalid pointer in the 'path_info' variable. Such conditions can be achieved in a pretty standard Nginx configuration. The regexp in `fastcgi_split_path_info` directive can be broken using the newline character (in encoded form, %0a). Broken regexp leads to empty PATH_INFO, which triggers the bug. Successful exploitation would allow an unauthenticated remote attacker to execute arbitrary code on the target machine.

Solution:

VendorFix Update to version 7.1.33, 7.2.24, 7.3.11 or later. As an alternative a workaround to update the nginx configuration to mitigate this vulnerability is described at the PHP.net bugtracker linked in the references.

Result:

Installed version: 5.4.16 Fixed version: 7.1.33 Installation path / port: 443/tcp

References:

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog,https://bugs.php.net/bug.php?id=78599,https://www.php.net/ChangeLog-7.php#7.3.11,https://www.php.net/ChangeLog-7.php#7.2.24,https://www.php.net/ChangeLog-7.php#7.1.33,https://github.com/neex/phuip-fpizdam

Unique Alert ID: 1010820 Found on: 2023-10-06 Severity: Critical

OpenSSL: c_rehash script allows command injection (CVE-2022-1292) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-08-27
CVE ID:	CVE-2022-1292		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

OpenSSL is prone to a command injection vulnerability. The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script.

Solution:

VendorFix Update to version 1.0.2ze, 1.1.1o or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2ze Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20220503.txt

Unique Alert ID: 1010821 Found on: 2023-10-06 Severity: Critical

OpenSSL: c_rehash script allows command injection (CVE-2022-1292) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-08-27
CVE ID: CVE-2022-1292
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

OpenSSL is prone to a command injection vulnerability. The c_rehash script does not properly sanitise shell metacharact ers to prevent command injection. This script is distributed by some operating systems in a manner where it is automatic ally executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script .

Solution:

VendorFix Update to version 1.0.2ze, 1.1.1o or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2ze Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20220503.txt

Unique Alert ID: 1010822 Found on: 2023-10-06 Severity: Critical

OpenSSL: The c_rehash script allows command injection (CVE-2022-2068) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-08-27
CVE ID: CVE-2022-2068
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

OpenSSL is prone to a command injection vulnerability. In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prev ent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command exec uted through the shell. This script is distributed by some operating systems in a manner where it is automatically execute d. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool.

Solution:

VendorFix Update to version 1.0.2zf, 1.1.1p, 3.0.4 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2zf Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20220621.txt

Unique Alert ID: 1010823 Found on: 2023-10-06 Severity: Critical

OpenSSL: The c_rehash script allows command injection (CVE-2022-2068) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-08-27
CVE ID:	CVE-2022-2068		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

OpenSSL is prone to a command injection vulnerability. In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prev ent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command exec uted through the shell. This script is distributed by some operating systems in a manner where it is automatically execute d. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool.

Solution:

VendorFix Update to version 1.0.2zf, 1.1.1p, 3.0.4 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2zf Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20220621.txt

Unique Alert ID: 539158 Found on: 2023-10-06 Severity: Critical

OpenSSH X11 Forwarding Security Bypass Vulnerability (Linux) (tcp/22)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-1908		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

openssh is prone to a security bypass vulnerability. An access flaw was discovered in OpenSSH, It did not correctly handl e failures to generate authentication cookies for untrusted X11 forwarding. A malicious or compromised remote X applica tion could possibly use this flaw to establish a trusted connection to the local X server, even if only untrusted X11 forward ing was requested. Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.

Solution:

VendorFix Upgrade to OpenSSH version 7.2 or later.

Result:

Installed version: 6.6.1 Fixed version: 7.2 Installation path / port: 22/tcp

References:

- http://openwall.com/lists/oss-security/2016/01/15/13,https://bugzilla.redhat.com/show_bug.cgi?id=1298741#c4,htt p://www.openssh.com/txt/release-7.2,https://anongit.mindrot.org/openssh.git/commit/?id=ed4ce82dbfa8a3a3c8ea6 fa0db113c71e234416c,https://bugzilla.redhat.com/show_bug.cgi?id=1298741

Unique Alert ID: 539103 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server Multiple Vulnerabilities June17 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2017-7679,CVE-2017-3169,CVE-2017-3167		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Multiple flaws exist as, - The mod_mime can read one byte past t he end of a buffer when sending a malicious Content-Type response header. - The mod_ssl may dereference a NULL poin ter when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port. - An use of th e ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication require ments being bypassed. Successful exploitation will allow remote attackers to bypass authentication and perform unauthor ized actions, cause a denial-of-service condition and gain access to potentially sensitive information.

Solution:

VendorFix Update to Apache HTTP Server 2.2.33 or 2.4.26 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.26 Installation path / port: 443/tcp

References:

- http://seclists.org/oss-sec/2017/q2/509,http://httpd.apache.org/security/vulnerabilities_24.html,http://httpd.apache .org/security/vulnerabilities_22.html

Unique Alert ID: 539087 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server Multiple Vulnerabilities June17 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2017-7679,CVE-2017-3169,CVE-2017-3167		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Multiple flaws exist as, - The mod_mime can read one byte past t he end of a buffer when sending a malicious Content-Type response header. - The mod_ssl may dereference a NULL poin ter when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port. - An use of th e ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication require ments being bypassed. Successful exploitation will allow remote attackers to bypass authentication and perform unauthor ized actions, cause a denial-of-service condition and gain access to potentially sensitive information.

Solution:

VendorFix Update to Apache HTTP Server 2.2.33 or 2.4.26 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.26 Installation path / port: 80/tcp

References:

- http://seclists.org/oss-sec/2017/q2/509,http://httpd.apache.org/security/vulnerabilities_24.html,http://httpd.apache .org/security/vulnerabilities_22.html

Unique Alert ID: 539124 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities - 03 - Jul16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-4537,CVE-2016-4538,CVE-2016-4539,CVE-2016-4540,CVE-2016-4541,CVE-2016-4542,CVE-2016-4543,CVE-2016-4544	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws exist due to: - An improper validation of TIFF start data in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An improper validation of IFD sizes in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An improper construction of spprintf arguments, in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An error in 'grapheme_strpos function' in 'ext/intl/grapheme/grapheme_string.c'. - An error in 'xml_parse_into_struct' function in 'ext/xml/xml.c' script. - The 'bcpowmod' function in 'ext/bcmath/bcmath.c' improperly modifies certain data structures. - An improper validation of input passed to 'bcpowmod' function in 'ext/bcmath/bcmath.c' script. - An error in 'grapheme_strpos' function in ext/intl/grapheme/grapheme_string.c script. Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.5.35, or 5.6.21, or 7.0.6, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.35

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539127 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities - 03 - Jul16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-4537,CVE-2016-4538,CVE-2016-4539,CVE-2016-4540,CVE-2016-4541,CVE-2016-4542,CVE-2016-4543,CVE-2016-4544	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws exist due to: - An improper validation of TIFF start data in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An improper validation of IFD sizes in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An improper construction of spprintf arguments, in 'exif_process_TIFF_in_JPEG' function in 'ext/exif/exif.c' script. - An error in 'grapheme_strpos function' in 'ext/intl/grapheme/grapheme_string.c'. - An error in 'xml_parse_into_struct' function in 'ext/xml/xml.c' script. - The 'bcpowmod' function in 'ext/bcmath/bcmath.c' improperly modifies certain data structures. - An improper validation of input passed to 'bcpowmod' function in 'ext/bcmath/bcmath.c' script. - An error in 'grapheme_strpos' function in ext/intl/grapheme/grapheme_string.c script. Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.5.35, or 5.6.21, or 7.0.6, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.35

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539085 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities - 02 - Aug16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-5771,CVE-2016-5770		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - The 'spl_array.c' in the SPL extension improperly interacts with the unserialize implementation and garbage collection. - The integer overflow in the 'SplFileObject::fread' function in 'spl_directory.c' in the SPL extension. Successfully exploiting this issue allow remote attackers to cause a denial of service (use-after-free and application crash) or possibly execute arbitrary code or possibly have unspecified other impact via a large integer argument.

Solution:

VendorFix Update to PHP version 5.5.37, or 5.6.23, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.37

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539149 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities - 01 - Apr16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-3142,CVE-2016-3141		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - A use-after-free error in wddx.c script in the WDDX extension in PHP - An error in the phar_parse_zipfile function in zip.c script in the PHAR extension in PHP. Successfully exploiting this issue allow remote attackers to gain access to potentially sensitive information and conduct a denial of service (memory corruption and application crash).

Solution:

VendorFix Update to PHP version 5.5.33 or 5.6.19 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.33

References:

- https://bugs.php.net/bug.php?id=71587,https://bugs.php.net/bug.php?id=71498,https://secure.php.net/ChangeLog-5.php

Unique Alert ID: 919528 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server 2.4.0 - 2.4.46 Multiple Vulnerabilities - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2020-35452,CVE-2021-26690,CVE-2021-26691		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2020-35452: mod_auth _digest possible stack overflow by one null byte - CVE-2021-26690: mod_session NULL pointer dereference - CVE-2021-26691: mod_session response handling heap overflow - CVE-2020-35452: A specially crafted Digest nonce can cause a s tack overflow in mod_auth_digest. - CVE-2021-26690: A specially crafted Cookie header handled by mod_session can ca use a NULL pointer dereference and crash, leading to a possible Denial Of Service. - CVE-2021-26691: A specially crafted SessionHeader sent by an origin server could cause a heap overflow.

Solution:

VendorFix Update to version 2.4.48 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.48 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539150 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities - 01 - Apr16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-3142,CVE-2016-3141		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - A use-after-free error in wddx.c script in the WDDX ex tension in PHP - An error in the phar_parse_zipfile function in zip.c script in the PHAR extension in PHP. Successfully expl oiting this issue allow remote attackers to gain access to potentially sensitive information and conduct a denial of service (memory corruption and application crash).

Solution:

VendorFix Update to PHP version 5.5.33 or 5.6.19 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.33

References:

- https://bugs.php.net/bug.php?id=71587,https://bugs.php.net/bug.php?id=71498,https://secure.php.net/ChangeLog-5.php

Unique Alert ID: 539245 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities (Jul 2017 - 01) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2017-7890,CVE-2017-9224,CVE-2017-9225,CVE-2017-9226,CVE-2017-9227,CVE-2017-9228,CVE-2017-9229,CVE-2017-11144,CVE-2017-11145,CVE-2017-11628,CVE-2017-12933		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - An ext/date/lib/parse_date.c out-of-bounds read affecting the php_parse_date function. - The openssl extension PEM sealing code did not check the return value of the OpenSSL sealing function. - lack of bounds checks in the date extension's timelib_meridian parsing code. - A stack-based buffer overflow in the zend_ini_do_op() function in the 'Zend/zend_ini_parser.c' script. - The GIF decoding function gdImageCreateFromGifCtx in gd_gif_in.c in the GD Graphics Library (aka libgd) does not zero colorMap arrays before use. - Heap buffer overread (READ: 1) finish_nested_data from unserialize - Add oniguruma upstream fix Successfully exploiting this issue allow remote attackers to leak information from the interpreter, crash PHP interpreter and also disclose sensitive information.

Solution:

VendorFix Update to version 5.6.31, 7.0.21, 7.1.7 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.31 Installation path / port: 443/tcp

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539246 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities (Jul 2017 - 01) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2017-7890,CVE-2017-9224,CVE-2017-9225,CVE-2017-9226,CVE-2017-9227,CVE-2017-9228,CVE-2017-9229,CVE-2017-11144,CVE-2017-11145,CVE-2017-11628,CVE-2017-12933		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - An ext/date/lib/parse_date.c out-of-bounds read affecting the php_parse_date function. - The openssl extension PEM sealing code did not check the return value of the OpenSSL sealing function. - lack of bounds checks in the date extension's timelib_meridian parsing code. - A stack-based buffer overflow in the zend_ini_do_op() function in the 'Zend/zend_ini_parser.c' script. - The GIF decoding function gdImageCreateFromGifCtx in gd_gif_in.c in the GD Graphics Library (aka libgd) does not zero colorMap arrays before use. - Heap buffer overread (READ: 1) finish_nested_data from unserialize - Add oniguruma upstream fix Successfully exploiting this issue allow remote attackers to leak information from the interpreter, crash PHP interpreter and also disclose sensitive information.

Solution:

VendorFix Update to version 5.6.31, 7.0.21, 7.1.7 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.31 Installation path / port: 80/tcp

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 919529 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server 2.4.0 - 2.4.46 Multiple Vulnerabilities - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2020-35452,CVE-2021-26690,CVE-2021-26691	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2020-35452: mod_auth _digest possible stack overflow by one null byte - CVE-2021-26690: mod_session NULL pointer dereference - CVE-2021-26691: mod_session response handling heap overflow - CVE-2020-35452: A specially crafted Digest nonce can cause a s tack overflow in mod_auth_digest. - CVE-2021-26690: A specially crafted Cookie header handled by mod_session can ca use a NULL pointer dereference and crash, leading to a possible Denial Of Service. - CVE-2021-26691: A specially crafted SessionHeader sent by an origin server could cause a heap overflow.

Solution:

VendorFix Update to version 2.4.48 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.48 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539155 Found on: 2023-10-06 Severity: Critical

PHP Multiple DoS Vulnerabilities (Oct 2016) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-7568,CVE-2016-9137	
Cvss Base:	9.8	
Cvss Score:	9.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple denial of service (DoS) vulnerabilities. - Fixed bug #73003 (Integer Overflow in gdImageWebpCt x of gd_webp.c). - Fixed bug #73147 (Use After Free in PHP7 unserialize()). Successfully exploiting this issue allows a re mote attacker to cause a DoS, or possibly have unspecified other impact.

Solution:

VendorFix Update to version 5.6.27, 7.0.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.27 Installation path / port: 443/tcp

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php,http://seclists.org/oss-sec/2016/q3/639,https://bugs.php.net/bug.php?id=73003,https://bugs.php.net/bug.php?id=73147

Unique Alert ID: 539156 Found on: 2023-10-06 Severity: Critical

PHP Multiple DoS Vulnerabilities (Oct 2016) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-7568,CVE-2016-9137		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple denial of service (DoS) vulnerabilities. - Fixed bug #73003 (Integer Overflow in gdImageWebpCtx of gd_webp.c). - Fixed bug #73147 (Use After Free in PHP7 unserialize()). Successfully exploiting this issue allows a remote attacker to cause a DoS, or possibly have unspecified other impact.

Solution:

VendorFix Update to version 5.6.27, 7.0.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.27 Installation path / port: 80/tcp

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php,http://seclists.org/oss-sec/2016/q3/639,https://bugs.php.net/bug.php?id=73003,https://bugs.php.net/bug.php?id=73147

Unique Alert ID: 539134 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities - 02 - Aug16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-5771,CVE-2016-5770		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - The 'spl_array.c' in the SPL extension improperly interacts with the unserialize implementation and garbage collection. - The integer overflow in the 'SplFileObject::fread' function in 'spl_directory.c' in the SPL extension. Successfully exploiting this issue allow remote attackers to cause a denial of service (use-after-free and application crash) or possibly execute arbitrary code or possibly have unspecified other impact via a large integer argument.

Solution:

VendorFix Update to PHP version 5.5.37, or 5.6.23, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.37

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539179 Found on: 2023-10-06 Severity: Critical

PHP XML Entity Expansion And XML External Entity Vulnerabilities (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-8866
Cvss Base: 9.6
Cvss Score: 9.6
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Description:

PHP is prone to XML entity expansion and XML external entity vulnerabilities. The flaw is due to script 'ext/libxml/libxml.c' does not isolate each thread from 'libxml_disable_entity_loader' when PHP-FPM is used. Successfully exploiting this issue allow remote attackers to conduct XML External Entity (XXE) and XML Entity Expansion (XEE) attacks.

Solution:

VendorFix Update to PHP version 5.5.22, or 5.6.6, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.22

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539178 Found on: 2023-10-06 Severity: Critical

PHP XML Entity Expansion And XML External Entity Vulnerabilities (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-8866
Cvss Base: 9.6
Cvss Score: 9.6
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Description:

PHP is prone to XML entity expansion and XML external entity vulnerabilities. The flaw is due to script 'ext/libxml/libxml.c' does not isolate each thread from 'libxml_disable_entity_loader' when PHP-FPM is used. Successfully exploiting this issue allow remote attackers to conduct XML External Entity (XXE) and XML Entity Expansion (XEE) attacks.

Solution:

VendorFix Update to PHP version 5.5.22, or 5.6.6, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.22

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539195 Found on: 2023-10-06 Severity: Critical

PHP < 7.2.27, 7.3.x < 7.3.14, 7.4.x < 7.4.2 Multiple Vulnerabilities - Jan20 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2020-7059,CVE-2020-7060
Cvss Base: 9.1
Cvss Score: 9.1
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Description:

PHP is prone to multiple vulnerabilities. PHP is prone to multiple vulnerabilities: - OOB read in php_strip_tags_ex (CVE-2020-7059) - Global buffer-overflow in 'mbfl_filt_conv_big5_wchar' (CVE-2020-7060)

Solution:

VendorFix Update to version 7.2.27, 7.3.14, 7.4.2 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.27 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.27,https://www.php.net/ChangeLog-7.php#7.3.14,https://www.php.net/ChangeLog-7.php#7.4.2

Unique Alert ID: 539204 Found on: 2023-10-06 Severity: Critical

PHP Out of Bounds Read Memory Corruption Vulnerability - 01 - Mar16 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-1903
Cvss Base: 9.1
Cvss Score: 9.1
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Description:

PHP is prone to an out-of-bounds read memory corruption vulnerability. The flaw is due to memory corruption vulnerability via a large 'bgd_color' argument to the 'imagerotate' function in 'ext/gd/libgd/gd_interpolation.c' script. Successfully exploiting this issue allow remote attackers to obtain sensitive information or cause a denial-of-service condition.

Solution:

VendorFix Update to PHP version 5.5.31, or 5.6.17 or 7.0.2 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.31

References:

- https://bugs.php.net/bug.php?id=70976,http://www.openwall.com/lists/oss-security/2016/01/14/8

Unique Alert ID: 539203 Found on: 2023-10-06 Severity: Critical

PHP Out of Bounds Read Memory Corruption Vulnerability - 01 - Mar16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-1903
Cvss Base: 9.1
Cvss Score: 9.1

Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Description:

PHP is prone to an out-of-bounds read memory corruption vulnerability. The flaw is due to memory corruption vulnerabilit y via a large 'bgd_color' argument to the 'imagerotate' function in 'ext/gd/libgd/gd_interpolation.c' script. Successfully ex ploiting this issue allow remote attackers to obtain sensitive information or cause a denial-of-service condition.

Solution:

VendorFix Update to PHP version 5.5.31, or 5.6.17 or 7.0.2 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.31

References:

- https://bugs.php.net/bug.php?id=70976,http://www.openwall.com/lists/oss-security/2016/01/14/8

Unique Alert ID: 539202 Found on: 2023-10-06 Severity: Critical

PHP Denial of Service Vulnerability - 02 - Aug16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-5114
Cvss Base: 9.1
Cvss Score: 9.1
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to the 'sapi/fpm/fpm/fpm_log.c' script misinterpret s the semantics of the snprintf return value. Successfully exploiting this issue allow attackers to obtain sensitive informati on from process memory or cause a denial of service (out-of-bounds read and buffer overflow) via a long string.

Solution:

VendorFix Update to PHP version 5.5.31, or 5.6.17, or 7.0.2, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.31

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539193 Found on: 2023-10-06 Severity: Critical

PHP < 7.2.27, 7.3.x < 7.3.14, 7.4.x < 7.4.2 Multiple Vulnerabilities - Jan20 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2020-7059,CVE-2020-7060
Cvss Base: 9.1

Cvss Score: 9.1
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Description:

PHP is prone to multiple vulnerabilities. PHP is prone to multiple vulnerabilities: - OOB read in php_strip_tags_ex (CVE-2020-7059) - Global buffer-overflow in 'mbfl_filt_conv_big5_wchar' (CVE-2020-7060)

Solution:

VendorFix Update to version 7.2.27, 7.3.14, 7.4.2 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.27 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.27,https://www.php.net/ChangeLog-7.php#7.3.14,https://www.php.net/ChangeLog-7.php#7.4.2

Unique Alert ID: 539191 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2017-9788
Cvss Base: 9.1
Cvss Score: 9.1
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The flaw exists due to error in Apache 'mod_auth_digest' which does not properly initialize memory used to process 'Digest' type HTTP Authorization headers. Successful exploitation will allow remote attackers to cause the target service to crash. A remote user can obtain potentially sensitive information as well on the target system.

Solution:

VendorFix Update to Apache HTTP Server 2.2.34 or 2.4.27 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.27 Installation path / port: 80/tcp

References:

- http://www.securitytracker.com/id/1038906,http://httpd.apache.org/security/vulnerabilities_22.html,http://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539205 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server 'mod_auth_digest' Multiple Vulnerabilities (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2017-9788		
Cvss Base:	9.1		
Cvss Score:	9.1		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H		

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The flaw exists due to error in Apache 'mod_auth_digest' which does not properly initialize memory used to process 'Digest' type HTTP Authorization headers. Successful exploitation will allow remote attackers to cause the target service to crash. A remote user can obtain potentially sensitive information as well on the target system.

Solution:

VendorFix Update to Apache HTTP Server 2.2.34 or 2.4.27 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.27 Installation path / port: 443/tcp

References:

- http://www.securitytracker.com/id/1038906,http://httpd.apache.org/security/vulnerabilities_22.html,http://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539200 Found on: 2023-10-06 Severity: Critical

PHP Denial of Service Vulnerability - 02 - Aug16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-5114		
Cvss Base:	9.1		
Cvss Score:	9.1		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H		

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to the 'sapi/fpm/fpm/fpm_log.c' script misinterprets the semantics of the snprintf return value. Successfully exploiting this issue allow attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read and buffer overflow) via a long string.

Solution:

VendorFix Update to PHP version 5.5.31, or 5.6.17, or 7.0.2, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.31

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 1533213 Found on: 2023-10-06 Severity: Critical

PHP < 8.0.30, 8.1.x < 8.1.22, 8.2.x < 8.2.9 Security Update - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2023-10-06
CVE ID: CVE-2023-3823,CVE-2023-3824
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - CVE-2023-3823: Fixed bug GHSA-3qrf-m4j2-pcrr (Security issue with external entity loading in XML without enabling it) - CVE-2023-3824: Fixed bug GHSA-jqcx-ccgc-xwhv (Buffer mismanagement in phar_dir_read())

Solution:

VendorFix Update to version 8.0.30, 8.1.22, 8.2.9 or later.

Result:

Installed version: 5.4.16 Fixed version: 8.0.30 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-8.php#8.1.22,https://www.php.net/ChangeLog-8.php#8.0.30,https://www.php.net/ChangeLog-8.php#8.2.9,https://github.com/php/php-src/security/advisories/GHSA-3qrf-m4j2-pcrr,https://github.com/php/php-src/security/advisories/GHSA-jqcx-ccgc-xwhv

Unique Alert ID: 1533214 Found on: 2023-10-06 Severity: Critical

PHP < 8.0.30, 8.1.x < 8.1.22, 8.2.x < 8.2.9 Security Update - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2023-10-06
CVE ID: CVE-2023-3823,CVE-2023-3824
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - CVE-2023-3823: Fixed bug GHSA-3qrf-m4j2-pcrr (Security issue with external entity loading in XML without enabling it) - CVE-2023-3824: Fixed bug GHSA-jqcx-ccgc-xwhv (Buffer mismanagement in phar_dir_read())

Solution:

VendorFix Update to version 8.0.30, 8.1.22, 8.2.9 or later.

Result:

Installed version: 5.4.16 Fixed version: 8.0.30 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-8.php#8.1.22,https://www.php.net/ChangeLog-8.php#8.0.30,https://www.php.net/ChangeLog-8.php#8.2.9,https://github.com/php/php-src/security/advisories/GHSA-3qrf-m4j2-pcrr,https://github.com/php/php-src/security/advisories/GHSA-jqcx-ccgc-xwhv

Unique Alert ID: 539309 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities (Jun/Aug 2014) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-3981,CVE-2014-4721,CVE-2014-0207,CVE-2014-3478,CVE-2014-3479,CVE-2014-3480,CVE-2014-3487,CVE-2014-4049,CVE-2014-3515,CVE-2014-9912		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. The following vulnerabilities exist: - Fixed bug #67390 (insecure temporary file use in the configure script). (CVE-2014-3981). - Fixed bug #67498 (phpinfo() Type Confusion Information Leak Vulnerability). (CVE-2014-4721). - Fixed bug #67326 (cdf_read_short_sector insufficient boundary check). (CVE-2014-0207). - Fixed bug #67410 (mconvert incorrect handling of truncated pascal string size). (CVE-2014-3478). - Fixed bug #67411 (cdf_check_stream_offset insufficient boundary check). (CVE-2014-3479). - Fixed bug #67412 (cdf_count_chain insufficient boundary check). (CVE-2014-3480). - Fixed bug #67413 (cdf_read_property_info insufficient boundary check). (CVE-2014-3487). - Fixed bug #67432 (Fix potential segfault in dns_get_record()). (CVE-2014-4049). - Fixed bug #67492 (unserialize() SPL ArrayObject / SPLObjectStorage Type Confusion). (CVE-2014-3515). - Fixed bug #67397 (Buffer overflow in locale_get_display_name and uloc_getDisplayName (libicu 4.8.1)). (CVE-2014-9912).

Solution:

VendorFix Update to version 5.3.29, 5.4.30, 5.5.14 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.30 Installation path / port: 80/tcp

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=67390,https://bugs.php.net/bug.php?id=67498,https://bugs.php.net/bug.php?id=67326,https://bugs.php.net/bug.php?id=67410,https://bugs.php.net/bug.php?id=67411,https://bugs.php.net/bug.php?id=67412,https://bugs.php.net/bug.php?id=67413,https://bugs.php.net/bug.php?id=67432,https://bugs.php.net/bug.php?id=67492,http://seclists.org/fulldisclosure/2014/Jun/21,https://www.sektioneins.de/en/blog/14-07-04-phpinfo-infoleak.html,http://secunia.com/advisories/59575

Unique Alert ID: 539308 Found on: 2023-10-06 Severity: Critical

PHP Multiple Vulnerabilities (Jun/Aug 2014) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-3981,CVE-2014-4721,CVE-2014-0207,CVE-2014-3478,CVE-2014-3479,CVE-2014-3480,CVE-2014-3487,CVE-2014-4049,CVE-2014-3515,CVE-2014-9912		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. The following vulnerabilities exist: - Fixed bug #67390 (insecure temporary file use in the configure script). (CVE-2014-3981). - Fixed bug #67498 (phpinfo() Type Confusion Information Leak Vulnerability). (CVE-2014-4721). - Fixed bug #67326 (cdf_read_short_sector insufficient boundary check). (CVE-2014-0207). - Fixed bug #67410 (mconvert incorrect handling of truncated pascal string size). (CVE-2014-3478). - Fixed bug #67411 (cdf_check_stream_offset insufficient boundary check). (CVE-2014-3479). - Fixed bug #67412 (cdf_count_chain insufficient boundary check). (CVE-2014-3480). - Fixed bug #67413 (cdf_read_property_info insufficient boundary check). (CVE-2014-3487). - Fixed bug #67432 (Fix potential segfault in dns_get_record()). (CVE-2014-4049). - Fixed bug #67492 (unserialize() SPL ArrayObject / SPLObjectStorage Type Confusion). (CVE-2014-3515). - Fixed bug #67397 (Buffer overflow in locale_get_display_name and uloc_getDisplayName (libicu 4.8.1)). (CVE-2014-9912).

Solution:

VendorFix Update to version 5.3.29, 5.4.30, 5.5.14 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.30 Installation path / port: 443/tcp

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=67390,https://bugs.php.net/bug.php?id=67498,https://bugs.php.net/bug.php?id=67326,https://bugs.php.net/bug.php?id=67410,https://bugs.php.net/bug.php?id=67411,https://bugs.php.net/bug.php?id=67412,https://bugs.php.net/bug.php?id=67413,https://bugs.php.net/bug.php?id=67432,https://bugs.php.net/bug.php?id=67492,http://seclists.org/fulldisclosure/2014/Jun/21,https://www.sektioneins.de/en/blog/14-07-04-phpinfo-infoleak.html,http://secunia.com/advisories/59575

Unique Alert ID: 1533217 Found on: 2023-10-06 Severity: Critical

OpenBSD OpenSSH < 9.3p2 RCE Vulnerability (tcp/22)

Open Status:	Re-OPEN	**First Found:**	2023-10-06
CVE ID:	CVE-2023-38408		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

OpenBSD OpenSSH is prone to a remote code execution (RCE) vulnerability in OpenSSH's forwarded ssh-agent. A condition where specific libraries loaded via ssh-agent(1)'s PKCS#11 support could be abused to achieve remote code execution via a forwarded agent socket.

Solution:

VendorFix Update to version 9.3p2 or later.

Result:

Installed version: 6.6.1 Fixed version: 9.3p2 Installation path / port: 22/tcp

References:

- https://www.openssh.com/releasenotes.html#9.3p2,https://www.qualys.com/2023/07/19/cve-2023-38408/rce-openssh-forwarded-ssh-agent.txt

Unique Alert ID: 1533222 Found on: 2023-10-06 Severity: Critical

PHP < 7.4.33, 8.0.x < 8.0.25, 8.1.x < 8.1.12 Security Update - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2023-10-06
CVE ID:	CVE-2022-31630,CVE-2022-37454		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2022-31630: OOB read due to insufficient input validation in imageloadfont() - CVE-2022-37454: Buffer overflow in hash_update() on long parameter

Solution:

VendorFix Update to version 7.4.33, 8.0.25, 8.1.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.4.33 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.4.33,https://www.php.net/ChangeLog-8.php#8.0.25,https://www.php.net/

ChangeLog-8.php#8.1.12

Unique Alert ID: 1533223 Found on: 2023-10-06 Severity: Critical

PHP < 7.4.33, 8.0.x < 8.0.25, 8.1.x < 8.1.12 Security Update - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2023-10-06
CVE ID: CVE-2022-31630,CVE-2022-37454
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

PHP is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2022-31630: OOB read due to insufficien t input validation in imageloadfont() - CVE-2022-37454: Buffer overflow in hash_update() on long parameter

Solution:

VendorFix Update to version 7.4.33, 8.0.25, 8.1.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.4.33 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.4.33,https://www.php.net/ChangeLog-8.php#8.0.25,https://www.php.net/ChangeLog-8.php#8.1.12

Unique Alert ID: 1533228 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server 2.4.0 - 2.4.55 HTTP Request Smuggling Vulnerability (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2023-10-06
CVE ID: CVE-2023-25690
Cvss Base: 9.8
Cvss Score: 9.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

Apache HTTP Server is prone to a HTTP request smuggling vulnerability. Some mod_proxy configurations allow a HTTP R equest Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule o r ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data an d is then re-inserted into the proxied request-target using variable substitution. Request splitting/smuggling could result i n bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisonin g.

Solution:

VendorFix Update to version 2.4.56 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.56 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 1533229 Found on: 2023-10-06 Severity: Critical

Apache HTTP Server 2.4.0 - 2.4.55 HTTP Request Smuggling Vulnerability (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2023-10-06
CVE ID:	CVE-2023-25690		
Cvss Base:	9.8		
Cvss Score:	9.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

Apache HTTP Server is prone to a HTTP request smuggling vulnerability. Some mod_proxy configurations allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning.

Solution:

VendorFix Update to version 2.4.56 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.56 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539088 Found on: 2023-10-06 Severity: High

PHP Directory Traversal Vulnerability - Jul16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-9767,CVE-2015-6834,CVE-2015-6835,CVE-2015-6837,CVE-2015-6838		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to a directory traversal vulnerability. Multiple flaws are due to - An error in the 'ZipArchive::extractTo' function in 'ext/zip/php_zip.c' script. - The xsl_ext_function_php function in ext/xsl/xsltprocessor.c when libxml2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation after the principal argument loop. - Improper handling of multiple php_var_unserialize calls. - Multiple use-after-free vulnerabilities. Successfully exploiting this issue allow remote attackers to read arbitrary empty directories, also to cause a denial of service.

Solution:

VendorFix Update to PHP version 5.4.45, or 5.5.29, or 5.6.13, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.45

References:

- http://www.php.net/ChangeLog-5.php,http://www.openwall.com/lists/oss-security/2016/03/16/20

Unique Alert ID: 539090 Found on: 2023-10-06 Severity: High

PHP Directory Traversal Vulnerability - Jul16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-9767,CVE-2015-6834,CVE-2015-6835,CVE-2015-6837,CVE-2015-6838		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to a directory traversal vulnerability. Multiple flaws are due to - An error in the 'ZipArchive::extractTo' functi on in 'ext/zip/php_zip.c' script. - The xsl_ext_function_php function in ext/xsl/xsltprocessor.c when libxml2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation after the principal ar gument loop. - Improper handling of multiple php_var_unserialize calls. - Multiple use-after-free vulnerabilities. Successf ully exploiting this issue allow remote attackers to read arbitrary empty directories, also to cause a denial of service.

Solution:

VendorFix Update to PHP version 5.4.45, or 5.5.29, or 5.6.13, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.45

References:

- http://www.php.net/ChangeLog-5.php,http://www.openwall.com/lists/oss-security/2016/03/16/20

Unique Alert ID: 539122 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 03 - Sep16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-7412,CVE-2016-7413,CVE-2016-7414,CVE-2016-7416,CVE-2016-7417,CVE-2016-7418		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Use-after-free vulnerability in the 'wddx_stack_destro y' function in 'ext/wddx/wddx.c' script. - Improper verification of a BIT field has the UNSIGNED_FLAG flag in 'ext/mysqlnd /mysqlnd_wireprotocol.c' script. - The ZIP signature-verification feature does not ensure that the uncompressed_filesize f ield is large enough. - The script 'ext/spl/spl_array.c' proceeds with SplArray unserialization without validating a return v alue and data type. - The script 'ext/intl/msgformat/msgformat_format.c' does not properly restrict the locale length prov ided to the Locale class in the ICU library. - An error in the php_wddx_push_element function in ext/wddx/wddx.c. Succe ssfully exploiting this issue allow remote attackers to cause a denial of service, or possibly have unspecified other impact .

Solution:

VendorFix Update to PHP version 5.6.25, or 7.0.10, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.26

References:

- http://www.php.net/ChangeLog-7.php,http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539123 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 03 - Sep16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-7412,CVE-2016-7413,CVE-2016-7414,CVE-2016-7416,CVE-2016-7417,CVE-2016-7418		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Use-after-free vulnerability in the 'wddx_stack_destroy' function in 'ext/wddx/wddx.c' script. - Improper verification of a BIT field has the UNSIGNED_FLAG flag in 'ext/mysqlnd/mysqlnd_wireprotocol.c' script. - The ZIP signature-verification feature does not ensure that the uncompressed_filesize field is large enough. - The script 'ext/spl/spl_array.c' proceeds with SplArray unserialization without validating a return value and data type. - The script 'ext/intl/msgformat/msgformat_format.c' does not properly restrict the locale length provided to the Locale class in the ICU library. - An error in the php_wddx_push_element function in ext/wddx/wddx.c. Successfully exploiting this issue allow remote attackers to cause a denial of service, or possibly have unspecified other impact .

Solution:

VendorFix Update to PHP version 5.6.25, or 7.0.10, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.26

References:

- http://www.php.net/ChangeLog-7.php,http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539126 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 02 - Sep16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-7124,CVE-2016-7125,CVE-2016-7126,CVE-2016-7127,CVE-2016-7128,CVE-2016-7129,CVE-2016-7130,CVE-2016-7131,CVE-2016-7132		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to - An invalid wddxPacket XML document that is mishandled in a wddx_deserialize call in 'ext/wddx/wddx.c' script. - An error in 'php_wddx_pop_element' function in 'ext/wddx/wddx.c' script. - An error in 'php_wddx_process_data' function in 'ext/wddx/wddx.c' script. - Improper handling of the case of a thumbnail offset that exceeds the file size in 'exif_process_IFD_in_TIFF' function in 'ext/exif/exif.c' script. - Improper validation of gamma values in 'imagegammacorrect' function in 'ext/gd/gd.c' script. - Improper validation of number of colors in 'imagegammacorrect' function in 'ext/gd/gd.c' script. - The script 'ext/session/session.c' skips invalid session names in a way that triggers incorrect parsing. - Improper handling of certain objects in 'ext/standard/var_unserializer.c' script. Successfully exploiting this issue allow remote attackers to cause a denial of service, to obtain sensitive information from process memory, to inject arbitrary-type session data by leveraging control of a session name.

Solution:

VendorFix Update to PHP version 5.6.25, or 7.0.10, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.25

References:

- http://www.php.net/ChangeLog-7.php,http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539129 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 02 - Sep16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-7124,CVE-2016-7125,CVE-2016-7126,CVE-2016-7127,CVE-2016-7128,CVE-2016-7129,CVE-2016-7130,CVE-2016-7131,CVE-2016-7132		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to - An invalid wddxPacket XML document that is mishandle d in a wddx_deserialize call in 'ext/wddx/wddx.c' script. - An error in 'php_wddx_pop_element' function in 'ext/wddx/wdd x.c' script. - An error in 'php_wddx_process_data' function in 'ext/wddx/wddx.c' script. - Improper handling of the case of a thumbnail offset that exceeds the file size in 'exif_process_IFD_in_TIFF' function in 'ext/exif/exif.c' script. - Improper va lidation of gamma values in 'imagegammacorrect' function in 'ext/gd/gd.c' script. - Improper validation of number of colo rs in 'imagegammacorrect' function in 'ext/gd/gd.c' script. - The script 'ext/session/session.c' skips invalid session names in a way that triggers incorrect parsing. - Improper handling of certain objects in 'ext/standard/var_unserializer.c' script. Successfully exploiting this issue allow remote attackers to cause a denial of service, to obtain sensitive information from process memory, to inject arbitrary-type session data by leveraging control of a session name.

Solution:

VendorFix Update to PHP version 5.6.25, or 7.0.10, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.25

References:

- http://www.php.net/ChangeLog-7.php,http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539137 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Jul16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-4070,CVE-2016-4071,CVE-2016-4072,CVE-2016-4073,CVE-2015-8865		
Cvss Base:	7.3		
Cvss Score:	7.3		
Cvss Vector:	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Multiple integer overflows in the mbfl_strcut function in 'ext/mbstring/libmbfl/mbfl/mbfilter.c' script. - A format string vulnerability in the php_snmp_error function in 'ext/snmp/s nmp.c' script. - An improper handling of '\0' characters by the 'phar_analyze_path' function in 'ext/phar/phar.c' script. - A n integer overflow in the 'php_raw_url_encode' function in 'ext/standard/url.c' script. - An improper handling of continuati on-level jumps in 'file_check_mem' function in 'funcs.c' script. Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code.

Solution:

VendorFix Update to PHP version 5.5.34, or 5.6.20, or 7.0.5, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.34

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539140 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Jul16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-4070,CVE-2016-4071,CVE-2016-4072,CVE-2016-4073,CVE-2015-8865	
Cvss Base:	7.3	
Cvss Score:	7.3	
Cvss Vector:	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Multiple integer overflows in the mbfl_strcut function in 'ext/mbstring/libmbfl/mbfl/mbfilter.c' script. - A format string vulnerability in the php_snmp_error function in 'ext/snmp/snmp.c' script. - An improper handling of '\0' characters by the 'phar_analyze_path' function in 'ext/phar/phar.c' script. - An integer overflow in the 'php_raw_url_encode' function in 'ext/standard/url.c' script. - An improper handling of continuation-level jumps in 'file_check_mem' function in 'funcs.c' script. Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code.

Solution:

VendorFix Update to PHP version 5.5.34, or 5.6.20, or 7.0.5, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.34

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539145 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Aug16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-5773,CVE-2016-5772,CVE-2016-5769,CVE-2016-5768,CVE-2016-5766,CVE-2016-5767	
Cvss Base:	8.8	
Cvss Score:	8.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - The 'php_zip.c' script in the zip extension improperly interacts with the unserialize implementation and garbage collection. - The php_wddx_process_data function in 'wddx.c' script in the WDDX extension mishandled data in a wddx_deserialize call. - The multiple integer overflows in 'mcrypt.c' script in the mcrypt extension. - The double free vulnerability in the '_php_mb_regex_ereg_replace_exec' function in 'php_mbregex.c' script in the mbstring extension. - An integer overflow in the '_gd2GetHeader' function in 'gd_gd2.c' script in the GD Graphics Library. - An integer overflow in the 'gdImageCreate' function in 'gd.c' script in the GD Graphics Library. Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code.

Solution:

VendorFix Update to PHP version 5.5.37, or 5.6.23, or 7.0.8, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.37

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539148 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Aug16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-5773,CVE-2016-5772,CVE-2016-5769,CVE-2016-5768,CVE-2016-5766,CVE-2016-5767	
Cvss Base:	8.8	
Cvss Score:	8.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - The 'php_zip.c' script in the zip extension improperly i nteracts with the unserialize implementation and garbage collection. - The php_wddx_process_data function in 'wddx.c' sc ript in the WDDX extension mishandled data in a wddx_deserialize call. - The multiple integer overflows in 'mcrypt.c' scri pt in the mcrypt extension. - The double free vulnerability in the '_php_mb_regex_ereg_replace_exec' function in 'php_m bregex.c' script in the mbstring extension. - An integer overflow in the '_gd2GetHeader' function in 'gd_gd2.c' script in the GD Graphics Library. - An integer overflow in the 'gdImageCreate' function in 'gd.c' script in the GD Graphics Library. Su ccessfully exploiting this issue allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code.

Solution:

VendorFix Update to PHP version 5.5.37, or 5.6.23, or 7.0.8, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.37

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539239 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities (Nov 2016) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-8670,CVE-2016-9933,CVE-2016-9934,CVE-2016-10397	
Cvss Base:	7.5	
Cvss Score:	7.5	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N	

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - CVE-2016-8670: Stack Buffer Overflow in GD dynamic Getbuf - CVE-2016-9933, CVE-2016-9934: Multiple denial of service (DoS) vulnerabilities - CVE-2016-10397: Security by pass vulnerability

Solution:

VendorFix Update to version 5.6.28, 7.0.13 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.28 Installation path / port: 443/tcp

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php,http://bugs.php.net/73280,http://bugs.php.net/72696,http://bugs.php.net/73331,http://bugs.php.net/73192

Unique Alert ID: 539240 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities (Nov 2016) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-8670,CVE-2016-9933,CVE-2016-9934,CVE-2016-10397	
Cvss Base:	7.5	
Cvss Score:	7.5	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N	

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - CVE-2016-8670: Stack Buffer Overflow in GD dynamic Getbuf - CVE-2016-9933, CVE-2016-9934: Multiple denial of service (DoS) vulnerabilities - CVE-2016-10397: Security by pass vulnerability

Solution:

VendorFix Update to version 5.6.28, 7.0.13 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.28 Installation path / port: 80/tcp

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php,http://bugs.php.net/73280,http://bugs.php.net/72696,http://bugs.php.net/73331,http://bugs.php.net/73192

Unique Alert ID: 539114 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities (Jul 2016 - 05) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-6288,CVE-2016-6289,CVE-2016-6290,CVE-2016-6291,CVE-2016-6292,CVE-2016-6294,CVE-2016-6295,CVE-2016-6296,CVE-2016-6297,CVE-2016-6207,CVE-2016-5399	
Cvss Base:	7.8	
Cvss Score:	7.8	
Cvss Vector:	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws exist due to - An integer overflow in the 'php_stream_zip_opener' function in 'ext/zip/zip_stream.c' - An integer signedness error in the 'simplestring_addn' function in 'simplestring.c' in xmlrpc-epi - 'ext/snmp/snmp.c' improperly interacts with the unserialize implementation and garbage collection - The 'locale_accept_from_http' function in 'ext/intl/locale/locale_methods.c' does not properly restrict calls to the ICU 'uloc_acceptLanguageFromHTTP' function - An error in the 'exif_process_user_comment' function of 'ext/exif/exif.c' - An error in the 'exif_process_IFD_in_MAKERNOTE' function of 'ext/exif/exif.c' - 'ext/session/session.c' does not properly maintain a certain hash data structure - An integer overflow in the 'virtual_file_ex' function of 'TSRM/tsrm_virtual_cwd.c' - An error in the 'php_url_parse_ex' function of 'ext/standard/url.c' - Integer overflow error within _gdContributionsAlloc() - Inadequate error handling in bzread() Successfully exploiting these issues may allow attackers to cause a denial of service obtain sensitive information from process memory, or possibly have unspecified other impact.

Solution:

VendorFix Update to version 5.5.38, 5.6.24, 7.0.9, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.38 Installation path / port: 443/tcp

References:

- http://php.net/ChangeLog-5.php,http://php.net/ChangeLog-7.php,http://openwall.com/lists/oss-security/2016/07/24/2

Unique Alert ID: 539115 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities (Jul 2016 - 05) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-6288,CVE-2016-6289,CVE-2016-6290,CVE-2016-6291,CVE-2016-6292,CVE-2016-6294,CVE-2016-6295,CVE-2016-6296,CVE-2016-6297,CVE-2016-6207,CVE-2016-5399		
Cvss Base:	7.8		
Cvss Score:	7.8		
Cvss Vector:	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws exist due to - An integer overflow in the 'php_stream_zip_opener' function in 'ext/zip/zip_stream.c' - An integer signedness error in the 'simplestring_addn' function in 'simplestring.c' in xmlrpc-epi - 'ext/snmp/snmp.c' improperly interacts with the unserialize implementation and garbage collection - The 'locale_accept_from_http' function in 'ext/intl/locale/locale_methods.c' does not properly restrict calls to the ICU 'uloc_acceptLanguageFromHTTP' function - An error in the 'exif_process_user_comment' function of 'ext/exif/exif.c' - An error in the 'exif_process_IFD_in_MAKERNOTE' function of 'ext/exif/exif.c' - 'ext/session/session.c' does not properly maintain a certain hash data structure - An integer overflow in the 'virtual_file_ex' function of 'TSRM/tsrm_virtual_cwd.c' - An error in the 'php_url_parse_ex' function of 'ext/standard/url.c' - Integer overflow error within _gdContributionsAlloc() - Inadequate error handling in bzread() Successfully exploiting these issues may allow attackers to cause a denial of service obtain sensitive information from process memory, or possibly have unspecified other impact.

Solution:

VendorFix Update to version 5.5.38, 5.6.24, 7.0.9, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.38 Installation path / port: 80/tcp

References:

- http://php.net/ChangeLog-5.php,http://php.net/ChangeLog-7.php,http://openwall.com/lists/oss-security/2016/07/24/2

Unique Alert ID: 539279 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities (Jan 2017 - 02) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-10161,CVE-2016-10158,CVE-2016-10168,CVE-2016-10167,CVE-2017-11147,CVE-2016-10160,CVE-2016-10159		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - Fixed bug #73825 (Heap out of bounds read on unserialize in finish_nested_data()). (CVE-2016-10161) - Fixed bug #73737 (FPE when parsing a tag format). (CVE-2016-10158) - Fixed bug #73869 (Signed Integer Overflow gd_io.c). (CVE-2016-10168) - Fixed bug #73868 (DOS vulnerability in gdImageCreateFromGd2Ctx()). (CVE-2016-10167) - Fixed bug #73773 (Seg fault when loading hostile phar). (CVE-2017-11147) - Fixed bug #73768 (Memory corruption when loading hostile phar). (CVE-2016-10160) - Fixed bug #73764 (Crash while loading hostile phar archive). (CVE-2016-10159)

Solution:

VendorFix Update to version 5.6.30, 7.0.15, 7.1.1 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.30 Installation path / port: 443/tcp

References:

- http://bugs.php.net/73737,http://bugs.php.net/73869,http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php,http://bugs.php.net/73825,http://bugs.php.net/73868,http://bugs.php.net/73773,http://bugs.php.net/73768,http://bugs.php.net/73764

Unique Alert ID: 539280 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities (Jan 2017 - 02) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-10161,CVE-2016-10158,CVE-2016-10168,CVE-2016-10167,CVE-2017-11147,CVE-2016-10160,CVE-2016-10159	
Cvss Base:	7.5	
Cvss Score:	7.5	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - Fixed bug #73825 (Heap out of bounds read on unserialize in finish_nested_data()). (CVE-2016-10161) - Fixed bug #73737 (FPE when parsing a tag format). (CVE-2016-10158) - Fixed bug #73869 (Signed Integer Overflow gd_io.c). (CVE-2016-10168) - Fixed bug #73868 (DOS vulnerability in gdImageCreateFromGd2Ctx()). (CVE-2016-10167) - Fixed bug #73773 (Seg fault when loading hostile phar). (CVE-2017-11147) - Fixed bug #73768 (Memory corruption when loading hostile phar). (CVE-2016-10160) - Fixed bug #73764 (Crash while loading hostile phar archive). (CVE-2016-10159)

Solution:

VendorFix Update to version 5.6.30, 7.0.15, 7.1.1 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.30 Installation path / port: 80/tcp

References:

- http://bugs.php.net/73737,http://bugs.php.net/73869,http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php,http://bugs.php.net/73825,http://bugs.php.net/73868,http://bugs.php.net/73773,http://bugs.php.net/73768,http://bugs.php.net/73764

Unique Alert ID: 539112 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities (Feb 2019) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-10166,CVE-2019-9020,CVE-2019-9021,CVE-2019-9023,CVE-2019-9024,CVE-2019-6977	
Cvss Base:	8.8	
Cvss Score:	8.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - Fixed bug #77269 (efree() on uninitialized Heap data in imagescale leads to use-after-free). (CVE-2016-10166) - Fixed bug #77270 (imagecolormatch Out Of Bounds Write on Heap). (CVE-2019-6977) - Fixed bug #77370 (Buffer overflow on mb regex functions - fetch_token). (CVE-2019-9023) - Fixed bug #77371 (heap buffer overflow in mb regex functions - compile_string_node). (CVE-2019-9023) - Fixed bug #77381 (heap buffer overflow in multibyte match_at). (CVE-2019-9023) - Fixed bug #77382 (heap buffer overflow due to incorrect length in expand_case_fold_string). (CVE-2019-9023) - Fixed bug #77385 (buffer overflow in fetch_token). (CVE-2019-9023) - Fixed bug #77394 (Buffer overflow in multibyte case folding - unicode). (CVE-2019-9023) - Fixed bug #77418 (Heap overflow in utf32be_mbc_to_code). (CVE-2019-9023) - Fixed bug #77247 (heap buffer overflow in phar_detect_phar_fname_ext). (CVE-2019-9021) - Fixed bug #77242 (heap out of bounds read in xmlrpc_decode()). (CVE-2019-9020) - Fixed bug #77380 (Global out of bounds read in xmlrpc base64 code). (CVE-2019-9024)

Solution:

VendorFix Update to version 5.6.40, 7.1.16, 7.2.14, 7.3.1 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.40 Installation path / port: 443/tcp

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php,https://bugs.php.net/bug.php?id=77269,https://bugs.php.net/bug.php?id=77270,https://bugs.php.net/bug.php?id=77370,https://bugs.php.net/bug.php?id=77371,https://bugs.php.net/bug.php?id=77381,https://bugs.php.net/bug.php?id=77382,https://bugs.php.net/bug.php?id=77385,https://bugs.php.net/bug.php?id=77394,https://bugs.php.net/bug.php?id=77418,https://bugs.php.net/bug.php?id=77247,https://bugs.php.net/bug.php?id=77242,https://bugs.php.net/bug.php?id=77380

Unique Alert ID: 539113 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities (Feb 2019) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-10166,CVE-2019-9020,CVE-2019-9021,CVE-2019-9023,CVE-2019-9024,CVE-2019-6977	
Cvss Base:	8.8	
Cvss Score:	8.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - Fixed bug #77269 (efree() on uninitialized Heap data in imagescale leads to use-after-free). (CVE-2016-10166) - Fixed bug #77270 (imagecolormatch Out Of Bounds Write on Heap). (CVE-2019-6977) - Fixed bug #77370 (Buffer overflow on mb regex functions - fetch_token). (CVE-2019-9023) - Fixed bug #77371 (heap buffer overflow in mb regex functions - compile_string_node). (CVE-2019-9023) - Fixed bug #77381 (heap buffer overflow in multibyte match_at). (CVE-2019-9023) - Fixed bug #77382 (heap buffer overflow due to incorrect length in expand_case_fold_string). (CVE-2019-9023) - Fixed bug #77385 (buffer overflow in fetch_token). (CVE-2019-9023) - Fixed bug #77394 (Buffer overflow in multibyte case folding - unicode). (CVE-2019-9023) - Fixed bug #77418 (Heap overflow in utf32be_mbc_to_code). (CVE-2019-9023) - Fixed bug #77247 (heap buffer overflow in phar_detect_phar_fname_ext). (CVE-2019-9021) - Fixed bug #77242 (heap out of bounds read in xmlrpc_decode()). (CVE-2019-9020) - Fixed bug #77380 (Global out of bounds read in xmlrpc base64 code). (CVE-2019-9024)

Solution:

VendorFix Update to version 5.6.40, 7.1.16, 7.2.14, 7.3.1 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.40 Installation path / port: 80/tcp

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php,https://bugs.php.net/bug.php?id=77269,https://bugs.php.net/bug.php?id=77270,https://bugs.php.net/bug.php?id=77370,https://bugs.php.net/bug.php?id=77371,https://bugs.php.net/bug.php?id=77381,https://bugs.php.net/bug.php?id=77382,https://bugs.php.net/bug.php?id=77385,https://bugs.php.net/bug.php?id=77394,https://bugs.php.net/bug.php?id=77418,https://bugs.php.net/bug.php?id=77247,https://bugs.php.net/bug.php?id=77242,https://bugs.php.net/bug.php?id=77380

Unique Alert ID: 539172 Found on: 2023-10-06 Severity: High

PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-4343	
Cvss Base:	8.8	
Cvss Score:	8.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	

Description:

PHP is prone to denial of service and unspecified vulnerabilities. The flaw is due an improper handling of zero-size './/@LongLink' files by 'phar_make_dirstream' function in ext/phar/dirstream.c script. Successfully exploiting this issue allow remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.6.18, or 7.0.3, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.18

References:

- http://www.php.net/ChangeLog-5.php,http://www.openwall.com/lists/oss-security/2016/04/28/2

Unique Alert ID: 539189 Found on: 2023-10-06 Severity: High

PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-4343
Cvss Base: 8.8
Cvss Score: 8.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Description:

PHP is prone to denial of service and unspecified vulnerabilities. The flaw is due an improper handling of zero-size './/@LongLink' files by 'phar_make_dirstream' function in ext/phar/dirstream.c script. Successfully exploiting this issue allow remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.6.18, or 7.0.3, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.18

References:

- http://www.php.net/ChangeLog-5.php,http://www.openwall.com/lists/oss-security/2016/04/28/2

Unique Alert ID: 539125 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 03 - Aug16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-5096,CVE-2016-5094,CVE-2016-5095
Cvss Base: 8.6
Cvss Score: 8.6
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - An integer overflow in the fread function in 'ext/standard/file.c' script. - An integer overflow in the php_html_entities function in 'ext/standard/html.c' script. - An Integer overflow in the php_escape_html_entities_ex function in 'ext/standard/html.c' script. Successfully exploiting this issue allow remote attackers to cause a denial of service or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.5.36, or 5.6.22, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.36

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539128 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 03 - Aug16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-5096,CVE-2016-5094,CVE-2016-5095		
Cvss Base:	8.6		
Cvss Score:	8.6		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - An integer overflow in the fread function in 'ext/standard/file.c' script. - An integer overflow in the php_html_entities function in 'ext/standard/html.c' script. - An Integer overflow in the php_escape_html_entities_ex function in 'ext/standard/html.c' script. Successfully exploiting this issue allow remote attackers to cause a denial of service or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.5.36, or 5.6.22, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.36

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539120 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 04 - Aug16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2013-7456,CVE-2016-5093		
Cvss Base:	8.6		
Cvss Score:	8.6		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - The 'get_icu_value_internal' function in 'ext/intl/locale/locale_methods.c' script does not ensure the presence of a '\0' character. - The 'gd_interpolation.c' script in the GD Graphics Library mishandled by the imagescale function. Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.5.36, or 5.6.22, or 7.0.7, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.36

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539121 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 04 - Aug16 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2013-7456,CVE-2016-5093
Cvss Base: 8.6
Cvss Score: 8.6
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - The 'get_icu_value_internal' function in 'ext/intl/locale/locale_methods.c' script does not ensure the presence of a '\0' character. - The 'gd_interpolation.c' script in the GD Graphics Library mishandled by the imagescale function. Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.5.36, or 5.6.22, or 7.0.7, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.36

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539077 Found on: 2023-10-06 Severity: High

OpenSSH Multiple Vulnerabilities (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-6564,CVE-2015-6563,CVE-2015-5600
Cvss Base: 8.5
Cvss Score: 8.5

Description:

OpenSSH is prone to multiple vulnerabilities. Multiple flaws are due to: - Use-after-free vulnerability in the 'mm_answer_pam_free_ctx' function in monitor.c in sshd. - Vulnerability in 'kbdint_next_device' function in auth2-chall.c in sshd. - Vulnerability in the handler for the MONITOR_REQ_PAM_FREE_CTX request. Successful exploitation will allow an attacker to gain privileges, to conduct impersonation attacks, to conduct brute-force attacks or cause a denial of service.

Solution:

VendorFix Upgrade to OpenSSH 7.0 or later.

Result:

Installed version: 6.6.1 Fixed version: 7.0 Installation path / port: 22/tcp

References:

- http://seclists.org/fulldisclosure/2015/Aug/54,http://openwall.com/lists/oss-security/2015/07/23/4

Unique Alert ID: 539284 Found on: 2023-10-06 Severity: High

OpenSSH Client Information Leak (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18

CVE ID: CVE-2016-0777,CVE-2016-0778
Cvss Base: 8.1
Cvss Score: 8.1
Cvss Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

The OpenSSH client code between 5.4 and 7.1p1 contains experimental support for resuming SSH-connections (roaming) . The matching server code has never been shipped, but the client code was enabled by default and could be tricked by a malicious server into leaking client memory to the server, including private client user keys. The authentication of the ser ver host key prevents exploitation by a man-in-the-middle, so this information leak is restricted to connections to malicio us or compromised servers.

Solution:

VendorFix Update to 7.1p2 or newer.

Result:

Installed version: 6.6.1 Fixed version: 7.1p2 Installation path / port: 22/tcp

References:

- http://www.openssh.com/txt/release-7.1p2

Unique Alert ID: 539221 Found on: 2023-10-06 Severity: High

PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-5385,CVE-2016-6128
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a man-in-the-middle attack vulnerability. The following flaws exist: - The web servers running in a CGI or CGI-like context may assign client request proxy header values to internal HTTP_PROXY environment variables. - 'HTTP_ PROXY' is improperly trusted by some PHP libraries and applications - An unspecified flaw in the gdImageCropThreshold f unction in 'gd_crop.c' in the GD Graphics Library. Successfully exploiting this issue may allow remote, unauthenticated to conduct MITM attacks on internal server subrequests or direct the server to initiate connections to arbitrary hosts or to ca use a denial of service.

Solution:

VendorFix Update to PHP version 5.6.24 or 7.0.19.

Result:

Installed version: 5.4.16 Fixed version: 5.6.24/7.0.9

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php,http://www.kb.cert.org/vuls/id/797896, https://bugs.php.net/bug.php?id=72573,https://bugs.php.net/bug.php?id=72494

Unique Alert ID: 539222 Found on: 2023-10-06 Severity: High

Apache HTTP Server Man-in-the-Middle Attack Vulnerability - July16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-5387
Cvss Base: 8.1
Cvss Score: 8.1
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

Apache HTTP Server is prone to a man-in-the-middle attack vulnerability. The flaw is due to 'CGI Servlet' does not protec t applications from the presence of untrusted client data in the 'HTTP_PROXY' environment variable. Successful exploitati on will allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted proxy header in an HTTP request.

Solution:

VendorFix Update to version 2.4.24, or 2.2.32, or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.24 Installation path / port: 443/tcp

References:

- https://www.apache.org/security/asf-httpoxy-response.txt

Unique Alert ID: 1010815 Found on: 2023-10-06 Severity: High

PHP < 7.4.30, 8.0.x < 8.0.20, 8.1.x < 8.1.7 Security Update (Jun 2022) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-08-27
CVE ID: CVE-2022-31625,CVE-2022-31626
Cvss Base: 8.8
Cvss Score: 8.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Description:

PHP released new versions which include a security fix. The following vulnerabilities exist: - CVE-2022-31625: Uninitialize d array in pg_query_params() - CVE-2022-31626: mysqlnd/pdo password buffer overflow

Solution:

VendorFix Update to version 7.4.30, 8.0.20, 8.1.7 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.4.30 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.4.30,https://www.php.net/ChangeLog-8.php#8.0.20,https://www.php.net/ChangeLog-8.php#8.1.7,https://bugs.php.net/bug.php?id=81720,https://bugs.php.net/bug.php?id=81719

Unique Alert ID: 1010813 Found on: 2023-10-06 Severity: High

PHP < 7.4.30, 8.0.x < 8.0.20, 8.1.x < 8.1.7 Security Update (Jun 2022) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-08-27
CVE ID: CVE-2022-31625,CVE-2022-31626
Cvss Base: 8.8
Cvss Score: 8.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Description:

PHP released new versions which include a security fix. The following vulnerabilities exist: - CVE-2022-31625: Uninitialize d array in pg_query_params() - CVE-2022-31626: mysqlnd/pdo password buffer overflow

Solution:

VendorFix Update to version 7.4.30, 8.0.20, 8.1.7 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.4.30 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.4.30,https://www.php.net/ChangeLog-8.php#8.0.20,https://www.php.net/ChangeLog-8.php#8.1.7,https://bugs.php.net/bug.php?id=81720,https://bugs.php.net/bug.php?id=81719

Unique Alert ID: 539218 Found on: 2023-10-06 Severity: High

Apache HTTP Server Man-in-the-Middle Attack Vulnerability - July16 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-5387
Cvss Base: 8.1
Cvss Score: 8.1
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

Apache HTTP Server is prone to a man-in-the-middle attack vulnerability. The flaw is due to 'CGI Servlet' does not protec t applications from the presence of untrusted client data in the 'HTTP_PROXY' environment variable. Successful exploitati on will allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted proxy header in an HTTP request.

Solution:

VendorFix Update to version 2.4.24, or 2.2.32, or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.24 Installation path / port: 80/tcp

References:

- https://www.apache.org/security/asf-httpoxy-response.txt

Unique Alert ID: 539220 Found on: 2023-10-06 Severity: High

PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-5385,CVE-2016-6128
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a man-in-the-middle attack vulnerability. The following flaws exist: - The web servers running in a CGI or CGI-like context may assign client request proxy header values to internal HTTP_PROXY environment variables. - 'HTTP_PROXY' is improperly trusted by some PHP libraries and applications - An unspecified flaw in the gdImageCropThreshold function in 'gd_crop.c' in the GD Graphics Library. Successfully exploiting this issue may allow remote, unauthenticated to conduct MITM attacks on internal server subrequests or direct the server to initiate connections to arbitrary hosts or to cause a denial of service.

Solution:

VendorFix Update to PHP version 5.6.24 or 7.0.19.

Result:

Installed version: 5.4.16 Fixed version: 5.6.24/7.0.9

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php,http://www.kb.cert.org/vuls/id/797896,https://bugs.php.net/bug.php?id=72573,https://bugs.php.net/bug.php?id=72494

Unique Alert ID: 1533205 Found on: 2023-10-06 Severity: High

PHP < 8.0.28, 8.1.x < 8.1.16, 8.2.x < 8.2.3 Security Update - Linux (tcp/443)

Open Status: NEW **First Found:** 2023-10-06
CVE ID: CVE-2023-0567,CVE-2023-0568,CVE-2023-0662
Cvss Base: 7.8
Cvss Score: 7.8

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - CVE-2023-0567: Fixed bug #81744 (Password_verify() always return true with some hash) - CVE-2023-0568: Fixed bug #81746 (1-byte array overrun in common path resolve code) - CVE-2023-0662: Fixed bug GHSA-54hq-v5wp-fqgv (DOS vulnerability when parsing multipart request body)

Solution:

VendorFix Update to version 8.0.28, 8.1.16, 8.2.3 or later.

Result:

Installed version: 5.4.16 Fixed version: 8.0.28 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-8.php#8.2.3,https://www.php.net/ChangeLog-8.php#8.1.16,https://www.php.net/ChangeLog-8.php#8.0.28,https://www.php.net/archive/2023.php#2023-02-14-2,https://www.php.net/archive/2023.php#2023-02-14-3,https://www.php.net/archive/2023.php#2023-02-14-1,http://bugs.php.net/81744,http://bugs.php.net/81746,https://github.com/php/php-src/security/advisories/GHSA-54hq-v5wp-fqgv,https://github.com/php/php-src/security/advisories/GHSA-7fj2-8x79-rjf4

Unique Alert ID: 1533206 Found on: 2023-10-06 Severity: High

PHP < 8.0.28, 8.1.x < 8.1.16, 8.2.x < 8.2.3 Security Update - Linux (tcp/80)

Open Status:	NEW	**First Found:**	2023-10-06
CVE ID:	CVE-2023-0567,CVE-2023-0568,CVE-2023-0662		
Cvss Base:	7.8		
Cvss Score:	7.8		

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - CVE-2023-0567: Fixed bug #81744 (Password_verify( ) always return true with some hash) - CVE-2023-0568: Fixed bug #81746 (1-byte array overrun in common path resolv e code) - CVE-2023-0662: Fixed bug GHSA-54hq-v5wp-fqgv (DOS vulnerability when parsing multipart request body)

Solution:

VendorFix Update to version 8.0.28, 8.1.16, 8.2.3 or later.

Result:

Installed version: 5.4.16 Fixed version: 8.0.28 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-8.php#8.2.3,https://www.php.net/ChangeLog-8.php#8.1.16,https://www.php.net/ChangeLog-8.php#8.0.28,https://www.php.net/archive/2023.php#2023-02-14-2,https://www.php.net/archive/2023.php#2023-02-14-3,https://www.php.net/archive/2023.php#2023-02-14-1,http://bugs.php.net/81744,http://bugs.php.net/81746,https://github.com/php/php-src/security/advisories/GHSA-54hq-v5wp-fqgv,https://github.com/php/php-src/security/advisories/GHSA-7fj2-8x79-rjf4

Unique Alert ID: 1533207 Found on: 2023-10-06 Severity: High

PHP < 8.0.22, 8.1.x < 8.1.9 Security Update - Linux (tcp/80)

Open Status:	NEW	**First Found:**	2023-10-06
CVE ID:	CVE-2022-4900		
Cvss Base:	7.8		
Cvss Score:	7.8		

Description:

PHP is prone to a buffer overflow vulnerability. Fixed potential overflow for the builtin server via the PHP_CLI_SERVER_W ORKERS environment variable.

Solution:

VendorFix Update to version 8.0.22, 8.1.9, 8.2.0 or later.

Result:

Installed version: 5.4.16 Fixed version: 8.0.22/8.1.9/8.2.0 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-8.php#8.2.0,https://www.php.net/ChangeLog-8.php#8.1.9,https://www.php.net/ChangeLog-8.php#8.0.22,https://github.com/php/php-src/issues/8989,https://github.com/php/php-src/pull/9000,https://github.com/php/php-src/commit/789a37f14405e2d1a05a76c9fb4ed2d49d4580d5,https://bugzilla.redhat.com/show_bug.cgi?id=2179880

Unique Alert ID: 1533208 Found on: 2023-10-06 Severity: High

PHP < 8.0.22, 8.1.x < 8.1.9 Security Update - Linux (tcp/443)

Open Status: NEW **First Found:** 2023-10-06
CVE ID: CVE-2022-4900

Cvss Base: 7.8
Cvss Score: 7.8

Description:

PHP is prone to a buffer overflow vulnerability. Fixed potential overflow for the builtin server via the PHP_CLI_SERVER_WORKERS environment variable.

Solution:

VendorFix Update to version 8.0.22, 8.1.9, 8.2.0 or later.

Result:

Installed version: 5.4.16 Fixed version: 8.0.22/8.1.9/8.2.0 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-8.php#8.2.0,https://www.php.net/ChangeLog-8.php#8.1.9,https://www.php.net/ChangeLog-8.php#8.0.22,https://github.com/php/php-src/issues/8989,https://github.com/php/php-src/pull/9000,https://github.com/php/php-src/commit/789a37f14405e2d1a05a76c9fb4ed2d49d4580d5,https://bugzilla.redhat.com/show_bug.cgi?id=2179880

Unique Alert ID: 1533209 Found on: 2023-10-06 Severity: High

PHP < 8.0.27, 8.1.x < 8.1.14, 8.2.x < 8.2.1 Security Update - Linux (tcp/80)

Open Status: NEW **First Found:** 2023-10-06
CVE ID: CVE-2022-31631

Cvss Base: 7.8
Cvss Score: 7.8

Description:

PHP is prone to an integer overflow vulnerability. Due to an uncaught integer overflow, PDO::quote() of PDO_SQLite may return a not properly quoted string.

Solution:

VendorFix Update to version 8.0.27, 8.1.14, 8.2.1 or later.

Result:

Installed version: 5.4.16 Fixed version: 8.0.27 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-8.php#8.0.27,https://www.php.net/ChangeLog-8.php#8.1.14,https://www.php.net/ChangeLog-8.php#8.2.1

Unique Alert ID: 1533210 Found on: 2023-10-06 Severity: High

PHP < 8.0.27, 8.1.x < 8.1.14, 8.2.x < 8.2.1 Security Update - Linux (tcp/443)

Open Status:	NEW	**First Found:**	2023-10-06
CVE ID:	CVE-2022-31631		
Cvss Base:	7.8		
Cvss Score:	7.8		

Description:

PHP is prone to an integer overflow vulnerability. Due to an uncaught integer overflow, PDO::quote() of PDO_SQLite may return a not properly quoted string.

Solution:

VendorFix Update to version 8.0.27, 8.1.14, 8.2.1 or later.

Result:

Installed version: 5.4.16 Fixed version: 8.0.27 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-8.php#8.0.27,https://www.php.net/ChangeLog-8.php#8.1.14,https://www.php.net/ChangeLog-8.php#8.2.1

Unique Alert ID: 539185 Found on: 2023-10-06 Severity: High

OpenBSD OpenSSH <= 8.6 Command Injection Vulnerability (tcp/22)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2020-15778		
Cvss Base:	7.8		
Cvss Score:	7.8		
Cvss Vector:	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H		

Description:

OpenBSD OpenSSH is prone to a command injection vulnerability. scp of OpenSSH allows command injection in spc.c via backtick characters in the destination argument. Successful exploitation would allow an attacker to execute arbitrary cod e on the target machine.

Solution:

WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Result:

Installed version: 6.6.1 Fixed version: None Installation path / port: 22/tcp

References:

- https://github.com/cpandya2909/CVE-2020-15778/

Unique Alert ID: 539164 Found on: 2023-10-06 Severity: High

OpenSSH Privilege Escalation Vulnerability - May16 (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18

CVE ID: CVE-2015-8325
Cvss Base: 7.8
Cvss Score: 7.8
Cvss Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Description:

openssh is prone to a privilege escalation vulnerability. The flaw exists due to an error in 'do_setup_env function' in 'session.c' script in sshd which trigger a crafted environment for the /bin/login program when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories. Successfully exploiting this issue will allow local users to gain privileges.

Solution:

VendorFix Upgrade to OpenSSH version 7.2p2-3 or later.

Result:

Installed version: 6.6.1 Fixed version: 7.2p2-3 Installation path / port: 22/tcp

References:

- https://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-8325.html,https://anongit.mindrot.org/openssh.git/commit/?id=85bdcd7c92fe7ff133bbc4e10a65c91810f88755

Unique Alert ID: 539101 Found on: 2023-10-06 Severity: High

PHP Use-After-Free Remote Code EXecution Vulnerability - Jan15 (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-8142
Cvss Base: 7.5
Cvss Score: 7.5

Description:

PHP is prone to a use-after-free vulnerability. The flaw is due to Use-after-free vulnerability in the process_nested_data function in ext/standard/var _unserializer.re in PHP. Successful exploitation will allow remote attackers to execute arbitrary code via a crafted unserialize call.

Solution:

VendorFix Update to PHP version 5.4.36 or 5.5.20 or 5.6.4 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.36/5.5.20/5.6.4

References:

- http://php.net/ChangeLog-5.php,http://secunia.com/advisories/60920,https://bugs.php.net/bug.php?id=68594

Unique Alert ID: 919539 Found on: 2023-10-06 Severity: High

Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater) (tcp/22)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2002-20001,CVE-2022-40735		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

The remote SSH server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange (KEX) algorithms and thus could be prone to a denial of service (DoS) vulnerability. - CVE-2002-20001: The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE. - CVE-2022-40735: The Diffie-Hellman Key Agreement Protocol allows use of long exponents that arguably make certain calculations unnecessarily expensive, because the 1996 van Oorschot and Wiener paper found that '(appropriately) short exponents' can be used when there are adequate subgroup constraints, and these short exponents can lead to less expensive calculations than for long exponents. This issue is different from CVE-2002-20001 because it is based on an observation about exponent size, rather than an observation about numbers that are not public keys. The specific situations in which calculation expense would constitute a server-side vulnerability depend on the protocol (e.g., TLS, SSH, or IKE) and the DHE implementation details. In general, there might be an availability concern because of server-side resource consumption from DHE modular-exponentiation calculations. Finally, it is possible for an attacker to exploit this vulnerability and CVE-2002-20001 together. This vulnerability allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, also known as a D(HE)ater attack. There could be an increase in CPU usage in the affected component. For OpenSSH, users may observe issues such as a slowdown in SSH connections.

Solution:

Mitigation - DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For OpenSSH this limit can be configured via the 'MaxStartups' option, for other products please refer to the manual of the product in question on configuration possibilities.

Result:

The remote SSH server supports the following DHE KEX algorithm(s): diffie-hellman-group1-sha1 diffie-hellman-group14-sha1 diffie-hellman-group-exchange-sha1 diffie-hellman-group-exchange-sha256

References:

- https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol,https://github.com/Balasys/dheater

Unique Alert ID: 539206 Found on: 2023-10-06 Severity: High

Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2019-0217
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Description:

In Apache HTTP Server, a race condition in mod_auth_digest when running in a threaded server could allow a user with v alid credentials to authenticate using another username, bypassing configured access control restrictions.

Solution:

VendorFix Update to version 2.4.39 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.39 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539224 Found on: 2023-10-06 Severity: High

Apache HTTP Server 'Whitespace Defects' Multiple Vulnerabilities (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-8743
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Multiple flaws exist because the application accepted a broad patt ern of unusual whitespace patterns from the user-agent, including bare CR, FF, VTAB in parsing the request line and requ est header lines, as well as HTAB in parsing the request line. Any bare CR present in request lines was treated as whitesp ace and remained in the request field member 'the_request', while a bare CR in the request header field name would be honored as whitespace, and a bare CR in the request header field value was retained the input headers array. Implied ad ditional whitespace was accepted in the request line and prior to the ':' delimiter of any request header lines. Successful exploitation will allow remote attackers to conduct request smuggling, response splitting and cache pollution attacks.

Solution:

VendorFix Update to Apache HTTP Server 2.2.32 or 2.4.25 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.25 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_22.html,https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539233 Found on: 2023-10-06 Severity: High

Apache HTTP Server 'mod_auth_digest' DoS Vulnerability (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-2161		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

Apache HTTP Server is prone to a denial-of-service vulnerability. The flaw exists due to insufficient handling of malicious i nput to 'mod_auth_digest'. Successful exploitation will allow remote attackers to cause a denial-of-service condition.

Solution:

VendorFix Update to Apache HTTP Server 2.4.25 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.25 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2016-2161

Unique Alert ID: 539232 Found on: 2023-10-06 Severity: High

Apache HTTP Server 'mod_auth_digest' DoS Vulnerability (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-2161		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

Apache HTTP Server is prone to a denial-of-service vulnerability. The flaw exists due to insufficient handling of malicious i nput to 'mod_auth_digest'. Successful exploitation will allow remote attackers to cause a denial-of-service condition.

Solution:

VendorFix Update to Apache HTTP Server 2.4.25 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.25 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2016-2161

Unique Alert ID: 919540 Found on: 2023-10-06 Severity: High

Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2002-20001,CVE-2022-40735		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

The remote SSL/TLS server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange algorithms and thus could be pr one to a denial of service (DoS) vulnerability. - CVE-2002-20001: The Diffie-Hellman Key Agreement Protocol allows rem

ote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive ser ver-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest s upported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE. - CVE-2022-40735: The Diffie-Hellman Key Agreement Protocol allows use of lo ng exponents that arguably make certain calculations unnecessarily expensive, because the 1996 van Oorschot and Wien er paper found that '(appropriately) short exponents' can be used when there are adequate subgroup constraints, and th ese short exponents can lead to less expensive calculations than for long exponents. This issue is different from CVE-200 2-20001 because it is based on an observation about exponent size, rather than an observation about numbers that are n ot public keys. The specific situations in which calculation expense would constitute a server-side vulnerability depend on the protocol (e.g., TLS, SSH, or IKE) and the DHE implementation details. In general, there might be an availability conce rn because of server-side resource consumption from DHE modular-exponentiation calculations. Finally, it is possible for an attacker to exploit this vulnerability and CVE-2002-20001 together. This vulnerability allows remote attackers (from th e client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular -exponentiation calculations, also known as a D(HE)ater attack. There could be an increase in CPU usage in the affected component. For OpenSSH, users may observe issues such as a slowdown in SSH connections.

Solution:

Mitigation - DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities.

Result:

'DHE' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA 'DHE' cipher suites accepted by this service via the TLSv1.1
protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA 'DHE' cipher suites accepted by this service via the TLSv1.2
protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA

References:

- https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_K ey_Agreement_Protocol,https://github.com/Balasys/dheater

Unique Alert ID: 539223 Found on: 2023-10-06 Severity: High

Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2018-17199		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N		

Description:

In Apache HTTP Server mod_session checks the session expiry time before decoding the session. This causes session ex piry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

Solution:

VendorFix Update to version 2.4.38 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.38 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539238 Found on: 2023-10-06 Severity: High

Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2018-17199		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N		

Description:

In Apache HTTP Server mod_session checks the session expiry time before decoding the session. This causes session ex piry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

Solution:

VendorFix Update to version 2.4.38 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.38 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539207 Found on: 2023-10-06 Severity: High

Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerability (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2019-0217		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H		

Description:

In Apache HTTP Server, a race condition in mod_auth_digest when running in a threaded server could allow a user with v alid credentials to authenticate using another username, bypassing configured access control restrictions.

Solution:

VendorFix Update to version 2.4.39 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.39 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 919541 Found on: 2023-10-06 Severity: High

Apache HTTP Server < 2.4.48 NULL Pointer Dereference Vulnerability - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-31618
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

Apache HTTP Server is prone to a NULL pointer dereference vulnerability. Apache HTTP Server protocol handler for the H TTP/2 protocol checks received request headers against the size limitations as configured for the server and used for the HTTP/1 protocol as well. On violation of these restrictions an HTTP response is sent to the client with a status code indicati ng why the request was rejected. This rejection response was not fully initialised in the HTTP/2 protocol handler if the off ending header was the very first one received or appeared in a footer. This led to a NULL pointer dereference on initialise d memory, crashing reliably the child process. Successful exploitation will allow an attacker to crash the server.

Solution:

VendorFix Update to version 2.4.48 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.48 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 919542 Found on: 2023-10-06 Severity: High

Apache HTTP Server < 2.4.48 NULL Pointer Dereference Vulnerability - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-31618
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

Apache HTTP Server is prone to a NULL pointer dereference vulnerability. Apache HTTP Server protocol handler for the H TTP/2 protocol checks received request headers against the size limitations as configured for the server and used for the HTTP/1 protocol as well. On violation of these restrictions an HTTP response is sent to the client with a status code indicati ng why the request was rejected. This rejection response was not fully initialised in the HTTP/2 protocol handler if the off ending header was the very first one received or appeared in a footer. This led to a NULL pointer dereference on initialise d memory, crashing reliably the child process. Successful exploitation will allow an attacker to crash the server.

Solution:

VendorFix Update to version 2.4.48 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.48 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539282 Found on: 2023-10-06 Severity: High

PHP 'timelib_meridian' Heap Based Buffer Overflow Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2017-16642
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

PHP is prone to a heap buffer overflow vulnerability. The flaw exists due to an error in the date extension's 'timelib_meridian' handling of 'front of' and 'back of' directives. Successfully exploiting this issue allow attacker to execute arbitrary code with elevated privileges within the context of a privileged process.

Solution:

VendorFix Update to PHP version 5.6.32, 7.0.25, 7.1.11, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.32 Installation path / port: 80/tcp

References:

- http://php.net/ChangeLog-5.php,http://php.net/ChangeLog-7.php,https://bugs.php.net/bug.php?id=75055

Unique Alert ID: 539281 Found on: 2023-10-06 Severity: High

PHP 'timelib_meridian' Heap Based Buffer Overflow Vulnerability (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2017-16642
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

PHP is prone to a heap buffer overflow vulnerability. The flaw exists due to an error in the date extension's 'timelib_meridian' handling of 'front of' and 'back of' directives. Successfully exploiting this issue allow attacker to execute arbitrary code with elevated privileges within the context of a privileged process.

Solution:

VendorFix Update to PHP version 5.6.32, 7.0.25, 7.1.11, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.32 Installation path / port: 443/tcp

References:

- http://php.net/ChangeLog-5.php,http://php.net/ChangeLog-7.php,https://bugs.php.net/bug.php?id=75055

Unique Alert ID: 1010825 Found on: 2023-10-06 Severity: High

OpenSSL: Infinite loop in BN_mod_sqrt() reachable when parsing certificates (CVE-2022-0778) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-08-27
CVE ID: CVE-2022-0778
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

OpenSSL is prone to an infinite loop vulnerability. The BN_mod_sqrt() function, which computes a modular square root, c ontains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certific ates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point enco ded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve pa rameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an ex ternally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - T LS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else wh ich parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker ca n control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parse d during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-sig ned certificate to trigger the loop during verification of the certificate signature.

Solution:

VendorFix Update to version 1.0.2zd, 1.1.1n, 3.0.2 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2zd Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20220315.txt

Unique Alert ID: 1010824 Found on: 2023-10-06 Severity: High

OpenSSL: Infinite loop in BN_mod_sqrt() reachable when parsing certificates (CVE-2022-0778) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2022-08-27
CVE ID:	CVE-2022-0778	
Cvss Base:	7.5	
Cvss Score:	7.5	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	

Description:

OpenSSL is prone to an infinite loop vulnerability. The BN_mod_sqrt() function, which computes a modular square root, c ontains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certific ates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point enco ded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve pa rameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an ex ternally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - T LS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else wh ich parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker ca n control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parse d during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-sig ned certificate to trigger the loop during verification of the certificate signature.

Solution:

VendorFix Update to version 1.0.2zd, 1.1.1n, 3.0.2 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2zd Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20220315.txt

Unique Alert ID: 919537 Found on: 2023-10-06 Severity: High

OpenSSL: Integer overflow in CipherUpdate (CVE-2021-23840) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2021-23840	
Cvss Base:	7.5	
Cvss Score:	7.5	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	

Description:

OpenSSL is prone to an integer overflow vulnerability. Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_Decrypt Update may overflow the output length argument in some cases where the input length is close to the maximum permissi ble length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating succes s), but the output length value will be negative. This vulnerability could cause applications to behave incorrectly or crash.

Solution:

VendorFix Update to version 1.0.2y, 1.1.1j or later. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2y / 1.1.1j Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20210216.txt

Unique Alert ID: 919538 Found on: 2023-10-06 Severity: High

OpenSSL: Integer overflow in CipherUpdate (CVE-2021-23840) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2021-23840	
Cvss Base:	7.5	
Cvss Score:	7.5	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	

Description:

OpenSSL is prone to an integer overflow vulnerability. Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_Decrypt Update may overflow the output length argument in some cases where the input length is close to the maximum permissi ble length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating succes s), but the output length value will be negative. This vulnerability could cause applications to behave incorrectly or crash.

Solution:

VendorFix Update to version 1.0.2y, 1.1.1j or later. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2y / 1.1.1j Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20210216.txt

Unique Alert ID: 539234 Found on: 2023-10-06 Severity: High

Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-1303
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

Apache HTTP Server is prone to a denial of service vulnerability. The flaw exists as the Apache HTTP Server fails to saniti ze against a specially crafted HTTP request header. Successful exploitation will allow an attacker to crash the Apache HTT P Server resulting in denial of service condition.

Solution:

VendorFix Update to version 2.4.30 or later. Please see the references for more information.

Result:

Installed version: 2.4.6 Fixed version: 2.4.30 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539236 Found on: 2023-10-06 Severity: High

Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-1303
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

Apache HTTP Server is prone to a denial of service vulnerability. The flaw exists as the Apache HTTP Server fails to saniti ze against a specially crafted HTTP request header. Successful exploitation will allow an attacker to crash the Apache HTT P Server resulting in denial of service condition.

Solution:

VendorFix Update to version 2.4.30 or later. Please see the references for more information.

Result:

Installed version: 2.4.6 Fixed version: 2.4.30 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539276 Found on: 2023-10-06 Severity: High

PHP 'WDDX Deserialization' Denial of Service Vulnerability - (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2017-11143		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw exists due to an invalid free error for an empty boolean element in ext/wddx/wddx.c script. Successfully exploiting this issue allow remote attackers inject XML for deserialization to crash the PHP interpreter.

Solution:

VendorFix Update to PHP version 5.6.31 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.31

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539275 Found on: 2023-10-06 Severity: High

PHP 'WDDX Deserialization' Denial of Service Vulnerability - (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2017-11143		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw exists due to an invalid free error for an empty boolean element in ext/wddx/wddx.c script. Successfully exploiting this issue allow remote attackers inject XML for deserialization to crash the PHP interpreter.

Solution:

VendorFix Update to PHP version 5.6.31 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.31

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539079 Found on: 2023-10-06 Severity: High

PHP Denial of Service Vulnerability Jul17 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2017-11142
Cvss Base: 7.5
Cvss Score: 7.5

Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw exists due to improper handling of long form variables in main/php_variables.c script. Successfully exploiting this issue allow an attacker to cause a CPU consumption denial of ser vice attack.

Solution:

VendorFix Update to PHP version 5.6.31, 7.0.17, 7.1.3 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.31

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539081 Found on: 2023-10-06 Severity: High

PHP Denial of Service Vulnerability Jul17 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2017-11142
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw exists due to improper handling of long form variables in main/php_variables.c script. Successfully exploiting this issue allow an attacker to cause a CPU consumption denial of ser vice attack.

Solution:

VendorFix Update to PHP version 5.6.31, 7.0.17, 7.1.3 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.31

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539278 Found on: 2023-10-06 Severity: High

PHP Multiple Denial of Service Vulnerabilities (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-8877,CVE-2015-8879,CVE-2015-8874
Cvss Base: 7.5

Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to multiple denial of service (DoS) vulnerabilities. Multiple flaws are due to - An improper handling of driver behavior for SQL_WVARCHAR columns in the 'odbc_bindcols function' in 'ext/odbc/php_odbc.c' script. - The 'gdImageScal eTwoPass' function in gd_interpolation.c script in the GD Graphics Library uses inconsistent allocate and free approaches. Successfully exploiting this issue allow remote attackers to cause a denial of service (application crash or memory consu ption).

Solution:

VendorFix Update to PHP version 5.6.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.12

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539277 Found on: 2023-10-06 Severity: High

PHP Multiple Denial of Service Vulnerabilities (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-8877,CVE-2015-8879,CVE-2015-8874
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to multiple denial of service (DoS) vulnerabilities. Multiple flaws are due to - An improper handling of driver behavior for SQL_WVARCHAR columns in the 'odbc_bindcols function' in 'ext/odbc/php_odbc.c' script. - The 'gdImageScal eTwoPass' function in gd_interpolation.c script in the GD Graphics Library uses inconsistent allocate and free approaches. Successfully exploiting this issue allow remote attackers to cause a denial of service (application crash or memory consu ption).

Solution:

VendorFix Update to PHP version 5.6.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.12

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539227 Found on: 2023-10-06 Severity: High

Apache HTTP Server OPTIONS Memory Leak Vulnerability (Optionsbleed) - Version Check (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2017-9798
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

Apache HTTP Server allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. Optionsbleed is a use after free er ror in the Apache HTTP Server that causes a corrupted Allow header to be constructed in response to HTTP OPTIONS req uests. This can leak pieces of arbitrary memory from the server process that may contain secrets. The memory pieces c hange after multiple requests, so for a vulnerable host an arbitrary number of memory chunks can be leaked. The bug a ppears if a webmaster tries to use the 'Limit' directive with an invalid HTTP method. Example .htaccess: The successful e xploitation allows the attacker to read chunks of the host's memory.

Solution:

VendorFix Update to Apache HTTP Server 2.4.28. For Apache HTTP Server running version 2.2.34 apply the patch linked in the references. As a workaround the usage of .htaccess should be disabled completely via the 'AllowOverride None' directive within the webservers configuration. Furthermore all statements within the webserver configuration needs to be verified for invalid HTTP methods.

Result:

Installed version: 2.4.6 Fixed version: 2.4.28 Installation path / port: 80/tcp

References:

- http://openwall.com/lists/oss-security/2017/09/18/2,https://blog.fuzzing-project.org/60-Optionsbleed-HTTP-OPTION S-method-can-leak-Apaches-server-memory.html,https://archive.apache.org/dist/httpd/patches/apply_to_2.2.34/

Unique Alert ID: 539226 Found on: 2023-10-06 Severity: High

Apache HTTP Server OPTIONS Memory Leak Vulnerability (Optionsbleed) - Version Check (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2017-9798
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

Apache HTTP Server allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. Optionsbleed is a use after free er ror in the Apache HTTP Server that causes a corrupted Allow header to be constructed in response to HTTP OPTIONS req uests. This can leak pieces of arbitrary memory from the server process that may contain secrets. The memory pieces c hange after multiple requests, so for a vulnerable host an arbitrary number of memory chunks can be leaked. The bug a ppears if a webmaster tries to use the 'Limit' directive with an invalid HTTP method. Example .htaccess: The successful e xploitation allows the attacker to read chunks of the host's memory.

Solution:

VendorFix Update to Apache HTTP Server 2.4.28. For Apache HTTP Server running version 2.2.34 apply the patch linked in the references. As a workaround the usage of .htaccess should be disabled completely via the 'AllowOverride None' directive within the webservers configuration. Furthermore all statements within the webserver configuration needs to be verified for invalid HTTP methods.

Result:

Installed version: 2.4.6 Fixed version: 2.4.28 Installation path / port: 443/tcp

References:

- http://openwall.com/lists/oss-security/2017/09/18/2,https://blog.fuzzing-project.org/60-Optionsbleed-HTTP-OPTIONS-method-can-leak-Apaches-server-memory.html,https://archive.apache.org/dist/httpd/patches/apply_to_2.2.34/

Unique Alert ID: 919543 Found on: 2023-10-06 Severity: High

Apache HTTP Server mod_session_crypto Vulnerability (Dec 2016) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2016-0736
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

Apache HTTP Server is prone to a vulnerability in mod_session_crypto. mod_sessioncrypto is encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This makes it vulnerable to padding oracle attacks, particularly with CBC. An authentication tag (SipHash MAC) is now added to prevent such attacks.

Solution:

VendorFix Update to version 2.4.25 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.25 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 919544 Found on: 2023-10-06 Severity: High

Apache HTTP Server mod_session_crypto Vulnerability (Dec 2016) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2016-0736
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

Apache HTTP Server is prone to a vulnerability in mod_session_crypto. mod_sessioncrypto is encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This makes it vulnerable to padding oracle attacks, particularly with CBC. An authentication tag (SipHash MAC) is now added to prevent such attacks.

Solution:

VendorFix Update to version 2.4.25 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.25 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 1533211 Found on: 2023-10-06 Severity: High

OpenSSL 1.0.2 < 1.0.2zg, 1.1.1 < 1.1.1t, 3.0 < 3.0.8 Multiple Vulnerabilities - Linux (tcp/80)

Open Status: NEW **First Found:** 2023-10-06
CVE ID: CVE-2022-4304,CVE-2023-0215,CVE-2023-0286
Cvss Base: 7.4
Cvss Score: 7.4
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H

Description:

OpenSSL is prone to multiple vulnerabilities. The following flaws exist: - CVE-2022-4304: Timing Oracle in RSA Decryptio n - CVE-2023-0215: Use-after-free following BIO_new_NDEF - CVE-2023-0286: X.400 address type confusion in X.509 G eneralName

Solution:

VendorFix Update to version 1.0.2zg, 1.1.1t, 3.0.8 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2zg Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20230207.txt

Unique Alert ID: 1533212 Found on: 2023-10-06 Severity: High

OpenSSL 1.0.2 < 1.0.2zg, 1.1.1 < 1.1.1t, 3.0 < 3.0.8 Multiple Vulnerabilities - Linux (tcp/443)

Open Status: NEW **First Found:** 2023-10-06
CVE ID: CVE-2022-4304,CVE-2023-0215,CVE-2023-0286
Cvss Base: 7.4
Cvss Score: 7.4
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H

Description:

OpenSSL is prone to multiple vulnerabilities. The following flaws exist: - CVE-2022-4304: Timing Oracle in RSA Decryptio n - CVE-2023-0215: Use-after-free following BIO_new_NDEF - CVE-2023-0286: X.400 address type confusion in X.509 G eneralName

Solution:

VendorFix Update to version 1.0.2zg, 1.1.1t, 3.0.8 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2zg Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20230207.txt

Unique Alert ID: 539225 Found on: 2023-10-06 Severity: High

Apache HTTP Server 'Whitespace Defects' Multiple Vulnerabilities (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-8743
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Multiple flaws exist because the application accepted a broad patt ern of unusual whitespace patterns from the user-agent, including bare CR, FF, VTAB in parsing the request line and requ est header lines, as well as HTAB in parsing the request line. Any bare CR present in request lines was treated as whitesp ace and remained in the request field member 'the_request', while a bare CR in the request header field name would be honored as whitespace, and a bare CR in the request header field value was retained the input headers array. Implied ad ditional whitespace was accepted in the request line and prior to the ':' delimiter of any request header lines. Successful exploitation will allow remote attackers to conduct request smuggling, response splitting and cache pollution attacks.

Solution:

VendorFix Update to Apache HTTP Server 2.2.32 or 2.4.25 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.25 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_22.html,https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539256 Found on: 2023-10-06 Severity: High

PHP 'CVE-2017-7189' Improper Input Validation Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2017-7189
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

PHP is improperly validating input from untrusted input. main/streams/xp_socket.c in PHP misparses fsockopen calls, suc h as by interpreting fsockopen('127.0.0.1:80', 443) as if the address/port were 127.0.0.1:80:443, which is later truncated to 127.0.0.1:80. This behavior has a security risk if the explicitly provided port number (i.e., 443 in this example) is hard coded into an application as a security policy, but the hostname argument (i.e., 127.0.0.1:80 in this example) is obtained from untrusted input.

Solution:

WillNotFix No solution was made available by the vendor. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one. Note: PHP versions 7.0.18 and 7.1.4 introduced a fix which was reverted again in version 7.0.19 / 7.1.5 respectively and the fix wasn't introduced again as of today (08-2020).

Result:

Installed version: 5.4.16 Fixed version: None Installation path / port: 80/tcp

References:

- https://bugs.php.net/bug.php?id=74192,https://bugs.php.net/bug.php?id=74429,https://github.com/php/php-src/commit/bab0b99f376dac9170ac81382a5ed526938d595a

Unique Alert ID: 539254 Found on: 2023-10-06 Severity: High

PHP 'CVE-2017-7189' Improper Input Validation Vulnerability (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2017-7189
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

PHP is improperly validating input from untrusted input. main/streams/xp_socket.c in PHP misparses fsockopen calls, such as by interpreting fsockopen('127.0.0.1:80', 443) as if the address/port were 127.0.0.1:80:443, which is later truncated to 127.0.0.1:80. This behavior has a security risk if the explicitly provided port number (i.e., 443 in this example) is hard coded into an application as a security policy, but the hostname argument (i.e., 127.0.0.1:80 in this example) is obtained from untrusted input.

Solution:

WillNotFix No solution was made available by the vendor. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one. Note: PHP versions 7.0.18 and 7.1.4 introduced a fix which was reverted again in version 7.0.19 / 7.1.5 respectively and the fix wasn't introduced again as of today (08-2020).

Result:

Installed version: 5.4.16 Fixed version: None Installation path / port: 443/tcp

References:

- https://bugs.php.net/bug.php?id=74192,https://bugs.php.net/bug.php?id=74429,https://github.com/php/php-src/commit/bab0b99f376dac9170ac81382a5ed526938d595a

Unique Alert ID: 539255 Found on: 2023-10-06 Severity: High

PHP 'CVE-2018-19935' - 'imap_mail' Denial of Service Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-19935
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw exists due to a NULL pointer dereference and application crash via an empty string in the message argument to the imap_mail function of ext/imap/php_imap.c. Successful exploitation will allow attackers to cause a denial of service of the affected application.

Solution:

VendorFix Update to version 5.6.39, 7.0.33, 7.1.26, 7.2.14, 7.3.0 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.39 Installation path / port: 80/tcp

References:

- https://bugs.php.net/bug.php?id=77020

Unique Alert ID: 539253 Found on: 2023-10-06 Severity: High

PHP 'CVE-2018-19935' - 'imap_mail' Denial of Service Vulnerability (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-19935
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw exists due to a NULL pointer dereference and application crash via an empty string in the message argument to the imap_mail function of ext/imap/php_imap.c. Successful exploit ation will allow attackers to cause a denial of service of the affected application.

Solution:

VendorFix Update to version 5.6.39, 7.0.33, 7.1.26, 7.2.14, 7.3.0 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.39 Installation path / port: 443/tcp

References:

- https://bugs.php.net/bug.php?id=77020

Unique Alert ID: 539242 Found on: 2023-10-06 Severity: High

PHP 'stream_get_meta_data' Privilege Escalation Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-10712
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Description:

PHP is prone to a privilege escalation vulnerability. The flaw exists due to error in the function stream_get_meta_data of t he component File Upload. The manipulation as part of a Return Value leads to a privilege escalation vulnerability (Metad ata). Successfully exploitation will allow an attacker to update the 'metadata' and affect on confidentiality, integrity, and a vailability.

Solution:

VendorFix Update to PHP version 5.5.32, 7.0.3, or 5.6.18 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.32 Installation path / port: 80/tcp

References:

- https://bugs.php.net/bug.php?id=71323

Unique Alert ID: 539241 Found on: 2023-10-06 Severity: High

PHP 'stream_get_meta_data' Privilege Escalation Vulnerability (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-10712
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Description:

PHP is prone to a privilege escalation vulnerability. The flaw exists due to error in the function stream_get_meta_data of t he component File Upload. The manipulation as part of a Return Value leads to a privilege escalation vulnerability (Metad ata). Successfully exploitation will allow an attacker to update the 'metadata' and affect on confidentiality, integrity, and a vailability.

Solution:

VendorFix Update to PHP version 5.5.32, 7.0.3, or 5.6.18 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.32 Installation path / port: 443/tcp

References:

- https://bugs.php.net/bug.php?id=71323

Unique Alert ID: 539262 Found on: 2023-10-06 Severity: High

PHP < 7.2.30, 7.3 < 7.3.17, 7.4 < 7.4.5 DoS Vulnerability - Apr20 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2020-7067
Cvss Base: 7.5
Cvss Score: 7.5

Description:

PHP is prone to a denial-of-service vulnerability. If 'CHARSET_EBCDIC' is defined (usually, on systems with EBCDIC enc oding support), an out-of-bounds read can occur using a malformed url-encoded string.

Solution:

VendorFix Update to version 7.2.30, 7.3.17, 7.4.5 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.30 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.30,https://www.php.net/ChangeLog-7.php#7.3.17,https://www.php.net/ ChangeLog-7.php#7.4.5

Unique Alert ID: 539260 Found on: 2023-10-06 Severity: High

PHP < 7.2.30, 7.3 < 7.3.17, 7.4 < 7.4.5 DoS Vulnerability - Apr20 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2020-7067
Cvss Base: 7.5
Cvss Score: 7.5

Description:

PHP is prone to a denial-of-service vulnerability. If 'CHARSET_EBCDIC' is defined (usually, on systems with EBCDIC enc oding support), an out-of-bounds read can occur using a malformed url-encoded string.

Solution:

VendorFix Update to version 7.2.30, 7.3.17, 7.4.5 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.30 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.30,https://www.php.net/ChangeLog-7.php#7.3.17,https://www.php.net/ ChangeLog-7.php#7.4.5

Unique Alert ID: 919545 Found on: 2023-10-06 Severity: High

PHP < 7.3.27, 7.4.x < 7.4.15, 8.0.x < 8.0.2 NULL Deference Vulnerability (Feb 2021) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2021-21702		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to a NULL dereference vulnerability in the SoapClient.

Solution:

VendorFix Update to version 7.3.27, 7.4.15, 8.0.2 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.27 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.27,https://www.php.net/ChangeLog-7.php#7.4.15,https://www.php.net/ChangeLog-8.php#8.0.2

Unique Alert ID: 919546 Found on: 2023-10-06 Severity: High

PHP < 7.3.27, 7.4.x < 7.4.15, 8.0.x < 8.0.2 NULL Deference Vulnerability (Feb 2021) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2021-21702		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to a NULL dereference vulnerability in the SoapClient.

Solution:

VendorFix Update to version 7.3.27, 7.4.15, 8.0.2 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.27 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.27,https://www.php.net/ChangeLog-7.php#7.4.15,https://www.php.net/ChangeLog-8.php#8.0.2

Unique Alert ID: 539250 Found on: 2023-10-06 Severity: High

PHP Fileinfo Component Denial of Service Vulnerability (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-0236		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due an improper validation of input to zero root_storag e value in a CDF file. Successfully exploiting this issue allow remote attackers to cause a denial of service.

Solution:

VendorFix Update to PHP version 5.6.0

Result:

Installed version: 5.4.16 Fixed version: 5.6.0

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539249 Found on: 2023-10-06 Severity: High

PHP Fileinfo Component Denial of Service Vulnerability (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-0236
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due an improper validation of input to zero root_storag e value in a CDF file. Successfully exploiting this issue allow remote attackers to cause a denial of service.

Solution:

VendorFix Update to PHP version 5.6.0

Result:

Installed version: 5.4.16 Fixed version: 5.6.0

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539154 Found on: 2023-10-06 Severity: High

PHP Multiple Double Free Vulnerabilities - Jan15 (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-9425,CVE-2014-9709
Cvss Base: 7.5
Cvss Score: 7.5

Description:

PHP is prone to a denial of service (DoS) vulnerability. Multiple flaws are due to: - Double free error in the 'zend_ts_hash _graceful_destroy' function in 'zend_ts_hash.c script in the Zend Engine in PHP. - flaw in the 'GetCode_' function in 'gd_gi f_in.c' script in GD Graphics Library (LibGD). Successful exploitation will allow remote attackers to cause a denial of servi ce or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.5.21 or 5.6.5 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.21/5.6.5

References:

- http://securitytracker.com/id/1031479,https://bugs.php.net/bug.php?id=68676

Unique Alert ID: 539153 Found on: 2023-10-06 Severity: High

PHP Multiple Double Free Vulnerabilities - Jan15 (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-9425,CVE-2014-9709		
Cvss Base:	7.5		
Cvss Score:	7.5		

Description:

PHP is prone to a denial of service (DoS) vulnerability. Multiple flaws are due to: - Double free error in the 'zend_ts_hash _graceful_destroy' function in 'zend_ts_hash.c script in the Zend Engine in PHP. - flaw in the 'GetCode_' function in 'gd_gi f_in.c' script in GD Graphics Library (LibGD). Successful exploitation will allow remote attackers to cause a denial of servi ce or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.5.21 or 5.6.5 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.21/5.6.5

References:

- http://securitytracker.com/id/1031479,https://bugs.php.net/bug.php?id=68676

Unique Alert ID: 539248 Found on: 2023-10-06 Severity: High

PHP Multiple Heap Buffer Overflow and Information Disclosure Vulnerabilities (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2018-14851,CVE-2018-14883,CVE-2018-15132		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N		

Description:

PHP is prone to multiple heap buffer overflow and information disclosure vulnerabilities. Multiple flaws exist due to: - exif _process_IFD_in_MAKERNOTE function in exif.c file suffers from improper validation against crafted JPEG files. - exif_thu mbnail_extract function in exif.c file suffers from improper validation of length of 'ImageInfo->Thumbnail.offset + ImageI nfo->Thumbnail.size' - linkinfo function on windows doesn't implement openbasedir check. Successful exploitation will allo w attackers to cause heap overflow, denial of service and disclose sensitive information.

Solution:

VendorFix Update to PHP version 5.6.37, 7.0.31, 7.1.20 or 7.2.8 or later. Please see the references for more information.

Result:

Installed version: 5.4.16 Fixed version: 5.6.37 Installation path / port: 80/tcp

References:

- https://access.redhat.com/security/cve/cve-2018-14851,https://bugs.php.net/bug.php?id=76557,https://bugs.php.n et/bug.php?id=76423,https://bugs.php.net/bug.php?id=76459

Unique Alert ID: 539247 Found on: 2023-10-06 Severity: High

PHP Multiple Heap Buffer Overflow and Information Disclosure Vulnerabilities (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-14851,CVE-2018-14883,CVE-2018-15132
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

PHP is prone to multiple heap buffer overflow and information disclosure vulnerabilities. Multiple flaws exist due to: - exif_process_IFD_in_MAKERNOTE function in exif.c file suffers from improper validation against crafted JPEG files. - exif_thumbnail_extract function in exif.c file suffers from improper validation of length of 'ImageInfo->Thumbnail.offset + ImageInfo->Thumbnail.size' - linkinfo function on windows doesn't implement openbasedir check. Successful exploitation will allow attackers to cause heap overflow, denial of service and disclose sensitive information.

Solution:

VendorFix Update to PHP version 5.6.37, 7.0.31, 7.1.20 or 7.2.8 or later. Please see the references for more information.

Result:

Installed version: 5.4.16 Fixed version: 5.6.37 Installation path / port: 443/tcp

References:

- https://access.redhat.com/security/cve/cve-2018-14851,https://bugs.php.net/bug.php?id=76557,https://bugs.php.net/bug.php?id=76423,https://bugs.php.net/bug.php?id=76459

Unique Alert ID: 539152 Found on: 2023-10-06 Severity: High

PHP Multiple Remote Code Execution Vulnerabilities - Jul15 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-0273,CVE-2014-9705
Cvss Base: 7.5
Cvss Score: 7.5

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Multiple use-after-free vulnerabilities in 'ext/date/php_date.c' script. - Heap-based buffer overflow in the 'enchant_broker_request_dict' function in 'ext/enchant/enchant.c' script. Successfully exploiting this issue allow remote attackers to execute arbitrary code via some crafted dimensions.

Solution:

VendorFix Update to PHP 5.4.38 or 5.5.22 or 5.6.6 or later.

Result:

Installed Version: 5.4.16 Fixed Version: 5.4.48

References:

- http://php.net/ChangeLog-5.php,https://bugzilla.redhat.com/show_bug.cgi?id=1194730,http://lists.opensuse.org/opensuse-updates/2015-04/msg00002.html

Unique Alert ID: 539151 Found on: 2023-10-06 Severity: High

PHP Multiple Remote Code Execution Vulnerabilities - Jul15 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18

CVE ID: CVE-2015-0273,CVE-2014-9705
Cvss Base: 7.5
Cvss Score: 7.5

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Multiple use-after-free vulnerabilities in 'ext/date/php_date.c' script. - Heap-based buffer overflow in the 'enchant_broker_request_dict' function in 'ext/enchant/enchant.c' script. Successfully exploiting this issue allow remote attackers to execute arbitrary code via some crafted dimensions.

Solution:

VendorFix Update to PHP 5.4.38 or 5.5.22 or 5.6.6 or later.

Result:

Installed Version: 5.4.16 Fixed Version: 5.4.48

References:

- http://php.net/ChangeLog-5.php,https://bugzilla.redhat.com/show_bug.cgi?id=1194730,http://lists.opensuse.org/opensuse-updates/2015-04/msg00002.html

Unique Alert ID: 539147 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Feb15 (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-0232,CVE-2015-0231,CVE-2014-9652,CVE-2014-9653
Cvss Base: 7.5
Cvss Score: 7.5

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Flaw in the 'exif_process_unicode' function in ext/exif/exif.c script when parsing JPEG EXIF entries. - A use-after-free error in the 'process_nested_data' function in ext/standard/var_unserializer.re script. - a flaw in 'readelf.c' script in Fine Free File. - an out-of-bounds read flaw in 'src/softmagic.c' script in Fine Free File. Successful exploitation will allow remote attackers to cause a denial of service or possibly execute arbitrary code via different crafted dimensions.

Solution:

VendorFix Update to PHP version 5.4.37 or 5.5.21 or 5.6.5 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.37

References:

- https://bugs.php.net/bug.php?id=68799,https://bugs.php.net/bug.php?id=68710

Unique Alert ID: 539146 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Feb15 (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2015-0232,CVE-2015-0231,CVE-2014-9652,CVE-2014-9653	
Cvss Base:	7.5	
Cvss Score:	7.5	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Flaw in the 'exif_process_unicode' function in ext/exif/exif.c script when parsing JPEG EXIF entries. - A use-after-free error in the 'process_nested_data' function in ext/standard/var_unserializer.re script. - a flaw in 'readelf.c' script in Fine Free File. - an out-of-bounds read flaw in 'src/softmagic.c' script in Fine Free File. Successful exploitation will allow remote attackers to cause a denial of service or possibly execute arbitrary code via different crafted dimensions.

Solution:

VendorFix Update to PHP version 5.4.37 or 5.5.21 or 5.6.5 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.37

References:

- https://bugs.php.net/bug.php?id=68799,https://bugs.php.net/bug.php?id=68710

Unique Alert ID: 539143 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Jan15 (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2014-3670,CVE-2014-3669,CVE-2014-3668	
Cvss Base:	7.5	
Cvss Score:	7.5	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - The exif_ifd_make_value function in exif.c in the EXIF extension in PHP operates on floating-point arrays incorrectly. - Integer overflow in the object_custom function in ext/standard/var _unserializer.c in PHP. - Buffer overflow in the date_from_ISO8601 function in the mkgmtime implementation in libxmlrpc/xmlrpc.c in the XMLRPC extension in PHP. Successful exploitation will allow remote attackers to cause a denial of service or possibly execute arbitrary code via different crafted dimensions.

Solution:

VendorFix Update to PHP version 5.4.34 or 5.5.18 or 5.6.2 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.34/5.5.18/5.6.2

References:

- https://bugs.php.net/bug.php?id=68044

Unique Alert ID: 539141 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Jan15 (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-3670,CVE-2014-3669,CVE-2014-3668		
Cvss Base:	7.5		
Cvss Score:	7.5		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - The exif_ifd_make_value function in exif.c in the EXIF extension in PHP operates on floating-point arrays incorrectly. - Integer overflow in the object_custom function in ext/standard/var _unserializer.c in PHP. - Buffer overflow in the date_from_ISO8601 function in the mkgmtime implementation in libxmlrpc/xmlrpc.c in the XMLRPC extension in PHP. Successful exploitation will allow remote attackers to cause a denial of service or possibly execute arbitrary code via different crafted dimensions.

Solution:

VendorFix Update to PHP version 5.4.34 or 5.5.18 or 5.6.2 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.34/5.5.18/5.6.2

References:

- https://bugs.php.net/bug.php?id=68044

Unique Alert ID: 539139 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Jun15 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-4148,CVE-2015-4147,CVE-2015-2787,CVE-2015-2348,CVE-2015-2331		
Cvss Base:	7.5		
Cvss Score:	7.5		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - 'do_soap_call' function in ext/soap/soap.c script in PHP does not verify that the uri property is a string. - 'SoapClient::__call' method in ext/soap/soap.c script in PHP does not verify that __default_headers is an array. - use-after-free error related to the 'unserialize' function when using DateInterval input. - a flaw in the 'move_uploaded_file' function that is triggered when handling NULL bytes. - an integer overflow condition in the '_zip_cdir_new' function in 'zip_dirent.c' script. Successfully exploiting this issue allow remote attackers to obtain sensitive information by providing crafted serialized data with an int data type and to execute arbitrary code by providing crafted serialized data with an unexpected data type.

Solution:

VendorFix Update to PHP 5.4.39 or 5.5.23 or 5.6.7 or later.

Result:

Installed Version: 5.4.16 Fixed Version: 5.4.39

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=69085,http://openwall.com/lists/oss-security/2015/06/01/4

Unique Alert ID: 539135 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Jun15 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-4148,CVE-2015-4147,CVE-2015-2787,CVE-2015-2348,CVE-2015-2331		
Cvss Base:	7.5		
Cvss Score:	7.5		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - 'do_soap_call' function in ext/soap/soap.c script in PHP does not verify that the uri property is a string. - 'SoapClient::__call' method in ext/soap/soap.c script in PHP does not verify that __default_headers is an array. - use-after-free error related to the 'unserialize' function when using DateInterval input. - a flaw in the 'move_uploaded_file' function that is triggered when handling NULL bytes. - an integer overflow condition in the '_zip_cdir_new' function in 'zip_dirent.c' script. Successfully exploiting this issue allow remote attackers to obtain sensitive information by providing crafted serialized data with an int data type and to execute arbitrary code by providing crafted serialized data with an unexpected data type.

Solution:

VendorFix Update to PHP 5.4.39 or 5.5.23 or 5.6.7 or later.

Result:

Installed Version: 5.4.16 Fixed Version: 5.4.39

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=69085,http://openwall.com/lists/oss-security/2015/06/01/4

Unique Alert ID: 539133 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 02 - Jan15 (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-9426		
Cvss Base:	7.5		
Cvss Score:	7.5		

Description:

PHP is prone to multiple vulnerabilities. The flaw is due to a free operation on a stack-based character array by The apprentice_load function in libmagic/apprentice.c in the Fileinfo component. Successful exploitation will allow remote attackers to cause a denial of service or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.6.5 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.5

References:

- https://bugs.php.net/bug.php?id=68665,http://securitytracker.com/id/1031480

Unique Alert ID: 539132 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 02 - Jan15 (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-9426		
Cvss Base:	7.5		
Cvss Score:	7.5		

Description:

PHP is prone to multiple vulnerabilities. The flaw is due to a free operation on a stack-based character array by The apprentice_load function in libmagic/apprentice.c in the Fileinfo component. Successful exploitation will allow remote attackers to cause a denial of service or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.6.5 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.5

References:

- https://bugs.php.net/bug.php?id=68665,http://securitytracker.com/id/1031480

Unique Alert ID: 539131 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 02 - Jun15 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-4026,CVE-2015-4025,CVE-2015-4024,CVE-2015-4022,CVE-2015-4021		
Cvss Base:	7.5		
Cvss Score:	7.5		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Algorithmic complexity vulnerability in the 'multipart_buffer_headers' function in main/rfc1867.c script in PHP. - 'pcntl_exec' implementation in PHP truncates a pathname upon encountering a \x00 character. - Integer overflow in the 'ftp_genlist' function in ext/ftp/ftp.c script in PHP. - The 'phar_parse_tarfile' function in ext/phar/tar.c script in PHP does not verify that the first character of a filename is different from the \0 character. Successfully exploiting this issue allow remote attackers to cause a denial of service, bypass intended extension restrictions and access and execute files or directories with unexpected names via crafted dimensions and remote FTP servers to execute arbitrary code.

Solution:

VendorFix Update to PHP 5.4.41 or 5.5.25 or 5.6.9 or later.

Result:

Installed Version: 5.4.16 Fixed Version: 5.4.41

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=69085,http://openwall.com/lists/oss-security/2015/06/01/4

Unique Alert ID: 539130 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 02 - Jun15 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-4026,CVE-2015-4025,CVE-2015-4024,CVE-2015-4022,CVE-2015-4021		
Cvss Base:	7.5		
Cvss Score:	7.5		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Algorithmic complexity vulnerability in the 'multipart_buffer_headers' function in main/rfc1867.c script in PHP. - 'pcntl_exec' implementation in PHP truncates a pathname upon encountering a \x00 character. - Integer overflow in the 'ftp_genlist' function in ext/ftp/ftp.c script in PHP. - The 'phar_parse_tarfile' function in ext/phar/tar.c script in PHP does not verify that the first character of a filename is different from the \0 character. Successfully exploiting this issue allow remote attackers to cause a denial of service, bypass intended extension restrictions and access and execute files or directories with unexpected names via crafted dimensions and remote FTP servers to execute arbitrary code.

Solution:

VendorFix Update to PHP 5.4.41 or 5.5.25 or 5.6.9 or later.

Result:

Installed Version: 5.4.16 Fixed Version: 5.4.41

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=69085,http://openwall.com/lists/oss-security/2015/06/01/4

Unique Alert ID: 539075 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - Dec18 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2018-19518,CVE-2018-20783,CVE-2018-19396		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to multiple security vulnerabilities. The flaws exist due to: - the imap_open functions which allows to run arbitrary shell commands via mailbox parameter. - a Heap Buffer Overflow (READ: 4) in phar_parse_pharfile. - ext/standard/var_unserializer.c allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class. Successful exploitation will allow remote attackers to execute remote code on the affected application/system and/or cause a cause a denial of service.

Solution:

VendorFix Update to version 5.6.39, 7.0.33, 7.1.25, 7.2.13, 7.3.0 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.39 Installation path / port: 80/tcp

References:

- https://bugs.php.net/bug.php?id=76428,https://bugs.php.net/bug.php?id=77153,https://bugs.php.net/bug.php?id=7

7160,https://bugs.php.net/bug.php?id=77143,https://github.com/Bo0oM/PHP_imap_open_exploit/blob/master/exploit.php,https://www.exploit-db.com/exploits/45914/,https://www.openwall.com/lists/oss-security/2018/11/22/3

Unique Alert ID: 539073 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - Dec18 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2018-19518,CVE-2018-20783,CVE-2018-19396	
Cvss Base:	7.5	
Cvss Score:	7.5	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	

Description:

PHP is prone to multiple security vulnerabilities. The flaws exist due to: - the imap_open functions which allows to run arb itrary shell commands via mailbox parameter. - a Heap Buffer Overflow (READ: 4) in phar_parse_pharfile. - ext/standard /var_unserializer.c allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dot net, or variant class. Successful exploitation will allow remote attackers to execute remote code on the affected applicatio n/system and/or cause a cause a denial of service.

Solution:

VendorFix Update to version 5.6.39, 7.0.33, 7.1.25, 7.2.13, 7.3.0 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.39 Installation path / port: 443/tcp

References:

- https://bugs.php.net/bug.php?id=76428,https://bugs.php.net/bug.php?id=77153,https://bugs.php.net/bug.php?id=77160,https://bugs.php.net/bug.php?id=77143,https://github.com/Bo0oM/PHP_imap_open_exploit/blob/master/exploit.php,https://www.exploit-db.com/exploits/45914/,https://www.openwall.com/lists/oss-security/2018/11/22/3

Unique Alert ID: 539111 Found on: 2023-10-06 Severity: High

PHP Out of Bounds Read Multiple Vulnerabilities - Jan15 (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2014-9427	
Cvss Base:	7.5	
Cvss Score:	7.5	

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to an out-of-bounds read error in sapi/cgi/cgi_mai n.c in the CGI component in PHP. Successful exploitation will allow remote attackers to obtain sensitive information and tr igger unexpected code execution .

Solution:

VendorFix Update to PHP version 5.4.37 or 5.5.21 or 5.6.5 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.37/5.5.21/5.6.5

References:

- https://bugs.php.net/bug.php?id=68618

Unique Alert ID: 539110 Found on: 2023-10-06 Severity: High

PHP Out of Bounds Read Multiple Vulnerabilities - Jan15 (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-9427
Cvss Base: 7.5
Cvss Score: 7.5

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to an out-of-bounds read error in sapi/cgi/cgi_main.c in the CGI component in PHP. Successful exploitation will allow remote attackers to obtain sensitive information and trigger unexpected code execution .

Solution:

VendorFix Update to PHP version 5.4.37 or 5.5.21 or 5.6.5 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.37/5.5.21/5.6.5

References:

- https://bugs.php.net/bug.php?id=68618

Unique Alert ID: 539109 Found on: 2023-10-06 Severity: High

PHP Remote Code Execution and Denial of Service Vulnerabilities - Dec13 (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2013-6420
Cvss Base: 7.5
Cvss Score: 7.5

Description:

PHP is prone to a remote code execution (RCE) vulnerability. The flaw is due to a boundary error within the 'asn1_time_to_time_t' function in 'ext/openssl/openssl.c' when parsing X.509 certificates. Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption).

Solution:

VendorFix Update to PHP version 5.3.28 or 5.4.23 or 5.5.7 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.3.28/5.4.23/5.5.7

References:

- http://secunia.com/advisories/56055,http://packetstormsecurity.com/files/124436/PHP-openssl_x509_parse-Memory-Corruption.html

Unique Alert ID: 539108 Found on: 2023-10-06 Severity: High

PHP Remote Code Execution and Denial of Service Vulnerabilities - Dec13 (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2013-6420
Cvss Base: 7.5
Cvss Score: 7.5

Description:

PHP is prone to a remote code execution (RCE) vulnerability. The flaw is due to a boundary error within the 'asn1_time_t

o_time_t' function in 'ext/openssl/openssl.c' when parsing X.509 certificates. Successful exploitation will allow remote atta ckers to execute arbitrary code or cause a denial of service (memory corruption).

Solution:

VendorFix Update to PHP version 5.3.28 or 5.4.23 or 5.5.7 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.3.28/5.4.23/5.5.7

References:

- http://secunia.com/advisories/56055,http://packetstormsecurity.com/files/124436/PHP-openssl_x509_parse-Memor y-Corruption.html

Unique Alert ID: 539102 Found on: 2023-10-06 Severity: High

PHP Use-After-Free Remote Code EXecution Vulnerability - Jan15 (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-8142
Cvss Base: 7.5
Cvss Score: 7.5

Description:

PHP is prone to a use-after-free vulnerability. The flaw is due to Use-after-free vulnerability in the process_nested_data f unction in ext/standard/var _unserializer.re in PHP. Successful exploitation will allow remote attackers to execute arbitrar y code via a crafted unserialize call.

Solution:

VendorFix Update to PHP version 5.4.36 or 5.5.20 or 5.6.4 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.36/5.5.20/5.6.4

References:

- http://php.net/ChangeLog-5.php,http://secunia.com/advisories/60920,https://bugs.php.net/bug.php?id=68594

Unique Alert ID: 919548 Found on: 2023-10-06 Severity: High

OpenSSL: Read Buffer Overruns Processing ASN.1 Strings (20210824) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-3712
Cvss Base: 7.4
Cvss Score: 7.4
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H

Description:

OpenSSL is prone to a buffer overflow vulnerability. ASN.1 strings are represented internally within OpenSSL as an ASN1 _STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are represented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own 'd2i' functions (and other similar parsing fun ctions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL termina te the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_ STRING structures which do not NUL terminate the byte array by directly setting the 'data' and 'length' fields in the ASN1 _STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that prin t ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is n ot guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be pri nted, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application with out NUL terminating the 'data' field, then a read buffer overrun can occur. The same thing can also occur during name co nstraints processing of certificates (for example if a certificate has been directly constructed by the application instead of

loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). I t can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext).

Solution:

VendorFix Update to version 1.0.2za, 1.1.1l or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2za / 1.1.1l Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20210824.txt

Unique Alert ID: 919547 Found on: 2023-10-06 Severity: High

OpenSSL: Read Buffer Overruns Processing ASN.1 Strings (20210824) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-3712
Cvss Base: 7.4
Cvss Score: 7.4
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H

Description:

OpenSSL is prone to a buffer overflow vulnerability. ASN.1 strings are represented internally within OpenSSL as an ASN1 _STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are represented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own 'd2i' functions (and other similar parsing fun ctions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL termina te the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_ STRING structures which do not NUL terminate the byte array by directly setting the 'data' and 'length' fields in the ASN1 _STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that prin t ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is n ot guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be pri nted, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application with out NUL terminating the 'data' field, then a read buffer overrun can occur. The same thing can also occur during name co nstraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). I t can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext).

Solution:

VendorFix Update to version 1.0.2za, 1.1.1l or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2za / 1.1.1l Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20210824.txt

Unique Alert ID: 539138 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Mar16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-6831,CVE-2015-6832,CVE-2015-6833		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - The multiple use-after-free vulnerabilities in SPL unser ialize implementation. - An insufficient validation of user supplied input by 'phar/phar_object.c' script. Successfully exploit ing this issue allow remote attackers to execute arbitrary code and to create or overwrite arbitrary files on the system an d this may lead to launch further attacks.

Solution:

VendorFix Update to PHP version 5.4.44 or 5.5.28 or 5.6.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.44

References:

- https://bugs.php.net/bug.php?id=70068,http://www.openwall.com/lists/oss-security/2015/08/19/3

Unique Alert ID: 539136 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Mar16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-6831,CVE-2015-6832,CVE-2015-6833		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - The multiple use-after-free vulnerabilities in SPL unser ialize implementation. - An insufficient validation of user supplied input by 'phar/phar_object.c' script. Successfully exploit ing this issue allow remote attackers to execute arbitrary code and to create or overwrite arbitrary files on the system an d this may lead to launch further attacks.

Solution:

VendorFix Update to PHP version 5.4.44 or 5.5.28 or 5.6.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.44

References:

- https://bugs.php.net/bug.php?id=70068,http://www.openwall.com/lists/oss-security/2015/08/19/3

Unique Alert ID: 539107 Found on: 2023-10-06 Severity: High

PHP 'serialize_function_call' Function Type Confusion Vulnerability - Mar16 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-6836
Cvss Base: 7.3
Cvss Score: 7.3
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Description:

PHP is prone to a remote code execution (RCE) vulnerability. The flaw is due to 'SoapClient __call' method in 'ext/soap/soap.c' scripr does not properly manage headers. Successfully exploiting this issue allow remote attackers to execute arbitrary code in the context of the user running the affected application. Failed exploit attempts will likely cause a denial-of-service condition.

Solution:

VendorFix Update to PHP version 5.4.45, or 5.5.29, or 5.6.13 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.45

References:

- http://www.php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=70388

Unique Alert ID: 539106 Found on: 2023-10-06 Severity: High

PHP 'serialize_function_call' Function Type Confusion Vulnerability - Mar16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-6836
Cvss Base: 7.3
Cvss Score: 7.3
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Description:

PHP is prone to a remote code execution (RCE) vulnerability. The flaw is due to 'SoapClient __call' method in 'ext/soap/soap.c' scripr does not properly manage headers. Successfully exploiting this issue allow remote attackers to execute arbitrary code in the context of the user running the affected application. Failed exploit attempts will likely cause a denial-of-service condition.

Solution:

VendorFix Update to PHP version 5.4.45, or 5.5.29, or 5.6.13 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.45

References:

- http://www.php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=70388

Unique Alert ID: 539157 Found on: 2023-10-06 Severity: High

OpenSSH Multiple Vulnerabilities Jan17 (Linux) (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-10009,CVE-2016-10010,CVE-2016-10011,CVE-2016-10012,CVE-2016-10708

Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

openssh is prone to multiple vulnerabilities. Multiple flaws exist due to: - An 'authfile.c' script does not properly consider t he effects of realloc on buffer contents. - The shared memory manager (associated with pre-authentication compression) does not ensure that a bounds check is enforced by all compilers. - The sshd in OpenSSH creates forwarded Unix-domain sockets as root, when privilege separation is not used. - An untrusted search path vulnerability in ssh-agent.c in ssh-agen t. - NULL pointer dereference error due to an out-of-sequence NEWKEYS message. Successfully exploiting this issue allow s local users to obtain sensitive private-key information, to gain privileges, conduct a senial-of-service condition and allo ws remote attackers to execute arbitrary local PKCS#11 modules.

Solution:

VendorFix Upgrade to OpenSSH version 7.4 or later.

Result:

Installed version: 6.6.1 Fixed version: 7.4 Installation path / port: 22/tcp

References:

- https://www.openssh.com/txt/release-7.4,http://www.openwall.com/lists/oss-security/2016/12/19/2,http://blog.swiecki.net/2018/01/fuzzing-tcp-servers.html,https://anongit.mindrot.org/openssh.git/commit/?id=28652bca29046f62c7045e933e6b931de1d16737

Unique Alert ID: 539163 Found on: 2023-10-06 Severity: High

PHP 'FastCGI Process Manager' Privilege Escalation Vulnerability (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-0185
Cvss Base: 7.2
Cvss Score: 7.2

Description:

PHP is prone to a privilege escalation vulnerability. The flaw is due to error in 'sapi/fpm/fpm/fpm_unix.c' within FastCGI P rocess Manager that sets insecure permissions for a unix socket. Successful exploitation will allow remote attackers to ga in access to the socket and gain elevated privileges.

Solution:

VendorFix Update to PHP version 5.4.28 or 5.5.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.28/5.5.12

References:

- http://seclists.org/oss-sec/2014/q2/192,http://www.php.net/archive/2014.php#id2014-05-01-1,http://www.openwall.com/lists/oss-security/2014/04/29/5

Unique Alert ID: 539165 Found on: 2023-10-06 Severity: High

PHP 'FastCGI Process Manager' Privilege Escalation Vulnerability (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-0185
Cvss Base: 7.2
Cvss Score: 7.2

Description:

PHP is prone to a privilege escalation vulnerability. The flaw is due to error in 'sapi/fpm/fpm/fpm_unix.c' within FastCGI P rocess Manager that sets insecure permissions for a unix socket. Successful exploitation will allow remote attackers to ga in access to the socket and gain elevated privileges.

Solution:

VendorFix Update to PHP version 5.4.28 or 5.5.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.28/5.5.12

References:

- http://seclists.org/oss-sec/2014/q2/192,http://www.php.net/archive/2014.php#id2014-05-01-1,http://www.openwall .com/lists/oss-security/2014/04/29/5

Unique Alert ID: 539201 Found on: 2023-10-06 Severity: High

PHP 'make_http_soap_request' DoS / Information Disclosure Vulnerability - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-3185
Cvss Base: 7.1
Cvss Score: 7.1
Cvss Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) and an information disclosure vulnerability. The flaw is due an error in the 'mak e_http_soap_request' function of the 'ext/soap/php_http.c' script. Successfully exploiting this issue allow remote attacker s to obtain sensitive information from process memory or cause a denial of service.

Solution:

VendorFix Update to version 5.4.44, 5.5.28, 5.6.12, 7.0.4 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.44

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539198 Found on: 2023-10-06 Severity: High

PHP 'make_http_soap_request' DoS / Information Disclosure Vulnerability - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-3185
Cvss Base: 7.1
Cvss Score: 7.1
Cvss Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) and an information disclosure vulnerability. The flaw is due an error in the 'make_http_soap_request' function of the 'ext/soap/php_http.c' script. Successfully exploiting this issue allow remote attackers to obtain sensitive information from process memory or cause a denial of service.

Solution:

VendorFix Update to version 5.4.44, 5.5.28, 5.6.12, 7.0.4 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.44

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 919551 Found on: 2023-10-06 Severity: High

OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability (tcp/22)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2021-41617		
Cvss Base:	7.0		
Cvss Score:	7.0		
Cvss Vector:	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H		

Description:

OpenSSH is prone to a privilege scalation vulnerability in certain configurations. sshd failed to correctly initialise supplemental groups when executing an AuthorizedKeysCommand or AuthorizedPrincipalsCommand, where a AuthorizedKeysCommandUser or AuthorizedPrincipalsCommandUser directive has been set to run the command as a different user. Instead these commands would inherit the groups that sshd was started with. Depending on system configuration, inherited groups may allow AuthorizedKeysCommand/AuthorizedPrincipalsCommand helper programs to gain unintended privilege. Neither AuthorizedKeysCommand nor AuthorizedPrincipalsCommand are enabled by default in sshd_config.

Solution:

VendorFix Update to version 8.8 or later.

Result:

Installed version: 6.6.1 Fixed version: 8.8 Installation path / port: 22/tcp

References:

- https://www.openssh.com/txt/release-8.8

Unique Alert ID: 919550 Found on: 2023-10-06 Severity: High

PHP 5.3.7 - 7.3.31, 7.4.x < 7.4.25, 8.0.x < 8.0.12 Security Update (Oct 2021) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2021-21703		
Cvss Base:	7.0		
Cvss Score:	7.0		
Cvss Vector:	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP released new versions which includes a security fix. Fixed bug #81026 (PHP-FPM oob R/W in root process leading to privilege escalation).

Solution:

VendorFix Update to version 7.3.32 (not released yet), 7.4.25, 8.0.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.32 (not released yet) Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.32,https://www.php.net/ChangeLog-7.php#7.4.25,https://www.php.net/ChangeLog-8.php#8.0.12,http://bugs.php.net/81026,https://www.ambionics.io/blog/php-fpm-local-root

Unique Alert ID: 919549 Found on: 2023-10-06 Severity: High

PHP 5.3.7 - 7.3.31, 7.4.x < 7.4.25, 8.0.x < 8.0.12 Security Update (Oct 2021) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2021-21703		
Cvss Base:	7.0		
Cvss Score:	7.0		
Cvss Vector:	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP released new versions which includes a security fix. Fixed bug #81026 (PHP-FPM oob R/W in root process leading to privilege escalation).

Solution:

VendorFix Update to version 7.3.32 (not released yet), 7.4.25, 8.0.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.32 (not released yet) Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.32,https://www.php.net/ChangeLog-7.php#7.4.25,https://www.php.net/ChangeLog-8.php#8.0.12,http://bugs.php.net/81026,https://www.ambionics.io/blog/php-fpm-local-root

Unique Alert ID: 539088 Found on: 2023-10-06 Severity: High

PHP Directory Traversal Vulnerability - Jul16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-9767,CVE-2015-6834,CVE-2015-6835,CVE-2015-6837,CVE-2015-6838		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to a directory traversal vulnerability. Multiple flaws are due to - An error in the 'ZipArchive::extractTo' function in 'ext/zip/php_zip.c' script. - The xsl_ext_function_php function in ext/xsl/xsltprocessor.c when libxml2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation after the principal argument loop. - Improper handling of multiple php_var_unserialize calls. - Multiple use-after-free vulnerabilities. Successfully exploiting this issue allow remote attackers to read arbitrary empty directories, also to cause a denial of service.

Solution:

VendorFix Update to PHP version 5.4.45, or 5.5.29, or 5.6.13, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.45

References:

- http://www.php.net/ChangeLog-5.php,http://www.openwall.com/lists/oss-security/2016/03/16/20

Unique Alert ID: 539090 Found on: 2023-10-06 Severity: High

PHP Directory Traversal Vulnerability - Jul16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-9767,CVE-2015-6834,CVE-2015-6835,CVE-2015-6837,CVE-2015-6838		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to a directory traversal vulnerability. Multiple flaws are due to - An error in the 'ZipArchive::extractTo' functi on in 'ext/zip/php_zip.c' script. - The xsl_ext_function_php function in ext/xsl/xsltprocessor.c when libxml2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation after the principal ar gument loop. - Improper handling of multiple php_var_unserialize calls. - Multiple use-after-free vulnerabilities. Successf ully exploiting this issue allow remote attackers to read arbitrary empty directories, also to cause a denial of service.

Solution:

VendorFix Update to PHP version 5.4.45, or 5.5.29, or 5.6.13, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.45

References:

- http://www.php.net/ChangeLog-5.php,http://www.openwall.com/lists/oss-security/2016/03/16/20

Unique Alert ID: 539122 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 03 - Sep16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-7412,CVE-2016-7413,CVE-2016-7414,CVE-2016-7416,CVE-2016-7417,CVE-2016-7418		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Use-after-free vulnerability in the 'wddx_stack_destro y' function in 'ext/wddx/wddx.c' script. - Improper verification of a BIT field has the UNSIGNED_FLAG flag in 'ext/mysqlnd /mysqlnd_wireprotocol.c' script. - The ZIP signature-verification feature does not ensure that the uncompressed_filesize f ield is large enough. - The script 'ext/spl/spl_array.c' proceeds with SplArray unserialization without validating a return v alue and data type. - The script 'ext/intl/msgformat/msgformat_format.c' does not properly restrict the locale length prov ided to the Locale class in the ICU library. - An error in the php_wddx_push_element function in ext/wddx/wddx.c. Succe ssfully exploiting this issue allow remote attackers to cause a denial of service, or possibly have unspecified other impact .

Solution:

VendorFix Update to PHP version 5.6.25, or 7.0.10, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.26

References:

- http://www.php.net/ChangeLog-7.php,http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539123 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 03 - Sep16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-7412,CVE-2016-7413,CVE-2016-7414,CVE-2016-7416,CVE-2016-7417,CVE-2016-7418		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Use-after-free vulnerability in the 'wddx_stack_destroy' function in 'ext/wddx/wddx.c' script. - Improper verification of a BIT field has the UNSIGNED_FLAG flag in 'ext/mysqlnd/mysqlnd_wireprotocol.c' script. - The ZIP signature-verification feature does not ensure that the uncompressed_filesize field is large enough. - The script 'ext/spl/spl_array.c' proceeds with SplArray unserialization without validating a return value and data type. - The script 'ext/intl/msgformat/msgformat_format.c' does not properly restrict the locale length provided to the Locale class in the ICU library. - An error in the php_wddx_push_element function in ext/wddx/wddx.c. Successfully exploiting this issue allow remote attackers to cause a denial of service, or possibly have unspecified other impact .

Solution:

VendorFix Update to PHP version 5.6.25, or 7.0.10, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.26

References:

- http://www.php.net/ChangeLog-7.php,http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539126 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 02 - Sep16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-7124,CVE-2016-7125,CVE-2016-7126,CVE-2016-7127,CVE-2016-7128,CVE-2016-7129,CVE-2016-7130,CVE-2016-7131,CVE-2016-7132		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to - An invalid wddxPacket XML document that is mishandled in a wddx_deserialize call in 'ext/wddx/wddx.c' script. - An error in 'php_wddx_pop_element' function in 'ext/wddx/wddx.c' script. - An error in 'php_wddx_process_data' function in 'ext/wddx/wddx.c' script. - Improper handling of the case of a thumbnail offset that exceeds the file size in 'exif_process_IFD_in_TIFF' function in 'ext/exif/exif.c' script. - Improper validation of gamma values in 'imagegammacorrect' function in 'ext/gd/gd.c' script. - Improper validation of number of colors in 'imagegammacorrect' function in 'ext/gd/gd.c' script. - The script 'ext/session/session.c' skips invalid session names in a way that triggers incorrect parsing. - Improper handling of certain objects in 'ext/standard/var_unserializer.c' script. Successfully exploiting this issue allow remote attackers to cause a denial of service, to obtain sensitive information from process memory, to inject arbitrary-type session data by leveraging control of a session name.

Solution:

VendorFix Update to PHP version 5.6.25, or 7.0.10, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.25

References:

- http://www.php.net/ChangeLog-7.php,http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539129 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 02 - Sep16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-7124,CVE-2016-7125,CVE-2016-7126,CVE-2016-7127,CVE-2016-7128,CVE-2016-7129,CVE-2016-7130,CVE-2016-7131,CVE-2016-7132	
Cvss Base:	7.5	
Cvss Score:	7.5	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to - An invalid wddxPacket XML document that is mishandle d in a wddx_deserialize call in 'ext/wddx/wddx.c' script. - An error in 'php_wddx_pop_element' function in 'ext/wddx/wdd x.c' script. - An error in 'php_wddx_process_data' function in 'ext/wddx/wddx.c' script. - Improper handling of the case of a thumbnail offset that exceeds the file size in 'exif_process_IFD_in_TIFF' function in 'ext/exif/exif.c' script. - Improper va lidation of gamma values in 'imagegammacorrect' function in 'ext/gd/gd.c' script. - Improper validation of number of colo rs in 'imagegammacorrect' function in 'ext/gd/gd.c' script. - The script 'ext/session/session.c' skips invalid session names in a way that triggers incorrect parsing. - Improper handling of certain objects in 'ext/standard/var_unserializer.c' script. Successfully exploiting this issue allow remote attackers to cause a denial of service, to obtain sensitive information from process memory, to inject arbitrary-type session data by leveraging control of a session name.

Solution:

VendorFix Update to PHP version 5.6.25, or 7.0.10, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.25

References:

- http://www.php.net/ChangeLog-7.php,http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539137 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Jul16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-4070,CVE-2016-4071,CVE-2016-4072,CVE-2016-4073,CVE-2015-8865	
Cvss Base:	7.3	
Cvss Score:	7.3	
Cvss Vector:	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Multiple integer overflows in the mbfl_strcut function in 'ext/mbstring/libmbfl/mbfl/mbfilter.c' script. - A format string vulnerability in the php_snmp_error function in 'ext/snmp/s nmp.c' script. - An improper handling of '\0' characters by the 'phar_analyze_path' function in 'ext/phar/phar.c' script. - A n integer overflow in the 'php_raw_url_encode' function in 'ext/standard/url.c' script. - An improper handling of continuati on-level jumps in 'file_check_mem' function in 'funcs.c' script. Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code.

Solution:

VendorFix Update to PHP version 5.5.34, or 5.6.20, or 7.0.5, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.34

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539140 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Jul16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-4070,CVE-2016-4071,CVE-2016-4072,CVE-2016-4073,CVE-2015-8865	
Cvss Base:	7.3	
Cvss Score:	7.3	
Cvss Vector:	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Multiple integer overflows in the mbfl_strcut function in 'ext/mbstring/libmbfl/mbfl/mbfilter.c' script. - A format string vulnerability in the php_snmp_error function in 'ext/snmp/snmp.c' script. - An improper handling of '\0' characters by the 'phar_analyze_path' function in 'ext/phar/phar.c' script. - An integer overflow in the 'php_raw_url_encode' function in 'ext/standard/url.c' script. - An improper handling of continuation-level jumps in 'file_check_mem' function in 'funcs.c' script. Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code.

Solution:

VendorFix Update to PHP version 5.5.34, or 5.6.20, or 7.0.5, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.34

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539145 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Aug16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-5773,CVE-2016-5772,CVE-2016-5769,CVE-2016-5768,CVE-2016-5766,CVE-2016-5767	
Cvss Base:	8.8	
Cvss Score:	8.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - The 'php_zip.c' script in the zip extension improperly interacts with the unserialize implementation and garbage collection. - The php_wddx_process_data function in 'wddx.c' script in the WDDX extension mishandled data in a wddx_deserialize call. - The multiple integer overflows in 'mcrypt.c' script in the mcrypt extension. - The double free vulnerability in the '_php_mb_regex_ereg_replace_exec' function in 'php_mbregex.c' script in the mbstring extension. - An integer overflow in the '_gd2GetHeader' function in 'gd_gd2.c' script in the GD Graphics Library. - An integer overflow in the 'gdImageCreate' function in 'gd.c' script in the GD Graphics Library. Successfully exploiting this issue allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code.

Solution:

VendorFix Update to PHP version 5.5.37, or 5.6.23, or 7.0.8, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.37

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539148 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Aug16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-5773,CVE-2016-5772,CVE-2016-5769,CVE-2016-5768,CVE-2016-5766,CVE-2016-5767	
Cvss Base:	8.8	
Cvss Score:	8.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - The 'php_zip.c' script in the zip extension improperly i nteracts with the unserialize implementation and garbage collection. - The php_wddx_process_data function in 'wddx.c' sc ript in the WDDX extension mishandled data in a wddx_deserialize call. - The multiple integer overflows in 'mcrypt.c' scri pt in the mcrypt extension. - The double free vulnerability in the '_php_mb_regex_ereg_replace_exec' function in 'php_m bregex.c' script in the mbstring extension. - An integer overflow in the '_gd2GetHeader' function in 'gd_gd2.c' script in the GD Graphics Library. - An integer overflow in the 'gdImageCreate' function in 'gd.c' script in the GD Graphics Library. Su ccessfully exploiting this issue allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code.

Solution:

VendorFix Update to PHP version 5.5.37, or 5.6.23, or 7.0.8, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.37

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539239 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities (Nov 2016) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-8670,CVE-2016-9933,CVE-2016-9934,CVE-2016-10397	
Cvss Base:	7.5	
Cvss Score:	7.5	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N	

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - CVE-2016-8670: Stack Buffer Overflow in GD dynamic Getbuf - CVE-2016-9933, CVE-2016-9934: Multiple denial of service (DoS) vulnerabilities - CVE-2016-10397: Security by pass vulnerability

Solution:

VendorFix Update to version 5.6.28, 7.0.13 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.28 Installation path / port: 443/tcp

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php,http://bugs.php.net/73280,http://bugs.php.net/72696,http://bugs.php.net/73331,http://bugs.php.net/73192

Unique Alert ID: 539240 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities (Nov 2016) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-8670,CVE-2016-9933,CVE-2016-9934,CVE-2016-10397		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N		

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - CVE-2016-8670: Stack Buffer Overflow in GD dynamic Getbuf - CVE-2016-9933, CVE-2016-9934: Multiple denial of service (DoS) vulnerabilities - CVE-2016-10397: Security by pass vulnerability

Solution:

VendorFix Update to version 5.6.28, 7.0.13 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.28 Installation path / port: 80/tcp

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php,http://bugs.php.net/73280,http://bugs.php.net/72696,http://bugs.php.net/73331,http://bugs.php.net/73192

Unique Alert ID: 539114 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities (Jul 2016 - 05) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-6288,CVE-2016-6289,CVE-2016-6290,CVE-2016-6291,CVE-2016-6292,CVE-2016-6294,CVE-2016-6295,CVE-2016-6296,CVE-2016-6297,CVE-2016-6207,CVE-2016-5399		
Cvss Base:	7.8		
Cvss Score:	7.8		
Cvss Vector:	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws exist due to - An integer overflow in the 'php_stream_zip_opener' function in 'ext/zip/zip_stream.c' - An integer signedness error in the 'simplestring_addn' function in 'simplestring.c' in xmlrpc-epi - 'ext/snmp/snmp.c' improperly interacts with the unserialize implementation and garbage collection - The 'locale_accept_from_http' function in 'ext/intl/locale/locale_methods.c' does not properly restrict calls to the ICU 'uloc_acceptLanguageFromHTTP' function - An error in the 'exif_process_user_comment' function of 'ext/exif/exif.c' - An error in the 'exif_process_IFD_in_MAKERNOTE' function of 'ext/exif/exif.c' - 'ext/session/session.c' does not properly maintain a certain hash data structure - An integer overflow in the 'virtual_file_ex' function of 'TSRM/tsrm_virtual_cwd.c' - An error in the 'php_url_parse_ex' function of 'ext/standard/url.c' - Integer overflow error within _gdContributionsAlloc() - Inadequate error handling in bzread() Successfully exploiting these issues may allow attackers to cause a denial of service obtain sensitive information from process memory, or possibly have unspecified other impact.

Solution:

VendorFix Update to version 5.5.38, 5.6.24, 7.0.9, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.38 Installation path / port: 443/tcp

References:

- http://php.net/ChangeLog-5.php,http://php.net/ChangeLog-7.php,http://openwall.com/lists/oss-security/2016/07/24/2

Unique Alert ID: 539115 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities (Jul 2016 - 05) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-6288,CVE-2016-6289,CVE-2016-6290,CVE-2016-6291,CVE-2016-6292,CVE-2016-6294,CVE-2016-6295,CVE-2016-6296,CVE-2016-6297,CVE-2016-6207,CVE-2016-5399		
Cvss Base:	7.8		
Cvss Score:	7.8		
Cvss Vector:	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws exist due to - An integer overflow in the 'php_stream_zip_opener' function in 'ext/zip/zip_stream.c' - An integer signedness error in the 'simplestring_addn' function in 'simplestring.c' in xmlrpc-epi - 'ext/snmp/snmp.c' improperly interacts with the unserialize implementation and garbage collection - The 'locale_accept_from_http' function in 'ext/intl/locale/locale_methods.c' does not properly restrict calls to the ICU 'uloc_acceptLanguageFromHTTP' function - An error in the 'exif_process_user_comment' function of 'ext/exif/exif.c' - An error in the 'exif_process_IFD_in_MAKERNOTE' function of 'ext/exif/exif.c' - 'ext/session/session.c' does not properly maintain a certain hash data structure - An integer overflow in the 'virtual_file_ex' function of 'TSRM/tsrm_virtual_cwd.c' - An error in the 'php_url_parse_ex' function of 'ext/standard/url.c' - Integer overflow error within _gdContributionsAlloc() - Inadequate error handling in bzread() Successfully exploiting these issues may allow attackers to cause a denial of service obtain sensitive information from process memory, or possibly have unspecified other impact.

Solution:

VendorFix Update to version 5.5.38, 5.6.24, 7.0.9, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.38 Installation path / port: 80/tcp

References:

- http://php.net/ChangeLog-5.php,http://php.net/ChangeLog-7.php,http://openwall.com/lists/oss-security/2016/07/24/2

Unique Alert ID: 539279 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities (Jan 2017 - 02) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-10161,CVE-2016-10158,CVE-2016-10168,CVE-2016-10167,CVE-2017-11147,CVE-2016-10160,CVE-2016-10159		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - Fixed bug #73825 (Heap out of bounds read on unserialize in finish_nested_data()). (CVE-2016-10161) - Fixed bug #73737 (FPE when parsing a tag format). (CVE-2016-10158) - Fixed bug #73869 (Signed Integer Overflow gd_io.c). (CVE-2016-10168) - Fixed bug #73868 (DOS vulnerability in gdImageCreateFromGd2Ctx()). (CVE-2016-10167) - Fixed bug #73773 (Seg fault when loading hostile phar). (CVE-2017-11147) - Fixed bug #73768 (Memory corruption when loading hostile phar). (CVE-2016-10160) - Fixed bug #73764 (Crash while loading hostile phar archive). (CVE-2016-10159)

Solution:

VendorFix Update to version 5.6.30, 7.0.15, 7.1.1 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.30 Installation path / port: 443/tcp

References:

- http://bugs.php.net/73737,http://bugs.php.net/73869,http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php,http://bugs.php.net/73825,http://bugs.php.net/73868,http://bugs.php.net/73773,http://bugs.php.net/73768,http://bugs.php.net/73764

Unique Alert ID: 539280 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities (Jan 2017 - 02) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-10161,CVE-2016-10158,CVE-2016-10168,CVE-2016-10167,CVE-2017-11147,CVE-2016-10160,CVE-2016-10159	
Cvss Base:	7.5	
Cvss Score:	7.5	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - Fixed bug #73825 (Heap out of bounds read on unserialize in finish_nested_data()). (CVE-2016-10161) - Fixed bug #73737 (FPE when parsing a tag format). (CVE-2016-10158) - Fixed bug #73869 (Signed Integer Overflow gd_io.c). (CVE-2016-10168) - Fixed bug #73868 (DOS vulnerability in gdImageCreateFromGd2Ctx()). (CVE-2016-10167) - Fixed bug #73773 (Seg fault when loading hostile phar). (CVE-2017-11147) - Fixed bug #73768 (Memory corruption when loading hostile phar). (CVE-2016-10160) - Fixed bug #73764 (Crash while loading hostile phar archive). (CVE-2016-10159)

Solution:

VendorFix Update to version 5.6.30, 7.0.15, 7.1.1 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.30 Installation path / port: 80/tcp

References:

- http://bugs.php.net/73737,http://bugs.php.net/73869,http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php,http://bugs.php.net/73825,http://bugs.php.net/73868,http://bugs.php.net/73773,http://bugs.php.net/73768,http://bugs.php.net/73764

Unique Alert ID: 539112 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities (Feb 2019) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-10166,CVE-2019-9020,CVE-2019-9021,CVE-2019-9023,CVE-2019-9024,CVE-2019-6977	
Cvss Base:	8.8	
Cvss Score:	8.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - Fixed bug #77269 (efree() on uninitialized Heap data in imagescale leads to use-after-free). (CVE-2016-10166) - Fixed bug #77270 (imagecolormatch Out Of Bounds Write on Heap). (CVE-2019-6977) - Fixed bug #77370 (Buffer overflow on mb regex functions - fetch_token). (CVE-2019-9023) - Fixed bug #77371 (heap buffer overflow in mb regex functions - compile_string_node). (CVE-2019-9023) - Fixed bug #77381 (heap buffer overflow in multibyte match_at). (CVE-2019-9023) - Fixed bug #77382 (heap buffer overflow due to incorrect length in expand_case_fold_string). (CVE-2019-9023) - Fixed bug #77385 (buffer overflow in fetch_token). (CVE-2019-9023) - Fixed bug #77394 (Buffer overflow in multibyte case folding - unicode). (CVE-2019-9023) - Fixed bug #77418 (Heap overflow in utf32be_mbc_to_code). (CVE-2019-9023) - Fixed bug #77247 (heap buffer overflow in phar_detect_phar_fname_ext). (CVE-2019-9021) - Fixed bug #77242 (heap out of bounds read in xmlrpc_decode()). (CVE-2019-9020) - Fixed bug #77380 (Global out of bounds read in xmlrpc base64 code). (CVE-2019-9024)

Solution:

VendorFix Update to version 5.6.40, 7.1.16, 7.2.14, 7.3.1 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.40 Installation path / port: 443/tcp

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php,https://bugs.php.net/bug.php?id=77269,https://bugs.php.net/bug.php?id=77270,https://bugs.php.net/bug.php?id=77370,https://bugs.php.net/bug.php?id=77371,https://bugs.php.net/bug.php?id=77381,https://bugs.php.net/bug.php?id=77382,https://bugs.php.net/bug.php?id=77385,https://bugs.php.net/bug.php?id=77394,https://bugs.php.net/bug.php?id=77418,https://bugs.php.net/bug.php?id=77247,https://bugs.php.net/bug.php?id=77242,https://bugs.php.net/bug.php?id=77380

Unique Alert ID: 539113 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities (Feb 2019) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-10166,CVE-2019-9020,CVE-2019-9021,CVE-2019-9023,CVE-2019-9024,CVE-2019-6977	
Cvss Base:	8.8	
Cvss Score:	8.8	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - Fixed bug #77269 (efree() on uninitialized Heap data in imagescale leads to use-after-free). (CVE-2016-10166) - Fixed bug #77270 (imagecolormatch Out Of Bounds Write on Heap). (CVE-2019-6977) - Fixed bug #77370 (Buffer overflow on mb regex functions - fetch_token). (CVE-2019-9023) - Fixed bug #77371 (heap buffer overflow in mb regex functions - compile_string_node). (CVE-2019-9023) - Fixed bug #77381 (heap buffer overflow in multibyte match_at). (CVE-2019-9023) - Fixed bug #77382 (heap buffer overflow due to incorrect length in expand_case_fold_string). (CVE-2019-9023) - Fixed bug #77385 (buffer overflow in fetch_token). (CVE-2019-9023) - Fixed bug #77394 (Buffer overflow in multibyte case folding - unicode). (CVE-2019-9023) - Fixed bug #77418 (Heap overflow in utf32be_mbc_to_code). (CVE-2019-9023) - Fixed bug #77247 (heap buffer overflow in phar_detect_phar_fname_ext). (CVE-2019-9021) - Fixed bug #77242 (heap out of bounds read in xmlrpc_decode()). (CVE-2019-9020) - Fixed bug #77380 (Global out of bounds read in xmlrpc base64 code). (CVE-2019-9024)

Solution:

VendorFix Update to version 5.6.40, 7.1.16, 7.2.14, 7.3.1 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.40 Installation path / port: 80/tcp

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php,https://bugs.php.net/bug.php?id=77269,https://bugs.php.net/bug.php?id=77270,https://bugs.php.net/bug.php?id=77370,https://bugs.php.net/bug.php?id=77371,https://bugs.php.net/bug.php?id=77381,https://bugs.php.net/bug.php?id=77382,https://bugs.php.net/bug.php?id=77385,https://bugs.php.net/bug.php?id=77394,https://bugs.php.net/bug.php?id=77418,https://bugs.php.net/bug.php?id=77247,https://bugs.php.net/bug.php?id=77242,https://bugs.php.net/bug.php?id=77380

Unique Alert ID: 539172 Found on: 2023-10-06 Severity: High

PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-4343	
Cvss Base:	8.8	
Cvss Score:	8.8	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	

Description:

PHP is prone to denial of service and unspecified vulnerabilities. The flaw is due an improper handling of zero-size './/@LongLink' files by 'phar_make_dirstream' function in ext/phar/dirstream.c script. Successfully exploiting this issue allow remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.6.18, or 7.0.3, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.18

References:

- http://www.php.net/ChangeLog-5.php,http://www.openwall.com/lists/oss-security/2016/04/28/2

Unique Alert ID: 539189 Found on: 2023-10-06 Severity: High

PHP Denial of Service And Unspecified Vulnerabilities - 02 - Jul16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-4343
Cvss Base: 8.8
Cvss Score: 8.8
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Description:

PHP is prone to denial of service and unspecified vulnerabilities. The flaw is due an improper handling of zero-size './/@LongLink' files by 'phar_make_dirstream' function in ext/phar/dirstream.c script. Successfully exploiting this issue allow remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.6.18, or 7.0.3, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.18

References:

- http://www.php.net/ChangeLog-5.php,http://www.openwall.com/lists/oss-security/2016/04/28/2

Unique Alert ID: 539125 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 03 - Aug16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-5096,CVE-2016-5094,CVE-2016-5095
Cvss Base: 8.6
Cvss Score: 8.6
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - An integer overflow in the fread function in 'ext/standard/file.c' script. - An integer overflow in the php_html_entities function in 'ext/standard/html.c' script. - An Integer overflow in the php_escape_html_entities_ex function in 'ext/standard/html.c' script. Successfully exploiting this issue allow remote attackers to cause a denial of service or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.5.36, or 5.6.22, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.36

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539128 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 03 - Aug16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-5096,CVE-2016-5094,CVE-2016-5095	
Cvss Base:	8.6	
Cvss Score:	8.6	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - An integer overflow in the fread function in 'ext/standard/file.c' script. - An integer overflow in the php_html_entities function in 'ext/standard/html.c' script. - An Integer overflow in the php_escape_html_entities_ex function in 'ext/standard/html.c' script. Successfully exploiting this issue allow remote attackers to cause a denial of service or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.5.36, or 5.6.22, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.36

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539120 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 04 - Aug16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2013-7456,CVE-2016-5093	
Cvss Base:	8.6	
Cvss Score:	8.6	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - The 'get_icu_value_internal' function in 'ext/intl/locale/locale_methods.c' script does not ensure the presence of a '\0' character. - The 'gd_interpolation.c' script in the GD Graphics Library mishandled by the imagescale function. Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.5.36, or 5.6.22, or 7.0.7, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.36

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539121 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 04 - Aug16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2013-7456,CVE-2016-5093		
Cvss Base:	8.6		
Cvss Score:	8.6		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - The 'get_icu_value_internal' function in 'ext/intl/locale/locale_methods.c' script does not ensure the presence of a '\0' character. - The 'gd_interpolation.c' script in the GD Graphics Library mishandled by the imagescale function. Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.5.36, or 5.6.22, or 7.0.7, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.36

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539077 Found on: 2023-10-06 Severity: High

OpenSSH Multiple Vulnerabilities (tcp/22)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-6564,CVE-2015-6563,CVE-2015-5600		
Cvss Base:	8.5		
Cvss Score:	8.5		

Description:

OpenSSH is prone to multiple vulnerabilities. Multiple flaws are due to: - Use-after-free vulnerability in the 'mm_answer_pam_free_ctx' function in monitor.c in sshd. - Vulnerability in 'kbdint_next_device' function in auth2-chall.c in sshd. - Vulnerability in the handler for the MONITOR_REQ_PAM_FREE_CTX request. Successful exploitation will allow an attacker to gain privileges, to conduct impersonation attacks, to conduct brute-force attacks or cause a denial of service.

Solution:

VendorFix Upgrade to OpenSSH 7.0 or later.

Result:

Installed version: 6.6.1 Fixed version: 7.0 Installation path / port: 22/tcp

References:

- http://seclists.org/fulldisclosure/2015/Aug/54,http://openwall.com/lists/oss-security/2015/07/23/4

Unique Alert ID: 539284 Found on: 2023-10-06 Severity: High

OpenSSH Client Information Leak (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18

CVE ID: CVE-2016-0777,CVE-2016-0778
Cvss Base: 8.1
Cvss Score: 8.1
Cvss Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Description:

The OpenSSH client code between 5.4 and 7.1p1 contains experimental support for resuming SSH-connections (roaming) . The matching server code has never been shipped, but the client code was enabled by default and could be tricked by a malicious server into leaking client memory to the server, including private client user keys. The authentication of the ser ver host key prevents exploitation by a man-in-the-middle, so this information leak is restricted to connections to malicio us or compromised servers.

Solution:

VendorFix Update to 7.1p2 or newer.

Result:

Installed version: 6.6.1 Fixed version: 7.1p2 Installation path / port: 22/tcp

References:

- http://www.openssh.com/txt/release-7.1p2

Unique Alert ID: 539221 Found on: 2023-10-06 Severity: High

PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-5385,CVE-2016-6128
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a man-in-the-middle attack vulnerability. The following flaws exist: - The web servers running in a CGI or CGI-like context may assign client request proxy header values to internal HTTP_PROXY environment variables. - 'HTTP_ PROXY' is improperly trusted by some PHP libraries and applications - An unspecified flaw in the gdImageCropThreshold f unction in 'gd_crop.c' in the GD Graphics Library. Successfully exploiting this issue may allow remote, unauthenticated to conduct MITM attacks on internal server subrequests or direct the server to initiate connections to arbitrary hosts or to ca use a denial of service.

Solution:

VendorFix Update to PHP version 5.6.24 or 7.0.19.

Result:

Installed version: 5.4.16 Fixed version: 5.6.24/7.0.9

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php,http://www.kb.cert.org/vuls/id/797896, https://bugs.php.net/bug.php?id=72573,https://bugs.php.net/bug.php?id=72494

Unique Alert ID: 539222 Found on: 2023-10-06 Severity: High

Apache HTTP Server Man-in-the-Middle Attack Vulnerability - July16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-5387		
Cvss Base:	8.1		
Cvss Score:	8.1		
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

Apache HTTP Server is prone to a man-in-the-middle attack vulnerability. The flaw is due to 'CGI Servlet' does not protec t applications from the presence of untrusted client data in the 'HTTP_PROXY' environment variable. Successful exploitati on will allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted proxy header in an HTTP request.

Solution:

VendorFix Update to version 2.4.24, or 2.2.32, or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.24 Installation path / port: 443/tcp

References:

- https://www.apache.org/security/asf-httpoxy-response.txt

Unique Alert ID: 1010815 Found on: 2023-10-06 Severity: High

PHP < 7.4.30, 8.0.x < 8.0.20, 8.1.x < 8.1.7 Security Update (Jun 2022) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-08-27
CVE ID:	CVE-2022-31625,CVE-2022-31626		
Cvss Base:	8.8		
Cvss Score:	8.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP released new versions which include a security fix. The following vulnerabilities exist: - CVE-2022-31625: Uninitialize d array in pg_query_params() - CVE-2022-31626: mysqlnd/pdo password buffer overflow

Solution:

VendorFix Update to version 7.4.30, 8.0.20, 8.1.7 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.4.30 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.4.30,https://www.php.net/ChangeLog-8.php#8.0.20,https://www.php.net/ChangeLog-8.php#8.1.7,https://bugs.php.net/bug.php?id=81720,https://bugs.php.net/bug.php?id=81719

Unique Alert ID: 1010813 Found on: 2023-10-06 Severity: High

PHP < 7.4.30, 8.0.x < 8.0.20, 8.1.x < 8.1.7 Security Update (Jun 2022) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-08-27
CVE ID:	CVE-2022-31625,CVE-2022-31626		
Cvss Base:	8.8		
Cvss Score:	8.8		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP released new versions which include a security fix. The following vulnerabilities exist: - CVE-2022-31625: Uninitialize d array in pg_query_params() - CVE-2022-31626: mysqlnd/pdo password buffer overflow

Solution:

VendorFix Update to version 7.4.30, 8.0.20, 8.1.7 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.4.30 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.4.30,https://www.php.net/ChangeLog-8.php#8.0.20,https://www.php.net/ChangeLog-8.php#8.1.7,https://bugs.php.net/bug.php?id=81720,https://bugs.php.net/bug.php?id=81719

Unique Alert ID: 539218 Found on: 2023-10-06 Severity: High

Apache HTTP Server Man-in-the-Middle Attack Vulnerability - July16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-5387		
Cvss Base:	8.1		
Cvss Score:	8.1		
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H		

Description:

Apache HTTP Server is prone to a man-in-the-middle attack vulnerability. The flaw is due to 'CGI Servlet' does not protec t applications from the presence of untrusted client data in the 'HTTP_PROXY' environment variable. Successful exploitati on will allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted proxy header in an HTTP request.

Solution:

VendorFix Update to version 2.4.24, or 2.2.32, or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.24 Installation path / port: 80/tcp

References:

- https://www.apache.org/security/asf-httpoxy-response.txt

Unique Alert ID: 539220 Found on: 2023-10-06 Severity: High

PHP Man-in-the-Middle Attack Vulnerability - Jul16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-5385,CVE-2016-6128
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a man-in-the-middle attack vulnerability. The following flaws exist: - The web servers running in a CGI or CGI-like context may assign client request proxy header values to internal HTTP_PROXY environment variables. - 'HTTP_PROXY' is improperly trusted by some PHP libraries and applications - An unspecified flaw in the gdImageCropThreshold function in 'gd_crop.c' in the GD Graphics Library. Successfully exploiting this issue may allow remote, unauthenticated to conduct MITM attacks on internal server subrequests or direct the server to initiate connections to arbitrary hosts or to cause a denial of service.

Solution:

VendorFix Update to PHP version 5.6.24 or 7.0.19.

Result:

Installed version: 5.4.16 Fixed version: 5.6.24/7.0.9

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php,http://www.kb.cert.org/vuls/id/797896,https://bugs.php.net/bug.php?id=72573,https://bugs.php.net/bug.php?id=72494

Unique Alert ID: 1533205 Found on: 2023-10-06 Severity: High

PHP < 8.0.28, 8.1.x < 8.1.16, 8.2.x < 8.2.3 Security Update - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2023-10-06
CVE ID: CVE-2023-0567,CVE-2023-0568,CVE-2023-0662
Cvss Base: 7.8
Cvss Score: 7.8

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - CVE-2023-0567: Fixed bug #81744 (Password_verify() always return true with some hash) - CVE-2023-0568: Fixed bug #81746 (1-byte array overrun in common path resolve code) - CVE-2023-0662: Fixed bug GHSA-54hq-v5wp-fqgv (DOS vulnerability when parsing multipart request body)

Solution:

VendorFix Update to version 8.0.28, 8.1.16, 8.2.3 or later.

Result:

Installed version: 5.4.16 Fixed version: 8.0.28 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-8.php#8.2.3,https://www.php.net/ChangeLog-8.php#8.1.16,https://www.php.net/ChangeLog-8.php#8.0.28,https://www.php.net/archive/2023.php#2023-02-14-2,https://www.php.net/archive/2023.php#2023-02-14-3,https://www.php.net/archive/2023.php#2023-02-14-1,http://bugs.php.net/81744,http://bugs.php.net/81746,https://github.com/php/php-src/security/advisories/GHSA-54hq-v5wp-fqgv,https://github.com/php/php-src/security/advisories/GHSA-7fj2-8x79-rjf4

Unique Alert ID: 1533206 Found on: 2023-10-06 Severity: High

PHP < 8.0.28, 8.1.x < 8.1.16, 8.2.x < 8.2.3 Security Update - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2023-10-06
CVE ID:	CVE-2023-0567,CVE-2023-0568,CVE-2023-0662		
Cvss Base:	7.8		
Cvss Score:	7.8		

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - CVE-2023-0567: Fixed bug #81744 (Password_verify( ) always return true with some hash) - CVE-2023-0568: Fixed bug #81746 (1-byte array overrun in common path resolv e code) - CVE-2023-0662: Fixed bug GHSA-54hq-v5wp-fqgv (DOS vulnerability when parsing multipart request body)

Solution:

VendorFix Update to version 8.0.28, 8.1.16, 8.2.3 or later.

Result:

Installed version: 5.4.16 Fixed version: 8.0.28 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-8.php#8.2.3,https://www.php.net/ChangeLog-8.php#8.1.16,https://www.php.net/ChangeLog-8.php#8.0.28,https://www.php.net/archive/2023.php#2023-02-14-2,https://www.php.net/archive/2023.php#2023-02-14-3,https://www.php.net/archive/2023.php#2023-02-14-1,http://bugs.php.net/81744,http://bugs.php.net/81746,https://github.com/php/php-src/security/advisories/GHSA-54hq-v5wp-fqgv,https://github.com/php/php-src/security/advisories/GHSA-7fj2-8x79-rjf4

Unique Alert ID: 1533207 Found on: 2023-10-06 Severity: High

PHP < 8.0.22, 8.1.x < 8.1.9 Security Update - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2023-10-06
CVE ID:	CVE-2022-4900		
Cvss Base:	7.8		
Cvss Score:	7.8		

Description:

PHP is prone to a buffer overflow vulnerability. Fixed potential overflow for the builtin server via the PHP_CLI_SERVER_W ORKERS environment variable.

Solution:

VendorFix Update to version 8.0.22, 8.1.9, 8.2.0 or later.

Result:

Installed version: 5.4.16 Fixed version: 8.0.22/8.1.9/8.2.0 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-8.php#8.2.0,https://www.php.net/ChangeLog-8.php#8.1.9,https://www.php.net/ChangeLog-8.php#8.0.22,https://github.com/php/php-src/issues/8989,https://github.com/php/php-src/pull/9000,https://github.com/php/php-src/commit/789a37f14405e2d1a05a76c9fb4ed2d49d4580d5,https://bugzilla.redhat.com/show_bug.cgi?id=2179880

Unique Alert ID: 1533208 Found on: 2023-10-06 Severity: High

PHP < 8.0.22, 8.1.x < 8.1.9 Security Update - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2023-10-06
CVE ID: CVE-2022-4900

Cvss Base: 7.8
Cvss Score: 7.8

Description:

PHP is prone to a buffer overflow vulnerability. Fixed potential overflow for the builtin server via the PHP_CLI_SERVER_WORKERS environment variable.

Solution:

VendorFix Update to version 8.0.22, 8.1.9, 8.2.0 or later.

Result:

Installed version: 5.4.16 Fixed version: 8.0.22/8.1.9/8.2.0 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-8.php#8.2.0,https://www.php.net/ChangeLog-8.php#8.1.9,https://www.php.net/ChangeLog-8.php#8.0.22,https://github.com/php/php-src/issues/8989,https://github.com/php/php-src/pull/9000,https://github.com/php/php-src/commit/789a37f14405e2d1a05a76c9fb4ed2d49d4580d5,https://bugzilla.redhat.com/show_bug.cgi?id=2179880

Unique Alert ID: 1533209 Found on: 2023-10-06 Severity: High

PHP < 8.0.27, 8.1.x < 8.1.14, 8.2.x < 8.2.1 Security Update - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2023-10-06
CVE ID: CVE-2022-31631

Cvss Base: 7.8
Cvss Score: 7.8

Description:

PHP is prone to an integer overflow vulnerability. Due to an uncaught integer overflow, PDO::quote() of PDO_SQLite may return a not properly quoted string.

Solution:

VendorFix Update to version 8.0.27, 8.1.14, 8.2.1 or later.

Result:

Installed version: 5.4.16 Fixed version: 8.0.27 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-8.php#8.0.27,https://www.php.net/ChangeLog-8.php#8.1.14,https://www.php.net/ChangeLog-8.php#8.2.1

Unique Alert ID: 1533210 Found on: 2023-10-06 Severity: High

PHP < 8.0.27, 8.1.x < 8.1.14, 8.2.x < 8.2.1 Security Update - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2023-10-06
CVE ID:	CVE-2022-31631		
Cvss Base:	7.8		
Cvss Score:	7.8		

Description:

PHP is prone to an integer overflow vulnerability. Due to an uncaught integer overflow, PDO::quote() of PDO_SQLite may return a not properly quoted string.

Solution:

VendorFix Update to version 8.0.27, 8.1.14, 8.2.1 or later.

Result:

Installed version: 5.4.16 Fixed version: 8.0.27 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-8.php#8.0.27,https://www.php.net/ChangeLog-8.php#8.1.14,https://www.php.net/ChangeLog-8.php#8.2.1

Unique Alert ID: 539185 Found on: 2023-10-06 Severity: High

OpenBSD OpenSSH <= 8.6 Command Injection Vulnerability (tcp/22)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2020-15778		
Cvss Base:	7.8		
Cvss Score:	7.8		
Cvss Vector:	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H		

Description:

OpenBSD OpenSSH is prone to a command injection vulnerability. scp of OpenSSH allows command injection in spc.c via backtick characters in the destination argument. Successful exploitation would allow an attacker to execute arbitrary cod e on the target machine.

Solution:

WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Result:

Installed version: 6.6.1 Fixed version: None Installation path / port: 22/tcp

References:

- https://github.com/cpandya2909/CVE-2020-15778/

Unique Alert ID: 539164 Found on: 2023-10-06 Severity: High

OpenSSH Privilege Escalation Vulnerability - May16 (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18

CVE ID: CVE-2015-8325
Cvss Base: 7.8
Cvss Score: 7.8
Cvss Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Description:

openssh is prone to a privilege escalation vulnerability. The flaw exists due to an error in 'do_setup_env function' in 'session.c' script in sshd which trigger a crafted environment for the /bin/login program when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories. Successfully exploiting this issue will allow local users to gain privileges.

Solution:

VendorFix Upgrade to OpenSSH version 7.2p2-3 or later.

Result:

Installed version: 6.6.1 Fixed version: 7.2p2-3 Installation path / port: 22/tcp

References:

- https://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-8325.html,https://anongit.mindrot.org/openssh.git/commit/?id=85bdcd7c92fe7ff133bbc4e10a65c91810f88755

Unique Alert ID: 539101 Found on: 2023-10-06 Severity: High

PHP Use-After-Free Remote Code EXecution Vulnerability - Jan15 (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-8142
Cvss Base: 7.5
Cvss Score: 7.5

Description:

PHP is prone to a use-after-free vulnerability. The flaw is due to Use-after-free vulnerability in the process_nested_data function in ext/standard/var _unserializer.re in PHP. Successful exploitation will allow remote attackers to execute arbitrary code via a crafted unserialize call.

Solution:

VendorFix Update to PHP version 5.4.36 or 5.5.20 or 5.6.4 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.36/5.5.20/5.6.4

References:

- http://php.net/ChangeLog-5.php,http://secunia.com/advisories/60920,https://bugs.php.net/bug.php?id=68594

Unique Alert ID: 919539 Found on: 2023-10-06 Severity: High

Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSH, D(HE)ater) (tcp/22)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2002-20001,CVE-2022-40735
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

The remote SSH server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange (KEX) algorithms and thus could be prone to a denial of service (DoS) vulnerability. - CVE-2002-20001: The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE. - CVE-2022-40735: The Diffie-Hellman Key Agreement Protocol allows use of long exponents that arguably make certain calculations unnecessarily expensive, because the 1996 van Oorschot and Wiener paper found that '(appropriately) short exponents' can be used when there are adequate subgroup constraints, and these short exponents can lead to less expensive calculations than for long exponents. This issue is different from CVE-2002-20001 because it is based on an observation about exponent size, rather than an observation about numbers that are not public keys. The specific situations in which calculation expense would constitute a server-side vulnerability depend on the protocol (e.g., TLS, SSH, or IKE) and the DHE implementation details. In general, there might be an availability concern because of server-side resource consumption from DHE modular-exponentiation calculations. Finally, it is possible for an attacker to exploit this vulnerability and CVE-2002-20001 together. This vulnerability allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, also known as a D(HE)ater attack. There could be an increase in CPU usage in the affected component. For OpenSSH, users may observe issues such as a slowdown in SSH connections.

Solution:

Mitigation - DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For OpenSSH this limit can be configured via the 'MaxStartups' option, for other products please refer to the manual of the product in question on configuration possibilities.

Result:

The remote SSH server supports the following DHE KEX algorithm(s): diffie-hellman-group1-sha1 diffie-hellman-group14-sha1 diffie-hellman-group-exchange-sha1 diffie-hellman-group-exchange-sha256

References:

- https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocol,https://github.com/Balasys/dheater

Unique Alert ID: 539206 Found on: 2023-10-06 Severity: High

Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerability (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2019-0217		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H		

Description:

In Apache HTTP Server, a race condition in mod_auth_digest when running in a threaded server could allow a user with v alid credentials to authenticate using another username, bypassing configured access control restrictions.

Solution:

VendorFix Update to version 2.4.39 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.39 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539224 Found on: 2023-10-06 Severity: High

Apache HTTP Server 'Whitespace Defects' Multiple Vulnerabilities (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-8743		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N		

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Multiple flaws exist because the application accepted a broad patt ern of unusual whitespace patterns from the user-agent, including bare CR, FF, VTAB in parsing the request line and requ est header lines, as well as HTAB in parsing the request line. Any bare CR present in request lines was treated as whitesp ace and remained in the request field member 'the_request', while a bare CR in the request header field name would be honored as whitespace, and a bare CR in the request header field value was retained the input headers array. Implied ad ditional whitespace was accepted in the request line and prior to the ':' delimiter of any request header lines. Successful exploitation will allow remote attackers to conduct request smuggling, response splitting and cache pollution attacks.

Solution:

VendorFix Update to Apache HTTP Server 2.2.32 or 2.4.25 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.25 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_22.html,https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539233 Found on: 2023-10-06 Severity: High

Apache HTTP Server 'mod_auth_digest' DoS Vulnerability (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-2161		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

Apache HTTP Server is prone to a denial-of-service vulnerability. The flaw exists due to insufficient handling of malicious i nput to 'mod_auth_digest'. Successful exploitation will allow remote attackers to cause a denial-of-service condition.

Solution:

VendorFix Update to Apache HTTP Server 2.4.25 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.25 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2016-2161

Unique Alert ID: 539232 Found on: 2023-10-06 Severity: High

Apache HTTP Server 'mod_auth_digest' DoS Vulnerability (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2016-2161		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

Apache HTTP Server is prone to a denial-of-service vulnerability. The flaw exists due to insufficient handling of malicious i nput to 'mod_auth_digest'. Successful exploitation will allow remote attackers to cause a denial-of-service condition.

Solution:

VendorFix Update to Apache HTTP Server 2.4.25 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.25 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2016-2161

Unique Alert ID: 919540 Found on: 2023-10-06 Severity: High

Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2002-20001,CVE-2022-40735		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

The remote SSL/TLS server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange algorithms and thus could be pr one to a denial of service (DoS) vulnerability. - CVE-2002-20001: The Diffie-Hellman Key Agreement Protocol allows rem

ote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive ser ver-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest s upported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE. - CVE-2022-40735: The Diffie-Hellman Key Agreement Protocol allows use of lo ng exponents that arguably make certain calculations unnecessarily expensive, because the 1996 van Oorschot and Wien er paper found that '(appropriately) short exponents' can be used when there are adequate subgroup constraints, and th ese short exponents can lead to less expensive calculations than for long exponents. This issue is different from CVE-200 2-20001 because it is based on an observation about exponent size, rather than an observation about numbers that are n ot public keys. The specific situations in which calculation expense would constitute a server-side vulnerability depend on the protocol (e.g., TLS, SSH, or IKE) and the DHE implementation details. In general, there might be an availability conce rn because of server-side resource consumption from DHE modular-exponentiation calculations. Finally, it is possible for an attacker to exploit this vulnerability and CVE-2002-20001 together. This vulnerability allows remote attackers (from th e client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular -exponentiation calculations, also known as a D(HE)ater attack. There could be an increase in CPU usage in the affected component. For OpenSSH, users may observe issues such as a slowdown in SSH connections.

Solution:

Mitigation - DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option, for other products please refer to the manual of the product in question on configuration possibilities.

Result:

'DHE' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA 'DHE' cipher suites accepted by this service via the TLSv1.1
protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA 'DHE' cipher suites accepted by this service via the TLSv1.2
protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA

References:

- https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_K ey_Agreement_Protocol,https://github.com/Balasys/dheater

Unique Alert ID: 539223 Found on: 2023-10-06 Severity: High

Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2018-17199		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N		

Description:

In Apache HTTP Server mod_session checks the session expiry time before decoding the session. This causes session ex piry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

Solution:

VendorFix Update to version 2.4.38 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.38 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539238 Found on: 2023-10-06 Severity: High

Apache HTTP Server < 2.4.38 mod_session_cookie Vulnerability (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-17199
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Description:

In Apache HTTP Server mod_session checks the session expiry time before decoding the session. This causes session ex piry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

Solution:

VendorFix Update to version 2.4.38 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.38 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539207 Found on: 2023-10-06 Severity: High

Apache HTTP Server < 2.4.39 mod_auth_digest Access Control Bypass Vulnerability (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2019-0217
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Description:

In Apache HTTP Server, a race condition in mod_auth_digest when running in a threaded server could allow a user with v alid credentials to authenticate using another username, bypassing configured access control restrictions.

Solution:

VendorFix Update to version 2.4.39 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.39 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 919541 Found on: 2023-10-06 Severity: High

Apache HTTP Server < 2.4.48 NULL Pointer Dereference Vulnerability - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2021-31618		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

Apache HTTP Server is prone to a NULL pointer dereference vulnerability. Apache HTTP Server protocol handler for the H TTP/2 protocol checks received request headers against the size limitations as configured for the server and used for the HTTP/1 protocol as well. On violation of these restrictions an HTTP response is sent to the client with a status code indicati ng why the request was rejected. This rejection response was not fully initialised in the HTTP/2 protocol handler if the off ending header was the very first one received or appeared in a footer. This led to a NULL pointer dereference on initialise d memory, crashing reliably the child process. Successful exploitation will allow an attacker to crash the server.

Solution:

VendorFix Update to version 2.4.48 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.48 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 919542 Found on: 2023-10-06 Severity: High

Apache HTTP Server < 2.4.48 NULL Pointer Dereference Vulnerability - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2021-31618		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

Apache HTTP Server is prone to a NULL pointer dereference vulnerability. Apache HTTP Server protocol handler for the H TTP/2 protocol checks received request headers against the size limitations as configured for the server and used for the HTTP/1 protocol as well. On violation of these restrictions an HTTP response is sent to the client with a status code indicati ng why the request was rejected. This rejection response was not fully initialised in the HTTP/2 protocol handler if the off ending header was the very first one received or appeared in a footer. This led to a NULL pointer dereference on initialise d memory, crashing reliably the child process. Successful exploitation will allow an attacker to crash the server.

Solution:

VendorFix Update to version 2.4.48 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.48 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539282 Found on: 2023-10-06 Severity: High

PHP 'timelib_meridian' Heap Based Buffer Overflow Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2017-16642
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

PHP is prone to a heap buffer overflow vulnerability. The flaw exists due to an error in the date extension's 'timelib_meridian' handling of 'front of' and 'back of' directives. Successfully exploiting this issue allow attacker to execute arbitrary code with elevated privileges within the context of a privileged process.

Solution:

VendorFix Update to PHP version 5.6.32, 7.0.25, 7.1.11, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.32 Installation path / port: 80/tcp

References:

- http://php.net/ChangeLog-5.php,http://php.net/ChangeLog-7.php,https://bugs.php.net/bug.php?id=75055

Unique Alert ID: 539281 Found on: 2023-10-06 Severity: High

PHP 'timelib_meridian' Heap Based Buffer Overflow Vulnerability (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2017-16642
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

PHP is prone to a heap buffer overflow vulnerability. The flaw exists due to an error in the date extension's 'timelib_meridian' handling of 'front of' and 'back of' directives. Successfully exploiting this issue allow attacker to execute arbitrary code with elevated privileges within the context of a privileged process.

Solution:

VendorFix Update to PHP version 5.6.32, 7.0.25, 7.1.11, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.32 Installation path / port: 443/tcp

References:

- http://php.net/ChangeLog-5.php,http://php.net/ChangeLog-7.php,https://bugs.php.net/bug.php?id=75055

Unique Alert ID: 1010825 Found on: 2023-10-06 Severity: High

OpenSSL: Infinite loop in BN_mod_sqrt() reachable when parsing certificates (CVE-2022-0778) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-08-27
CVE ID: CVE-2022-0778
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

OpenSSL is prone to an infinite loop vulnerability. The BN_mod_sqrt() function, which computes a modular square root, c ontains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certific ates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point enco ded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve pa rameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an ex ternally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - T LS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else wh ich parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker ca n control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parse d during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-sig ned certificate to trigger the loop during verification of the certificate signature.

Solution:

VendorFix Update to version 1.0.2zd, 1.1.1n, 3.0.2 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2zd Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20220315.txt

Unique Alert ID: 1010824 Found on: 2023-10-06 Severity: High

OpenSSL: Infinite loop in BN_mod_sqrt() reachable when parsing certificates (CVE-2022-0778) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-08-27
CVE ID:	CVE-2022-0778		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

OpenSSL is prone to an infinite loop vulnerability. The BN_mod_sqrt() function, which computes a modular square root, c ontains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certific ates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point enco ded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve pa rameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an ex ternally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - T LS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else wh ich parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker ca n control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parse d during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-sig ned certificate to trigger the loop during verification of the certificate signature.

Solution:

VendorFix Update to version 1.0.2zd, 1.1.1n, 3.0.2 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2zd Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20220315.txt

Unique Alert ID: 919537 Found on: 2023-10-06 Severity: High

OpenSSL: Integer overflow in CipherUpdate (CVE-2021-23840) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-23840
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

OpenSSL is prone to an integer overflow vulnerability. Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_Decrypt Update may overflow the output length argument in some cases where the input length is close to the maximum permissi ble length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating succes s), but the output length value will be negative. This vulnerability could cause applications to behave incorrectly or crash.

Solution:

VendorFix Update to version 1.0.2y, 1.1.1j or later. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2y / 1.1.1j Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20210216.txt

Unique Alert ID: 919538 Found on: 2023-10-06 Severity: High

OpenSSL: Integer overflow in CipherUpdate (CVE-2021-23840) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-23840
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

OpenSSL is prone to an integer overflow vulnerability. Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_Decrypt Update may overflow the output length argument in some cases where the input length is close to the maximum permissi ble length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating succes s), but the output length value will be negative. This vulnerability could cause applications to behave incorrectly or crash.

Solution:

VendorFix Update to version 1.0.2y, 1.1.1j or later. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2y / 1.1.1j Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20210216.txt

Unique Alert ID: 539234 Found on: 2023-10-06 Severity: High

Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-1303
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

Apache HTTP Server is prone to a denial of service vulnerability. The flaw exists as the Apache HTTP Server fails to saniti ze against a specially crafted HTTP request header. Successful exploitation will allow an attacker to crash the Apache HTT P Server resulting in denial of service condition.

Solution:

VendorFix Update to version 2.4.30 or later. Please see the references for more information.

Result:

Installed version: 2.4.6 Fixed version: 2.4.30 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539236 Found on: 2023-10-06 Severity: High

Apache HTTP Server Denial of Service Vulnerability-02 Apr18 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-1303
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

Apache HTTP Server is prone to a denial of service vulnerability. The flaw exists as the Apache HTTP Server fails to saniti ze against a specially crafted HTTP request header. Successful exploitation will allow an attacker to crash the Apache HTT P Server resulting in denial of service condition.

Solution:

VendorFix Update to version 2.4.30 or later. Please see the references for more information.

Result:

Installed version: 2.4.6 Fixed version: 2.4.30 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539276 Found on: 2023-10-06 Severity: High

PHP 'WDDX Deserialization' Denial of Service Vulnerability - (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2017-11143		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw exists due to an invalid free error for an empty boolean element in ext/wddx/wddx.c script. Successfully exploiting this issue allow remote attackers inject XML for deserialization to crash the PHP interpreter.

Solution:

VendorFix Update to PHP version 5.6.31 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.31

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539275 Found on: 2023-10-06 Severity: High

PHP 'WDDX Deserialization' Denial of Service Vulnerability - (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2017-11143		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw exists due to an invalid free error for an empty boolean element in ext/wddx/wddx.c script. Successfully exploiting this issue allow remote attackers inject XML for deserialization to crash the PHP interpreter.

Solution:

VendorFix Update to PHP version 5.6.31 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.31

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539079 Found on: 2023-10-06 Severity: High

PHP Denial of Service Vulnerability Jul17 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2017-11142
Cvss Base: 7.5
Cvss Score: 7.5

Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw exists due to improper handling of long form variables in main/php_variables.c script. Successfully exploiting this issue allow an attacker to cause a CPU consumption denial of ser vice attack.

Solution:

VendorFix Update to PHP version 5.6.31, 7.0.17, 7.1.3 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.31

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539081 Found on: 2023-10-06 Severity: High

PHP Denial of Service Vulnerability Jul17 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2017-11142
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw exists due to improper handling of long form variables in main/php_variables.c script. Successfully exploiting this issue allow an attacker to cause a CPU consumption denial of ser vice attack.

Solution:

VendorFix Update to PHP version 5.6.31, 7.0.17, 7.1.3 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.31

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539278 Found on: 2023-10-06 Severity: High

PHP Multiple Denial of Service Vulnerabilities (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-8877,CVE-2015-8879,CVE-2015-8874
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to multiple denial of service (DoS) vulnerabilities. Multiple flaws are due to - An improper handling of driver behavior for SQL_WVARCHAR columns in the 'odbc_bindcols function' in 'ext/odbc/php_odbc.c' script. - The 'gdImageScal eTwoPass' function in gd_interpolation.c script in the GD Graphics Library uses inconsistent allocate and free approaches. Successfully exploiting this issue allow remote attackers to cause a denial of service (application crash or memory consu ption).

Solution:

VendorFix Update to PHP version 5.6.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.12

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539277 Found on: 2023-10-06 Severity: High

PHP Multiple Denial of Service Vulnerabilities (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-8877,CVE-2015-8879,CVE-2015-8874
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to multiple denial of service (DoS) vulnerabilities. Multiple flaws are due to - An improper handling of driver behavior for SQL_WVARCHAR columns in the 'odbc_bindcols function' in 'ext/odbc/php_odbc.c' script. - The 'gdImageScal eTwoPass' function in gd_interpolation.c script in the GD Graphics Library uses inconsistent allocate and free approaches. Successfully exploiting this issue allow remote attackers to cause a denial of service (application crash or memory consu ption).

Solution:

VendorFix Update to PHP version 5.6.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.12

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539227 Found on: 2023-10-06 Severity: High

Apache HTTP Server OPTIONS Memory Leak Vulnerability (Optionsbleed) - Version Check (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2017-9798		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N		

Description:

Apache HTTP Server allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. Optionsbleed is a use after free er ror in the Apache HTTP Server that causes a corrupted Allow header to be constructed in response to HTTP OPTIONS req uests. This can leak pieces of arbitrary memory from the server process that may contain secrets. The memory pieces c hange after multiple requests, so for a vulnerable host an arbitrary number of memory chunks can be leaked. The bug a ppears if a webmaster tries to use the 'Limit' directive with an invalid HTTP method. Example .htaccess: The successful e xploitation allows the attacker to read chunks of the host's memory.

Solution:

VendorFix Update to Apache HTTP Server 2.4.28. For Apache HTTP Server running version 2.2.34 apply the patch linked in the references. As a workaround the usage of .htaccess should be disabled completely via the 'AllowOverride None' directive within the webservers configuration. Furthermore all statements within the webserver configuration needs to be verified for invalid HTTP methods.

Result:

Installed version: 2.4.6 Fixed version: 2.4.28 Installation path / port: 80/tcp

References:

- http://openwall.com/lists/oss-security/2017/09/18/2,https://blog.fuzzing-project.org/60-Optionsbleed-HTTP-OPTION S-method-can-leak-Apaches-server-memory.html,https://archive.apache.org/dist/httpd/patches/apply_to_2.2.34/

Unique Alert ID: 539226 Found on: 2023-10-06 Severity: High

Apache HTTP Server OPTIONS Memory Leak Vulnerability (Optionsbleed) - Version Check (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2017-9798		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N		

Description:

Apache HTTP Server allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. Optionsbleed is a use after free er ror in the Apache HTTP Server that causes a corrupted Allow header to be constructed in response to HTTP OPTIONS req uests. This can leak pieces of arbitrary memory from the server process that may contain secrets. The memory pieces c hange after multiple requests, so for a vulnerable host an arbitrary number of memory chunks can be leaked. The bug a ppears if a webmaster tries to use the 'Limit' directive with an invalid HTTP method. Example .htaccess: The successful e xploitation allows the attacker to read chunks of the host's memory.

Solution:

VendorFix Update to Apache HTTP Server 2.4.28. For Apache HTTP Server running version 2.2.34 apply the patch linked in the references. As a workaround the usage of .htaccess should be disabled completely via the 'AllowOverride None' directive within the webservers configuration. Furthermore all statements within the webserver configuration needs to be verified for invalid HTTP methods.

Result:

Installed version: 2.4.6 Fixed version: 2.4.28 Installation path / port: 443/tcp

References:

- http://openwall.com/lists/oss-security/2017/09/18/2,https://blog.fuzzing-project.org/60-Optionsbleed-HTTP-OPTIONS-method-can-leak-Apaches-server-memory.html,https://archive.apache.org/dist/httpd/patches/apply_to_2.2.34/

Unique Alert ID: 919543 Found on: 2023-10-06 Severity: High

Apache HTTP Server mod_session_crypto Vulnerability (Dec 2016) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2016-0736
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

Apache HTTP Server is prone to a vulnerability in mod_session_crypto. mod_sessioncrypto is encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This makes it vulnerable to padding oracle attacks, particularly with CBC. An authentication tag (SipHash MAC) is now added to prevent such attacks.

Solution:

VendorFix Update to version 2.4.25 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.25 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 919544 Found on: 2023-10-06 Severity: High

Apache HTTP Server mod_session_crypto Vulnerability (Dec 2016) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2016-0736
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

Apache HTTP Server is prone to a vulnerability in mod_session_crypto. mod_sessioncrypto is encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This makes it vulnerable to padding oracle attacks, particularly with CBC. An authentication tag (SipHash MAC) is now added to prevent such attacks.

Solution:

VendorFix Update to version 2.4.25 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.25 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 1533211 Found on: 2023-10-06 Severity: High

OpenSSL 1.0.2 < 1.0.2zg, 1.1.1 < 1.1.1t, 3.0 < 3.0.8 Multiple Vulnerabilities - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2023-10-06
CVE ID: CVE-2022-4304,CVE-2023-0215,CVE-2023-0286
Cvss Base: 7.4
Cvss Score: 7.4
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H

Description:

OpenSSL is prone to multiple vulnerabilities. The following flaws exist: - CVE-2022-4304: Timing Oracle in RSA Decryptio n - CVE-2023-0215: Use-after-free following BIO_new_NDEF - CVE-2023-0286: X.400 address type confusion in X.509 G eneralName

Solution:

VendorFix Update to version 1.0.2zg, 1.1.1t, 3.0.8 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2zg Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20230207.txt

Unique Alert ID: 1533212 Found on: 2023-10-06 Severity: High

OpenSSL 1.0.2 < 1.0.2zg, 1.1.1 < 1.1.1t, 3.0 < 3.0.8 Multiple Vulnerabilities - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2023-10-06
CVE ID: CVE-2022-4304,CVE-2023-0215,CVE-2023-0286
Cvss Base: 7.4
Cvss Score: 7.4
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H

Description:

OpenSSL is prone to multiple vulnerabilities. The following flaws exist: - CVE-2022-4304: Timing Oracle in RSA Decryptio n - CVE-2023-0215: Use-after-free following BIO_new_NDEF - CVE-2023-0286: X.400 address type confusion in X.509 G eneralName

Solution:

VendorFix Update to version 1.0.2zg, 1.1.1t, 3.0.8 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2zg Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20230207.txt

Unique Alert ID: 539225 Found on: 2023-10-06 Severity: High

Apache HTTP Server 'Whitespace Defects' Multiple Vulnerabilities (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-8743
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Multiple flaws exist because the application accepted a broad patt ern of unusual whitespace patterns from the user-agent, including bare CR, FF, VTAB in parsing the request line and requ est header lines, as well as HTAB in parsing the request line. Any bare CR present in request lines was treated as whitesp ace and remained in the request field member 'the_request', while a bare CR in the request header field name would be honored as whitespace, and a bare CR in the request header field value was retained the input headers array. Implied ad ditional whitespace was accepted in the request line and prior to the ':' delimiter of any request header lines. Successful exploitation will allow remote attackers to conduct request smuggling, response splitting and cache pollution attacks.

Solution:

VendorFix Update to Apache HTTP Server 2.2.32 or 2.4.25 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.25 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_22.html,https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539256 Found on: 2023-10-06 Severity: High

PHP 'CVE-2017-7189' Improper Input Validation Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2017-7189
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

PHP is improperly validating input from untrusted input. main/streams/xp_socket.c in PHP misparses fsockopen calls, suc h as by interpreting fsockopen('127.0.0.1:80', 443) as if the address/port were 127.0.0.1:80:443, which is later truncated to 127.0.0.1:80. This behavior has a security risk if the explicitly provided port number (i.e., 443 in this example) is hard coded into an application as a security policy, but the hostname argument (i.e., 127.0.0.1:80 in this example) is obtained from untrusted input.

Solution:

WillNotFix No solution was made available by the vendor. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one. Note: PHP versions 7.0.18 and 7.1.4 introduced a fix which was reverted again in version 7.0.19 / 7.1.5 respectively and the fix wasn't introduced again as of today (08-2020).

Result:

Installed version: 5.4.16 Fixed version: None Installation path / port: 80/tcp

References:

- https://bugs.php.net/bug.php?id=74192,https://bugs.php.net/bug.php?id=74429,https://github.com/php/php-src/commit/bab0b99f376dac9170ac81382a5ed526938d595a

Unique Alert ID: 539254 Found on: 2023-10-06 Severity: High

PHP 'CVE-2017-7189' Improper Input Validation Vulnerability (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2017-7189
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

PHP is improperly validating input from untrusted input. main/streams/xp_socket.c in PHP misparses fsockopen calls, such as by interpreting fsockopen('127.0.0.1:80', 443) as if the address/port were 127.0.0.1:80:443, which is later truncated to 127.0.0.1:80. This behavior has a security risk if the explicitly provided port number (i.e., 443 in this example) is hard coded into an application as a security policy, but the hostname argument (i.e., 127.0.0.1:80 in this example) is obtained from untrusted input.

Solution:

WillNotFix No solution was made available by the vendor. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one. Note: PHP versions 7.0.18 and 7.1.4 introduced a fix which was reverted again in version 7.0.19 / 7.1.5 respectively and the fix wasn't introduced again as of today (08-2020).

Result:

Installed version: 5.4.16 Fixed version: None Installation path / port: 443/tcp

References:

- https://bugs.php.net/bug.php?id=74192,https://bugs.php.net/bug.php?id=74429,https://github.com/php/php-src/commit/bab0b99f376dac9170ac81382a5ed526938d595a

Unique Alert ID: 539255 Found on: 2023-10-06 Severity: High

PHP 'CVE-2018-19935' - 'imap_mail' Denial of Service Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-19935
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw exists due to a NULL pointer dereference and application crash via an empty string in the message argument to the imap_mail function of ext/imap/php_imap.c. Successful exploitation will allow attackers to cause a denial of service of the affected application.

Solution:

VendorFix Update to version 5.6.39, 7.0.33, 7.1.26, 7.2.14, 7.3.0 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.39 Installation path / port: 80/tcp

References:

- https://bugs.php.net/bug.php?id=77020

Unique Alert ID: 539253 Found on: 2023-10-06 Severity: High

PHP 'CVE-2018-19935' - 'imap_mail' Denial of Service Vulnerability (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-19935
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw exists due to a NULL pointer dereference and application crash via an empty string in the message argument to the imap_mail function of ext/imap/php_imap.c. Successful exploit ation will allow attackers to cause a denial of service of the affected application.

Solution:

VendorFix Update to version 5.6.39, 7.0.33, 7.1.26, 7.2.14, 7.3.0 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.39 Installation path / port: 443/tcp

References:

- https://bugs.php.net/bug.php?id=77020

Unique Alert ID: 539242 Found on: 2023-10-06 Severity: High

PHP 'stream_get_meta_data' Privilege Escalation Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-10712
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Description:

PHP is prone to a privilege escalation vulnerability. The flaw exists due to error in the function stream_get_meta_data of t he component File Upload. The manipulation as part of a Return Value leads to a privilege escalation vulnerability (Metad ata). Successfully exploitation will allow an attacker to update the 'metadata' and affect on confidentiality, integrity, and a vailability.

Solution:

VendorFix Update to PHP version 5.5.32, 7.0.3, or 5.6.18 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.32 Installation path / port: 80/tcp

References:

- https://bugs.php.net/bug.php?id=71323

Unique Alert ID: 539241 Found on: 2023-10-06 Severity: High

PHP 'stream_get_meta_data' Privilege Escalation Vulnerability (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-10712
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Description:

PHP is prone to a privilege escalation vulnerability. The flaw exists due to error in the function stream_get_meta_data of t he component File Upload. The manipulation as part of a Return Value leads to a privilege escalation vulnerability (Metad ata). Successfully exploitation will allow an attacker to update the 'metadata' and affect on confidentiality, integrity, and a vailability.

Solution:

VendorFix Update to PHP version 5.5.32, 7.0.3, or 5.6.18 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.32 Installation path / port: 443/tcp

References:

- https://bugs.php.net/bug.php?id=71323

Unique Alert ID: 539262 Found on: 2023-10-06 Severity: High

PHP < 7.2.30, 7.3 < 7.3.17, 7.4 < 7.4.5 DoS Vulnerability - Apr20 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2020-7067
Cvss Base: 7.5
Cvss Score: 7.5

Description:

PHP is prone to a denial-of-service vulnerability. If 'CHARSET_EBCDIC' is defined (usually, on systems with EBCDIC enc oding support), an out-of-bounds read can occur using a malformed url-encoded string.

Solution:

VendorFix Update to version 7.2.30, 7.3.17, 7.4.5 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.30 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.30,https://www.php.net/ChangeLog-7.php#7.3.17,https://www.php.net/ ChangeLog-7.php#7.4.5

Unique Alert ID: 539260 Found on: 2023-10-06 Severity: High

PHP < 7.2.30, 7.3 < 7.3.17, 7.4 < 7.4.5 DoS Vulnerability - Apr20 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2020-7067
Cvss Base: 7.5
Cvss Score: 7.5

Description:

PHP is prone to a denial-of-service vulnerability. If 'CHARSET_EBCDIC' is defined (usually, on systems with EBCDIC enc oding support), an out-of-bounds read can occur using a malformed url-encoded string.

Solution:

VendorFix Update to version 7.2.30, 7.3.17, 7.4.5 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.30 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.30,https://www.php.net/ChangeLog-7.php#7.3.17,https://www.php.net/ ChangeLog-7.php#7.4.5

Unique Alert ID: 919545 Found on: 2023-10-06 Severity: High

PHP < 7.3.27, 7.4.x < 7.4.15, 8.0.x < 8.0.2 NULL Deference Vulnerability (Feb 2021) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-21702
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a NULL dereference vulnerability in the SoapClient.

Solution:

VendorFix Update to version 7.3.27, 7.4.15, 8.0.2 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.27 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.27,https://www.php.net/ChangeLog-7.php#7.4.15,https://www.php.net/ChangeLog-8.php#8.0.2

Unique Alert ID: 919546 Found on: 2023-10-06 Severity: High

PHP < 7.3.27, 7.4.x < 7.4.15, 8.0.x < 8.0.2 NULL Deference Vulnerability (Feb 2021) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-21702
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a NULL dereference vulnerability in the SoapClient.

Solution:

VendorFix Update to version 7.3.27, 7.4.15, 8.0.2 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.27 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.27,https://www.php.net/ChangeLog-7.php#7.4.15,https://www.php.net/ChangeLog-8.php#8.0.2

Unique Alert ID: 539250 Found on: 2023-10-06 Severity: High

PHP Fileinfo Component Denial of Service Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-0236
Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due an improper validation of input to zero root_storag e value in a CDF file. Successfully exploiting this issue allow remote attackers to cause a denial of service.

Solution:

VendorFix Update to PHP version 5.6.0

Result:

Installed version: 5.4.16 Fixed version: 5.6.0

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539249 Found on: 2023-10-06 Severity: High

PHP Fileinfo Component Denial of Service Vulnerability (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-0236		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due an improper validation of input to zero root_storag e value in a CDF file. Successfully exploiting this issue allow remote attackers to cause a denial of service.

Solution:

VendorFix Update to PHP version 5.6.0

Result:

Installed version: 5.4.16 Fixed version: 5.6.0

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539154 Found on: 2023-10-06 Severity: High

PHP Multiple Double Free Vulnerabilities - Jan15 (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-9425,CVE-2014-9709		
Cvss Base:	7.5		
Cvss Score:	7.5		

Description:

PHP is prone to a denial of service (DoS) vulnerability. Multiple flaws are due to: - Double free error in the 'zend_ts_hash _graceful_destroy' function in 'zend_ts_hash.c script in the Zend Engine in PHP. - flaw in the 'GetCode_' function in 'gd_gi f_in.c' script in GD Graphics Library (LibGD). Successful exploitation will allow remote attackers to cause a denial of servi ce or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.5.21 or 5.6.5 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.21/5.6.5

References:

- http://securitytracker.com/id/1031479,https://bugs.php.net/bug.php?id=68676

Unique Alert ID: 539153 Found on: 2023-10-06 Severity: High

PHP Multiple Double Free Vulnerabilities - Jan15 (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-9425,CVE-2014-9709		
Cvss Base:	7.5		
Cvss Score:	7.5		

Description:

PHP is prone to a denial of service (DoS) vulnerability. Multiple flaws are due to: - Double free error in the 'zend_ts_hash _graceful_destroy' function in 'zend_ts_hash.c script in the Zend Engine in PHP. - flaw in the 'GetCode_' function in 'gd_gi f_in.c' script in GD Graphics Library (LibGD). Successful exploitation will allow remote attackers to cause a denial of servi ce or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.5.21 or 5.6.5 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.21/5.6.5

References:

- http://securitytracker.com/id/1031479,https://bugs.php.net/bug.php?id=68676

Unique Alert ID: 539248 Found on: 2023-10-06 Severity: High

PHP Multiple Heap Buffer Overflow and Information Disclosure Vulnerabilities (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2018-14851,CVE-2018-14883,CVE-2018-15132		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N		

Description:

PHP is prone to multiple heap buffer overflow and information disclosure vulnerabilities. Multiple flaws exist due to: - exif _process_IFD_in_MAKERNOTE function in exif.c file suffers from improper validation against crafted JPEG files. - exif_thu mbnail_extract function in exif.c file suffers from improper validation of length of 'ImageInfo->Thumbnail.offset + ImageI nfo->Thumbnail.size' - linkinfo function on windows doesn't implement openbasedir check. Successful exploitation will allo w attackers to cause heap overflow, denial of service and disclose sensitive information.

Solution:

VendorFix Update to PHP version 5.6.37, 7.0.31, 7.1.20 or 7.2.8 or later. Please see the references for more information.

Result:

Installed version: 5.4.16 Fixed version: 5.6.37 Installation path / port: 80/tcp

References:

- https://access.redhat.com/security/cve/cve-2018-14851,https://bugs.php.net/bug.php?id=76557,https://bugs.php.n et/bug.php?id=76423,https://bugs.php.net/bug.php?id=76459

Unique Alert ID: 539247 Found on: 2023-10-06 Severity: High

PHP Multiple Heap Buffer Overflow and Information Disclosure Vulnerabilities (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2018-14851,CVE-2018-14883,CVE-2018-15132		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N		

Description:

PHP is prone to multiple heap buffer overflow and information disclosure vulnerabilities. Multiple flaws exist due to: - exif_process_IFD_in_MAKERNOTE function in exif.c file suffers from improper validation against crafted JPEG files. - exif_thumbnail_extract function in exif.c file suffers from improper validation of length of 'ImageInfo->Thumbnail.offset + ImageInfo->Thumbnail.size' - linkinfo function on windows doesn't implement openbasedir check. Successful exploitation will allow attackers to cause heap overflow, denial of service and disclose sensitive information.

Solution:

VendorFix Update to PHP version 5.6.37, 7.0.31, 7.1.20 or 7.2.8 or later. Please see the references for more information.

Result:

Installed version: 5.4.16 Fixed version: 5.6.37 Installation path / port: 443/tcp

References:

- https://access.redhat.com/security/cve/cve-2018-14851,https://bugs.php.net/bug.php?id=76557,https://bugs.php.net/bug.php?id=76423,https://bugs.php.net/bug.php?id=76459

Unique Alert ID: 539152 Found on: 2023-10-06 Severity: High

PHP Multiple Remote Code Execution Vulnerabilities - Jul15 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-0273,CVE-2014-9705		
Cvss Base:	7.5		
Cvss Score:	7.5		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Multiple use-after-free vulnerabilities in 'ext/date/php_date.c' script. - Heap-based buffer overflow in the 'enchant_broker_request_dict' function in 'ext/enchant/enchant.c' script. Successfully exploiting this issue allow remote attackers to execute arbitrary code via some crafted dimensions.

Solution:

VendorFix Update to PHP 5.4.38 or 5.5.22 or 5.6.6 or later.

Result:

Installed Version: 5.4.16 Fixed Version: 5.4.48

References:

- http://php.net/ChangeLog-5.php,https://bugzilla.redhat.com/show_bug.cgi?id=1194730,http://lists.opensuse.org/opensuse-updates/2015-04/msg00002.html

Unique Alert ID: 539151 Found on: 2023-10-06 Severity: High

PHP Multiple Remote Code Execution Vulnerabilities - Jul15 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18

CVE ID: CVE-2015-0273,CVE-2014-9705
Cvss Base: 7.5
Cvss Score: 7.5

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Multiple use-after-free vulnerabilities in 'ext/date/php_date.c' script. - Heap-based buffer overflow in the 'enchant_broker_request_dict' function in 'ext/enchant/enchant.c' script. Successfully exploiting this issue allow remote attackers to execute arbitrary code via some crafted dimensions.

Solution:

VendorFix Update to PHP 5.4.38 or 5.5.22 or 5.6.6 or later.

Result:

Installed Version: 5.4.16 Fixed Version: 5.4.48

References:

- http://php.net/ChangeLog-5.php,https://bugzilla.redhat.com/show_bug.cgi?id=1194730,http://lists.opensuse.org/opensuse-updates/2015-04/msg00002.html

Unique Alert ID: 539147 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Feb15 (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-0232,CVE-2015-0231,CVE-2014-9652,CVE-2014-9653
Cvss Base: 7.5
Cvss Score: 7.5

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Flaw in the 'exif_process_unicode' function in ext/exif/exif.c script when parsing JPEG EXIF entries. - A use-after-free error in the 'process_nested_data' function in ext/standard/var_unserializer.re script. - a flaw in 'readelf.c' script in Fine Free File. - an out-of-bounds read flaw in 'src/softmagic.c' script in Fine Free File. Successful exploitation will allow remote attackers to cause a denial of service or possibly execute arbitrary code via different crafted dimensions.

Solution:

VendorFix Update to PHP version 5.4.37 or 5.5.21 or 5.6.5 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.37

References:

- https://bugs.php.net/bug.php?id=68799,https://bugs.php.net/bug.php?id=68710

Unique Alert ID: 539146 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Feb15 (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2015-0232,CVE-2015-0231,CVE-2014-9652,CVE-2014-9653	
Cvss Base:	7.5	
Cvss Score:	7.5	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Flaw in the 'exif_process_unicode' function in ext/exif/exif.c script when parsing JPEG EXIF entries. - A use-after-free error in the 'process_nested_data' function in ext/standard/var_unserializer.re script. - a flaw in 'readelf.c' script in Fine Free File. - an out-of-bounds read flaw in 'src/softmagic.c' script in Fine Free File. Successful exploitation will allow remote attackers to cause a denial of service or possibly execute arbitrary code via different crafted dimensions.

Solution:

VendorFix Update to PHP version 5.4.37 or 5.5.21 or 5.6.5 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.37

References:

- https://bugs.php.net/bug.php?id=68799,https://bugs.php.net/bug.php?id=68710

Unique Alert ID: 539143 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Jan15 (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2014-3670,CVE-2014-3669,CVE-2014-3668	
Cvss Base:	7.5	
Cvss Score:	7.5	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - The exif_ifd_make_value function in exif.c in the EXIF extension in PHP operates on floating-point arrays incorrectly. - Integer overflow in the object_custom function in ext/standard/var _unserializer.c in PHP. - Buffer overflow in the date_from_ISO8601 function in the mkgmtime implementation in libxmlrpc/xmlrpc.c in the XMLRPC extension in PHP. Successful exploitation will allow remote attackers to cause a denial of service or possibly execute arbitrary code via different crafted dimensions.

Solution:

VendorFix Update to PHP version 5.4.34 or 5.5.18 or 5.6.2 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.34/5.5.18/5.6.2

References:

- https://bugs.php.net/bug.php?id=68044

Unique Alert ID: 539141 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Jan15 (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-3670,CVE-2014-3669,CVE-2014-3668		
Cvss Base:	7.5		
Cvss Score:	7.5		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - The exif_ifd_make_value function in exif.c in the EXIF extension in PHP operates on floating-point arrays incorrectly. - Integer overflow in the object_custom function in ext/standard/var _unserializer.c in PHP. - Buffer overflow in the date_from_ISO8601 function in the mkgmtime implementation in libxmlrpc/xmlrpc.c in the XMLRPC extension in PHP. Successful exploitation will allow remote attackers to cause a denial of service or possibly execute arbitrary code via different crafted dimensions.

Solution:

VendorFix Update to PHP version 5.4.34 or 5.5.18 or 5.6.2 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.34/5.5.18/5.6.2

References:

- https://bugs.php.net/bug.php?id=68044

Unique Alert ID: 539139 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Jun15 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-4148,CVE-2015-4147,CVE-2015-2787,CVE-2015-2348,CVE-2015-2331		
Cvss Base:	7.5		
Cvss Score:	7.5		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - 'do_soap_call' function in ext/soap/soap.c script in PHP does not verify that the uri property is a string. - 'SoapClient::__call' method in ext/soap/soap.c script in PHP does not verify that __default_headers is an array. - use-after-free error related to the 'unserialize' function when using DateInterval input. - a flaw in the 'move_uploaded_file' function that is triggered when handling NULL bytes. - an integer overflow condition in the '_zip_cdir_new' function in 'zip_dirent.c' script. Successfully exploiting this issue allow remote attackers to obtain sensitive information by providing crafted serialized data with an int data type and to execute arbitrary code by providing crafted serialized data with an unexpected data type.

Solution:

VendorFix Update to PHP 5.4.39 or 5.5.23 or 5.6.7 or later.

Result:

Installed Version: 5.4.16 Fixed Version: 5.4.39

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=69085,http://openwall.com/lists/oss-security/2015/06/01/4

Unique Alert ID: 539135 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Jun15 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2015-4148,CVE-2015-4147,CVE-2015-2787,CVE-2015-2348,CVE-2015-2331	
Cvss Base:	7.5	
Cvss Score:	7.5	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - 'do_soap_call' function in ext/soap/soap.c script in PHP does not verify that the uri property is a string. - 'SoapClient::__call' method in ext/soap/soap.c script in PHP does not verify that __default_headers is an array. - use-after-free error related to the 'unserialize' function when using DateInterval input. - a flaw in the 'move_uploaded_file' function that is triggered when handling NULL bytes. - an integer overflow condition in the '_zip_cdir_new' function in 'zip_dirent.c' script. Successfully exploiting this issue allow remote attackers to obtain sensitive information by providing crafted serialized data with an int data type and to execute arbitrary code by providing crafted serialized data with an unexpected data type.

Solution:

VendorFix Update to PHP 5.4.39 or 5.5.23 or 5.6.7 or later.

Result:

Installed Version: 5.4.16 Fixed Version: 5.4.39

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=69085,http://openwall.com/lists/oss-security/2015/06/01/4

Unique Alert ID: 539133 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 02 - Jan15 (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2014-9426	
Cvss Base:	7.5	
Cvss Score:	7.5	

Description:

PHP is prone to multiple vulnerabilities. The flaw is due to a free operation on a stack-based character array by The apprentice_load function in libmagic/apprentice.c in the Fileinfo component. Successful exploitation will allow remote attackers to cause a denial of service or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.6.5 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.5

References:

- https://bugs.php.net/bug.php?id=68665,http://securitytracker.com/id/1031480

Unique Alert ID: 539132 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 02 - Jan15 (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-9426		
Cvss Base:	7.5		
Cvss Score:	7.5		

Description:

PHP is prone to multiple vulnerabilities. The flaw is due to a free operation on a stack-based character array by The apprentice_load function in libmagic/apprentice.c in the Fileinfo component. Successful exploitation will allow remote attackers to cause a denial of service or possibly have unspecified other impact.

Solution:

VendorFix Update to PHP version 5.6.5 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.5

References:

- https://bugs.php.net/bug.php?id=68665,http://securitytracker.com/id/1031480

Unique Alert ID: 539131 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 02 - Jun15 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-4026,CVE-2015-4025,CVE-2015-4024,CVE-2015-4022,CVE-2015-4021		
Cvss Base:	7.5		
Cvss Score:	7.5		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Algorithmic complexity vulnerability in the 'multipart_buffer_headers' function in main/rfc1867.c script in PHP. - 'pcntl_exec' implementation in PHP truncates a pathname upon encountering a \x00 character. - Integer overflow in the 'ftp_genlist' function in ext/ftp/ftp.c script in PHP. - The 'phar_parse_tarfile' function in ext/phar/tar.c script in PHP does not verify that the first character of a filename is different from the \0 character. Successfully exploiting this issue allow remote attackers to cause a denial of service, bypass intended extension restrictions and access and execute files or directories with unexpected names via crafted dimensions and remote FTP servers to execute arbitrary code.

Solution:

VendorFix Update to PHP 5.4.41 or 5.5.25 or 5.6.9 or later.

Result:

Installed Version: 5.4.16 Fixed Version: 5.4.41

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=69085,http://openwall.com/lists/oss-security/2015/06/01/4

Unique Alert ID: 539130 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 02 - Jun15 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-4026,CVE-2015-4025,CVE-2015-4024,CVE-2015-4022,CVE-2015-4021		
Cvss Base:	7.5		
Cvss Score:	7.5		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Algorithmic complexity vulnerability in the 'multipart_buffer_headers' function in main/rfc1867.c script in PHP. - 'pcntl_exec' implementation in PHP truncates a pathname upon encountering a \x00 character. - Integer overflow in the 'ftp_genlist' function in ext/ftp/ftp.c script in PHP. - The 'phar_parse_tarfile' function in ext/phar/tar.c script in PHP does not verify that the first character of a filename is different from the \0 character. Successfully exploiting this issue allow remote attackers to cause a denial of service, bypass intended extension restrictions and access and execute files or directories with unexpected names via crafted dimensions and remote FTP servers to execute arbitrary code.

Solution:

VendorFix Update to PHP 5.4.41 or 5.5.25 or 5.6.9 or later.

Result:

Installed Version: 5.4.16 Fixed Version: 5.4.41

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=69085,http://openwall.com/lists/oss-security/2015/06/01/4

Unique Alert ID: 539075 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - Dec18 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2018-19518,CVE-2018-20783,CVE-2018-19396		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to multiple security vulnerabilities. The flaws exist due to: - the imap_open functions which allows to run arbitrary shell commands via mailbox parameter. - a Heap Buffer Overflow (READ: 4) in phar_parse_pharfile. - ext/standard/var_unserializer.c allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class. Successful exploitation will allow remote attackers to execute remote code on the affected application/system and/or cause a cause a denial of service.

Solution:

VendorFix Update to version 5.6.39, 7.0.33, 7.1.25, 7.2.13, 7.3.0 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.39 Installation path / port: 80/tcp

References:

- https://bugs.php.net/bug.php?id=76428,https://bugs.php.net/bug.php?id=77153,https://bugs.php.net/bug.php?id=7

7160,https://bugs.php.net/bug.php?id=77143,https://github.com/Bo0oM/PHP_imap_open_exploit/blob/master/exploit.php,https://www.exploit-db.com/exploits/45914/,https://www.openwall.com/lists/oss-security/2018/11/22/3

Unique Alert ID: 539073 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - Dec18 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2018-19518,CVE-2018-20783,CVE-2018-19396	
Cvss Base:	7.5	
Cvss Score:	7.5	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	

Description:

PHP is prone to multiple security vulnerabilities. The flaws exist due to: - the imap_open functions which allows to run arb itrary shell commands via mailbox parameter. - a Heap Buffer Overflow (READ: 4) in phar_parse_pharfile. - ext/standard /var_unserializer.c allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dot net, or variant class. Successful exploitation will allow remote attackers to execute remote code on the affected applicatio n/system and/or cause a cause a denial of service.

Solution:

VendorFix Update to version 5.6.39, 7.0.33, 7.1.25, 7.2.13, 7.3.0 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.39 Installation path / port: 443/tcp

References:

- https://bugs.php.net/bug.php?id=76428,https://bugs.php.net/bug.php?id=77153,https://bugs.php.net/bug.php?id=77160,https://bugs.php.net/bug.php?id=77143,https://github.com/Bo0oM/PHP_imap_open_exploit/blob/master/exploit.php,https://www.exploit-db.com/exploits/45914/,https://www.openwall.com/lists/oss-security/2018/11/22/3

Unique Alert ID: 539111 Found on: 2023-10-06 Severity: High

PHP Out of Bounds Read Multiple Vulnerabilities - Jan15 (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2014-9427	
Cvss Base:	7.5	
Cvss Score:	7.5	

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to an out-of-bounds read error in sapi/cgi/cgi_mai n.c in the CGI component in PHP. Successful exploitation will allow remote attackers to obtain sensitive information and tr igger unexpected code execution .

Solution:

VendorFix Update to PHP version 5.4.37 or 5.5.21 or 5.6.5 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.37/5.5.21/5.6.5

References:

- https://bugs.php.net/bug.php?id=68618

Unique Alert ID: 539110 Found on: 2023-10-06 Severity: High

PHP Out of Bounds Read Multiple Vulnerabilities - Jan15 (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-9427
Cvss Base: 7.5
Cvss Score: 7.5

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to an out-of-bounds read error in sapi/cgi/cgi_main.c in the CGI component in PHP. Successful exploitation will allow remote attackers to obtain sensitive information and trigger unexpected code execution .

Solution:

VendorFix Update to PHP version 5.4.37 or 5.5.21 or 5.6.5 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.37/5.5.21/5.6.5

References:

- https://bugs.php.net/bug.php?id=68618

Unique Alert ID: 539109 Found on: 2023-10-06 Severity: High

PHP Remote Code Execution and Denial of Service Vulnerabilities - Dec13 (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2013-6420
Cvss Base: 7.5
Cvss Score: 7.5

Description:

PHP is prone to a remote code execution (RCE) vulnerability. The flaw is due to a boundary error within the 'asn1_time_to_time_t' function in 'ext/openssl/openssl.c' when parsing X.509 certificates. Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption).

Solution:

VendorFix Update to PHP version 5.3.28 or 5.4.23 or 5.5.7 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.3.28/5.4.23/5.5.7

References:

- http://secunia.com/advisories/56055,http://packetstormsecurity.com/files/124436/PHP-openssl_x509_parse-Memory-Corruption.html

Unique Alert ID: 539108 Found on: 2023-10-06 Severity: High

PHP Remote Code Execution and Denial of Service Vulnerabilities - Dec13 (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2013-6420
Cvss Base: 7.5
Cvss Score: 7.5

Description:

PHP is prone to a remote code execution (RCE) vulnerability. The flaw is due to a boundary error within the 'asn1_time_t

o_time_t' function in 'ext/openssl/openssl.c' when parsing X.509 certificates. Successful exploitation will allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption).

Solution:

VendorFix Update to PHP version 5.3.28 or 5.4.23 or 5.5.7 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.3.28/5.4.23/5.5.7

References:

- http://secunia.com/advisories/56055,http://packetstormsecurity.com/files/124436/PHP-openssl_x509_parse-Memory-Corruption.html

Unique Alert ID: 539102 Found on: 2023-10-06 Severity: High

PHP Use-After-Free Remote Code EXecution Vulnerability - Jan15 (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-8142
Cvss Base: 7.5
Cvss Score: 7.5

Description:

PHP is prone to a use-after-free vulnerability. The flaw is due to Use-after-free vulnerability in the process_nested_data function in ext/standard/var _unserializer.re in PHP. Successful exploitation will allow remote attackers to execute arbitrary code via a crafted unserialize call.

Solution:

VendorFix Update to PHP version 5.4.36 or 5.5.20 or 5.6.4 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.36/5.5.20/5.6.4

References:

- http://php.net/ChangeLog-5.php,http://secunia.com/advisories/60920,https://bugs.php.net/bug.php?id=68594

Unique Alert ID: 919548 Found on: 2023-10-06 Severity: High

OpenSSL: Read Buffer Overruns Processing ASN.1 Strings (20210824) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-3712
Cvss Base: 7.4
Cvss Score: 7.4
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H

Description:

OpenSSL is prone to a buffer overflow vulnerability. ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are represented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own 'd2i' functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the 'data' and 'length' fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the 'data' field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of

loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). I t can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext).

Solution:

VendorFix Update to version 1.0.2za, 1.1.1l or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2za / 1.1.1l Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20210824.txt

Unique Alert ID: 919547 Found on: 2023-10-06 Severity: High

OpenSSL: Read Buffer Overruns Processing ASN.1 Strings (20210824) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-3712
Cvss Base: 7.4
Cvss Score: 7.4
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H

Description:

OpenSSL is prone to a buffer overflow vulnerability. ASN.1 strings are represented internally within OpenSSL as an ASN1 _STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are represented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own 'd2i' functions (and other similar parsing fun ctions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL termina te the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_ STRING structures which do not NUL terminate the byte array by directly setting the 'data' and 'length' fields in the ASN1 _STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that prin t ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is n ot guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be pri nted, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application with out NUL terminating the 'data' field, then a read buffer overrun can occur. The same thing can also occur during name co nstraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). I t can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext).

Solution:

VendorFix Update to version 1.0.2za, 1.1.1l or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2za / 1.1.1l Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20210824.txt

Unique Alert ID: 539138 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Mar16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-6831,CVE-2015-6832,CVE-2015-6833		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - The multiple use-after-free vulnerabilities in SPL unser ialize implementation. - An insufficient validation of user supplied input by 'phar/phar_object.c' script. Successfully exploit ing this issue allow remote attackers to execute arbitrary code and to create or overwrite arbitrary files on the system an d this may lead to launch further attacks.

Solution:

VendorFix Update to PHP version 5.4.44 or 5.5.28 or 5.6.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.44

References:

- https://bugs.php.net/bug.php?id=70068,http://www.openwall.com/lists/oss-security/2015/08/19/3

Unique Alert ID: 539136 Found on: 2023-10-06 Severity: High

PHP Multiple Vulnerabilities - 01 - Mar16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-6831,CVE-2015-6832,CVE-2015-6833		
Cvss Base:	7.5		
Cvss Score:	7.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - The multiple use-after-free vulnerabilities in SPL unser ialize implementation. - An insufficient validation of user supplied input by 'phar/phar_object.c' script. Successfully exploit ing this issue allow remote attackers to execute arbitrary code and to create or overwrite arbitrary files on the system an d this may lead to launch further attacks.

Solution:

VendorFix Update to PHP version 5.4.44 or 5.5.28 or 5.6.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.44

References:

- https://bugs.php.net/bug.php?id=70068,http://www.openwall.com/lists/oss-security/2015/08/19/3

Unique Alert ID: 539107 Found on: 2023-10-06 Severity: High

PHP 'serialize_function_call' Function Type Confusion Vulnerability - Mar16 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-6836
Cvss Base: 7.3
Cvss Score: 7.3
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Description:

PHP is prone to a remote code execution (RCE) vulnerability. The flaw is due to 'SoapClient __call' method in 'ext/soap/soap.c' scripr does not properly manage headers. Successfully exploiting this issue allow remote attackers to execute arbitrary code in the context of the user running the affected application. Failed exploit attempts will likely cause a denial-of-service condition.

Solution:

VendorFix Update to PHP version 5.4.45, or 5.5.29, or 5.6.13 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.45

References:

- http://www.php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=70388

Unique Alert ID: 539106 Found on: 2023-10-06 Severity: High

PHP 'serialize_function_call' Function Type Confusion Vulnerability - Mar16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-6836
Cvss Base: 7.3
Cvss Score: 7.3
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Description:

PHP is prone to a remote code execution (RCE) vulnerability. The flaw is due to 'SoapClient __call' method in 'ext/soap/soap.c' scripr does not properly manage headers. Successfully exploiting this issue allow remote attackers to execute arbitrary code in the context of the user running the affected application. Failed exploit attempts will likely cause a denial-of-service condition.

Solution:

VendorFix Update to PHP version 5.4.45, or 5.5.29, or 5.6.13 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.45

References:

- http://www.php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=70388

Unique Alert ID: 539157 Found on: 2023-10-06 Severity: High

OpenSSH Multiple Vulnerabilities Jan17 (Linux) (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-10009,CVE-2016-10010,CVE-2016-10011,CVE-2016-10012,CVE-2016-10708

Cvss Base: 7.5
Cvss Score: 7.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

openssh is prone to multiple vulnerabilities. Multiple flaws exist due to: - An 'authfile.c' script does not properly consider the effects of realloc on buffer contents. - The shared memory manager (associated with pre-authentication compression) does not ensure that a bounds check is enforced by all compilers. - The sshd in OpenSSH creates forwarded Unix-domain sockets as root, when privilege separation is not used. - An untrusted search path vulnerability in ssh-agent.c in ssh-agent. - NULL pointer dereference error due to an out-of-sequence NEWKEYS message. Successfully exploiting this issue allows local users to obtain sensitive private-key information, to gain privileges, conduct a senial-of-service condition and allows remote attackers to execute arbitrary local PKCS#11 modules.

Solution:

VendorFix Upgrade to OpenSSH version 7.4 or later.

Result:

Installed version: 6.6.1 Fixed version: 7.4 Installation path / port: 22/tcp

References:

- https://www.openssh.com/txt/release-7.4,http://www.openwall.com/lists/oss-security/2016/12/19/2,http://blog.swiecki.net/2018/01/fuzzing-tcp-servers.html,https://anongit.mindrot.org/openssh.git/commit/?id=28652bca29046f62c7045e933e6b931de1d16737

Unique Alert ID: 539163 Found on: 2023-10-06 Severity: High

PHP 'FastCGI Process Manager' Privilege Escalation Vulnerability (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-0185
Cvss Base: 7.2
Cvss Score: 7.2

Description:

PHP is prone to a privilege escalation vulnerability. The flaw is due to error in 'sapi/fpm/fpm/fpm_unix.c' within FastCGI Process Manager that sets insecure permissions for a unix socket. Successful exploitation will allow remote attackers to gain access to the socket and gain elevated privileges.

Solution:

VendorFix Update to PHP version 5.4.28 or 5.5.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.28/5.5.12

References:

- http://seclists.org/oss-sec/2014/q2/192,http://www.php.net/archive/2014.php#id2014-05-01-1,http://www.openwall.com/lists/oss-security/2014/04/29/5

Unique Alert ID: 539165 Found on: 2023-10-06 Severity: High

PHP 'FastCGI Process Manager' Privilege Escalation Vulnerability (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-0185
Cvss Base: 7.2
Cvss Score: 7.2

Description:

PHP is prone to a privilege escalation vulnerability. The flaw is due to error in 'sapi/fpm/fpm/fpm_unix.c' within FastCGI P rocess Manager that sets insecure permissions for a unix socket. Successful exploitation will allow remote attackers to ga in access to the socket and gain elevated privileges.

Solution:

VendorFix Update to PHP version 5.4.28 or 5.5.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.28/5.5.12

References:

- http://seclists.org/oss-sec/2014/q2/192,http://www.php.net/archive/2014.php#id2014-05-01-1,http://www.openwall .com/lists/oss-security/2014/04/29/5

Unique Alert ID: 539201 Found on: 2023-10-06 Severity: High

PHP 'make_http_soap_request' DoS / Information Disclosure Vulnerability - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-3185
Cvss Base: 7.1
Cvss Score: 7.1
Cvss Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) and an information disclosure vulnerability. The flaw is due an error in the 'mak e_http_soap_request' function of the 'ext/soap/php_http.c' script. Successfully exploiting this issue allow remote attacker s to obtain sensitive information from process memory or cause a denial of service.

Solution:

VendorFix Update to version 5.4.44, 5.5.28, 5.6.12, 7.0.4 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.44

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 539198 Found on: 2023-10-06 Severity: High

PHP 'make_http_soap_request' DoS / Information Disclosure Vulnerability - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-3185
Cvss Base: 7.1
Cvss Score: 7.1
Cvss Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) and an information disclosure vulnerability. The flaw is due an error in the 'make_http_soap_request' function of the 'ext/soap/php_http.c' script. Successfully exploiting this issue allow remote attackers to obtain sensitive information from process memory or cause a denial of service.

Solution:

VendorFix Update to version 5.4.44, 5.5.28, 5.6.12, 7.0.4 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.44

References:

- http://www.php.net/ChangeLog-5.php,http://www.php.net/ChangeLog-7.php

Unique Alert ID: 919551 Found on: 2023-10-06 Severity: High

OpenSSH 6.2 <= 8.7 Privilege Escalation Vulnerability (tcp/22)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2021-41617		
Cvss Base:	7.0		
Cvss Score:	7.0		
Cvss Vector:	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H		

Description:

OpenSSH is prone to a privilege scalation vulnerability in certain configurations. sshd failed to correctly initialise supplemental groups when executing an AuthorizedKeysCommand or AuthorizedPrincipalsCommand, where a AuthorizedKeysCommandUser or AuthorizedPrincipalsCommandUser directive has been set to run the command as a different user. Instead these commands would inherit the groups that sshd was started with. Depending on system configuration, inherited groups may allow AuthorizedKeysCommand/AuthorizedPrincipalsCommand helper programs to gain unintended privilege. Neither AuthorizedKeysCommand nor AuthorizedPrincipalsCommand are enabled by default in sshd_config.

Solution:

VendorFix Update to version 8.8 or later.

Result:

Installed version: 6.6.1 Fixed version: 8.8 Installation path / port: 22/tcp

References:

- https://www.openssh.com/txt/release-8.8

Unique Alert ID: 919550 Found on: 2023-10-06 Severity: High

PHP 5.3.7 - 7.3.31, 7.4.x < 7.4.25, 8.0.x < 8.0.12 Security Update (Oct 2021) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2021-21703		
Cvss Base:	7.0		
Cvss Score:	7.0		
Cvss Vector:	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP released new versions which includes a security fix. Fixed bug #81026 (PHP-FPM oob R/W in root process leading to privilege escalation).

Solution:

VendorFix Update to version 7.3.32 (not released yet), 7.4.25, 8.0.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.32 (not released yet) Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.32,https://www.php.net/ChangeLog-7.php#7.4.25,https://www.php.net/ChangeLog-8.php#8.0.12,http://bugs.php.net/81026,https://www.ambionics.io/blog/php-fpm-local-root

Unique Alert ID: 919549 Found on: 2023-10-06 Severity: High

PHP 5.3.7 - 7.3.31, 7.4.x < 7.4.25, 8.0.x < 8.0.12 Security Update (Oct 2021) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2021-21703		
Cvss Base:	7.0		
Cvss Score:	7.0		
Cvss Vector:	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H		

Description:

PHP released new versions which includes a security fix. Fixed bug #81026 (PHP-FPM oob R/W in root process leading to privilege escalation).

Solution:

VendorFix Update to version 7.3.32 (not released yet), 7.4.25, 8.0.12 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.32 (not released yet) Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.32,https://www.php.net/ChangeLog-7.php#7.4.25,https://www.php.net/ChangeLog-8.php#8.0.12,http://bugs.php.net/81026,https://www.ambionics.io/blog/php-fpm-local-root

Unique Alert ID: 539116 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities - 05 - Aug16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-4644,CVE-2015-4643,CVE-2015-4598		
Cvss Base:	6.5		
Cvss Score:	6.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N		

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws exist due to: - Improper validation of token extraction for table names, in the php_pgsql_meta_data function in pgsql.c in the PostgreSQL extension. - Integer overflow in the ftp_genlist function in ext/ftp/ftp.c - PHP does not ensure that pathnames lack %00 sequences. Successfully exploiting this issue allow remote attackers to cause a denial of service, to read or write to arbitrary files, also execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow.

Solution:

VendorFix Update to PHP version 5.4.42, or 5.5.26, or 5.6.10, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.42

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539118 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities - 05 - Aug16 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-4644,CVE-2015-4643,CVE-2015-4598
Cvss Base: 6.5
Cvss Score: 6.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws exist due to: - Improper validation of token extraction for table na mes, in the php_pgsql_meta_data function in pgsql.c in the PostgreSQL extension. - Integer overflow in the ftp_genlist fu nction in ext/ftp/ftp.c - PHP does not ensure that pathnames lack %00 sequences. Successfully exploiting this issue allow remote attackers to cause a denial of service, to read or write to arbitrary files, also execute arbitrary code via a long re ply to a LIST command, leading to a heap-based buffer overflow.

Solution:

VendorFix Update to PHP version 5.4.42, or 5.5.26, or 5.6.10, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.42

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539052 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities - 03 - Jun15 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-3329,CVE-2015-3307,CVE-2015-2783,CVE-2015-1352,CVE-2015-4599,CVE-2015-4600,CVE-2015-4602,CVE-2015-4603,CVE-2015-4604,CVE-2015-4605,CVE-2015-3411,CVE-2015-3412
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Multiple stack-based buffer overflows in the 'phar_set_ inode' function in phar_internal.h script in PHP. - Vulnerabilities in 'phar_parse_metadata' and 'phar_parse_pharfile' functi ons in ext/phar/phar.c script in PHP. - A NULL pointer dereference flaw in the 'build_tablename' function in 'ext/pgsql/pgs ql.c' script that is triggered when handling NULL return values for 'token'. Successfully exploiting this issue allow remote a ttackers to cause a denial of service, to obtain sensitive information from process memory and to execute arbitrary code via crafted dimensions.

Solution:

VendorFix Update to PHP 5.4.40 or 5.5.24 or 5.6.8 or later.

Result:

Installed Version: 5.4.16 Fixed Version: 5.4.40

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=69085,http://openwall.com/lists/oss-security/201 5/06/01/4

Unique Alert ID: 539180 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server Multiple Vulnerabilities Apr18 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2018-1312,CVE-2018-1283,CVE-2017-15715,CVE-2017-15710,CVE-2018-1301		
Cvss Base:	5.9		
Cvss Score:	5.9		
Cvss Vector:	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Multiple flaws exist due to: - Apache HTTP Server fails to correctl y generate the nonce sent to prevent reply attacks. - Misconfigured mod_session variable, HTTP_SESSION. - Apache HTT P Server fails to sanitize the expression specified in ''. - An error in Apache HTTP Server 'mod_authnz_ldap' when configu red with AuthLDAPCharsetConfig. - Apache HTTP Server fails to sanitize against a specially crafted request. Successful e xploitation will allow an attacker to replay HTTP requests across servers without detection, influence the user content, upl oad a malicious file, crash the Apache HTTP Server and perform denial of service attack.

Solution:

VendorFix Update to version 2.4.30 or later. Please see the references for more information.

Result:

Installed version: 2.4.6 Fixed version: 2.4.30 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539171 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server Multiple Vulnerabilities Apr18 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2018-1312,CVE-2018-1283,CVE-2017-15715,CVE-2017-15710,CVE-2018-1301		
Cvss Base:	5.9		
Cvss Score:	5.9		
Cvss Vector:	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Multiple flaws exist due to: - Apache HTTP Server fails to correctl y generate the nonce sent to prevent reply attacks. - Misconfigured mod_session variable, HTTP_SESSION. - Apache HTT P Server fails to sanitize the expression specified in ''. - An error in Apache HTTP Server 'mod_authnz_ldap' when configu red with AuthLDAPCharsetConfig. - Apache HTTP Server fails to sanitize against a specially crafted request. Successful e xploitation will allow an attacker to replay HTTP requests across servers without detection, influence the user content, upl oad a malicious file, crash the Apache HTTP Server and perform denial of service attack.

Solution:

VendorFix Update to version 2.4.30 or later. Please see the references for more information.

Result:

Installed version: 2.4.6 Fixed version: 2.4.30 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539071 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities - 03 - Jun15 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2015-3329,CVE-2015-3307,CVE-2015-2783,CVE-2015-1352,CVE-2015-4599,CVE-2015-4600,CVE-2015-4602,CVE-2015-4603,CVE-2015-4604,CVE-2015-4605,CVE-2015-3411,CVE-2015-3412	
Cvss Base:	5.3	
Cvss Score:	5.3	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Multiple stack-based buffer overflows in the 'phar_set_inode' function in phar_internal.h script in PHP. - Vulnerabilities in 'phar_parse_metadata' and 'phar_parse_pharfile' functions in ext/phar/phar.c script in PHP. - A NULL pointer dereference flaw in the 'build_tablename' function in 'ext/pgsql/pgsql.c' script that is triggered when handling NULL return values for 'token'. Successfully exploiting this issue allow remote attackers to cause a denial of service, to obtain sensitive information from process memory and to execute arbitrary code via crafted dimensions.

Solution:

VendorFix Update to PHP 5.4.40 or 5.5.24 or 5.6.8 or later.

Result:

Installed Version: 5.4.16 Fixed Version: 5.4.40

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=69085,http://openwall.com/lists/oss-security/2015/06/01/4

Unique Alert ID: 539186 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities May18 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2018-10549,CVE-2018-10546,CVE-2018-10548,CVE-2018-10547	
Cvss Base:	6.1	
Cvss Score:	6.1	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws exist due to - An out of bounds read error in 'exif_read_data' function while processing crafted JPG data. - An error in stream filter 'convert.iconv' which leads to infinite loop on invalid sequence. - An error in the LDAP module of PHP which allows a malicious LDAP server or man-in-the-middle attacker to crash PHP. - An error in the 'phar_do_404()' function in 'ext/phar/phar_object.c' script which returns parts of the request unfiltered, leading to another XSS vector. This is due to incomplete fix for CVE-2018-5712. Successful exploitation will allow an attacker to conduct XSS attacks, crash PHP, conduct denial-of-service condition and execute arbitrary code in the context of the affected application.

Solution:

VendorFix Update to version 7.2.5 or 7.0.30 or 5.6.36 or 7.1.17 or later. Please see the references for more information.

Result:

Installed version: 5.4.16 Fixed version: 5.6.36 Installation path / port: 443/tcp

References:

- http://www.php.net/ChangeLog-5.php#5.6.36,http://www.php.net/ChangeLog-7.php#7.0.30,http://www.php.net/ChangeLog-7.php#7.1.17,http://www.php.net/ChangeLog-7.php#7.2.5

Unique Alert ID: 539174 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities May18 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2018-10549,CVE-2018-10546,CVE-2018-10548,CVE-2018-10547	
Cvss Base:	6.1	
Cvss Score:	6.1	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws exist due to - An out of bounds read error in 'exif_read_data' function while processing crafted JPG data. - An error in stream filter 'convert.iconv' which leads to infinite loop on invalid sequence. - An error in the LDAP module of PHP which allows a malicious LDAP server or man-in-the-middle attacker to crash PHP. - An error in the 'phar_do_404()' function in 'ext/phar/phar_object.c' script which returns parts of the request unfiltered, leading to another XSS vector. This is due to incomplete fix for CVE-2018-5712. Successful exploitation will allow an attacker to conduct XSS attacks, crash PHP, conduct denial-of-service condition and execute arbitrary code in the context of the affected application.

Solution:

VendorFix Update to version 7.2.5 or 7.0.30 or 5.6.36 or 7.1.17 or later. Please see the references for more information.

Result:

Installed version: 5.4.16 Fixed version: 5.6.36 Installation path / port: 80/tcp

References:

- http://www.php.net/ChangeLog-5.php#5.6.36,http://www.php.net/ChangeLog-7.php#7.0.30,http://www.php.net/ChangeLog-7.php#7.1.17,http://www.php.net/ChangeLog-7.php#7.2.5

Unique Alert ID: 539083 Found on: 2023-10-06 Severity: Medium

OpenSSH Denial of Service And User Enumeration Vulnerabilities (Linux) (tcp/22)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-6515,CVE-2016-6210	
Cvss Base:	5.9	
Cvss Score:	5.9	
Cvss Vector:	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	

Description:

openssh is prone to denial of service and user enumeration vulnerabilities. Multiple flaws exist due to: - The auth_password function in 'auth-passwd.c' script does not limit password lengths for password authentication. - The sshd in OpenSSH, when SHA256 or SHA512 are used for user password hashing uses BLOWFISH hashing on a static password when the username does not exist and it takes much longer to calculate SHA256/SHA512 hash than BLOWFISH hash. Successfully exploiting this issue allows remote attackers to cause a denial of service (crypt CPU consumption) and to enumerate users by leveraging the timing difference between responses when a large password is provided.

Solution:

VendorFix Upgrade to OpenSSH version 7.3 or later.

Result:

Installed version: 6.6.1 Fixed version: 7.3 Installation path / port: 22/tcp

References:

- http://www.openssh.com/txt/release-7.3,http://seclists.org/fulldisclosure/2016/Jul/51,https://security-tracker.debian.org/tracker/CVE-2016-6210,http://openwall.com/lists/oss-security/2016/08/01/2

Unique Alert ID: 539271 Found on: 2023-10-06 Severity: Medium

OpenSSL: 1.0.2 < 1.0.2p / 1.1.0 < 1.1.0i Multiple Vulnerabilities (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2018-0732,CVE-2018-0737		
Cvss Base:	5.9		
Cvss Score:	5.9		
Cvss Vector:	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N		

Description:

OpenSSL is prone to multiple vulnerabilities. The flaws exist due to: - During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client (CVE-2018-0732). - The Open SSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack (CVE-2018-07 37). Successful exploitation will allow a remote attacker: - to cause the client to spend an unreasonably long period of ti me generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack (CVE-2018-0732). - with sufficient access to mount cache timing attacks during the RSA key generation pr ocess could recover the private key (CVE-2018-0737).

Solution:

VendorFix Upgrade to OpenSSL version 1.1.0i or 1.0.2p or later. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2p Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20180416.txt,https://www.openssl.org/news/secadv/20180612.txt,http://seclists.org/oss-sec/2018/q2/50,https://github.com/openssl/openssl/commit/ea7abeeabf92b7aca160bdd0208636d4da69f4f4,https://github.com/openssl/openssl/commit/3984ef0b72831da8b3ece4745cac4f8575b19098,https://github.com/openssl/openssl/commit/6939eab03a6e23d2bd2c3f5e34fe1d48e542e787,https://github.com/openssl/openssl/commit/349a41da1ad88ad87825414752a8ff5fdd6a6c3f

Unique Alert ID: 607309 Found on: 2023-10-06 Severity: Medium

OpenSSL: 1.0.2 < 1.0.2p / 1.1.0 < 1.1.0i Multiple Vulnerabilities (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-12-18
CVE ID:	CVE-2018-0732,CVE-2018-0737		
Cvss Base:	5.9		
Cvss Score:	5.9		
Cvss Vector:	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N		

Description:

OpenSSL is prone to multiple vulnerabilities. The flaws exist due to: - During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client (CVE-2018-0732). - The Open SSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack (CVE-2018-07 37). Successful exploitation will allow a remote attacker: - to cause the client to spend an unreasonably long period of ti me generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack (CVE-2018-0732). - with sufficient access to mount cache timing attacks during the RSA key generation pr ocess could recover the private key (CVE-2018-0737).

Solution:

VendorFix Upgrade to OpenSSL version 1.1.0i or 1.0.2p or later. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2p Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20180416.txt,https://www.openssl.org/news/secadv/20180612.txt,http://seclists.org/oss-sec/2018/q2/50,https://github.com/openssl/openssl/commit/ea7abeeabf92b7aca160bdd0208636d4da69

f4f4,https://github.com/openssl/openssl/commit/3984ef0b72831da8b3ece4745cac4f8575b19098,https://github.com/openssl/openssl/commit/6939eab03a6e23d2bd2c3f5e34fe1d48e542e787,https://github.com/openssl/openssl/commit/349a41da1ad88ad87825414752a8ff5fdd6a6c3f

Unique Alert ID: 539187 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities - Sep19 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 6.8
Cvss Score: 6.8

Description:

PHP is prone to multiple vulnerabilities. PHP is prone to multiple vulnerabilities: - Buffer overflow in zendparse - Cast to object confuses GC, causes crash - Exif crash (bus error) due to wrong alignment and invalid cast - Use-after-free in FPM master event handling

Solution:

VendorFix Update to version 7.2.22, 7.3.9 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.22 Installation path / port: 443/tcp

References:

- http://bugs.php.net/78363,http://bugs.php.net/78379,http://bugs.php.net/78333,http://bugs.php.net/77185,https://www.php.net/ChangeLog-7.php#7.3.9,https://www.php.net/ChangeLog-7.php#7.2.22

Unique Alert ID: 539190 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities - 04 - Jun15 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-3330
Cvss Base: 6.8
Cvss Score: 6.8

Description:

PHP is prone to multiple vulnerabilities. The flaw is due to vulnerability in 'php_handler' function in sapi/apache2handler/sapi_apache2.c script in PHP. Successfully exploiting this issue allow remote attackers to cause a denial of service or possibly execute arbitrary code via pipelined HTTP requests.

Solution:

VendorFix Update to PHP 5.4.40 or 5.5.24 or 5.6.8 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.40 Installation path / port: 80/tcp

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=69085,http://openwall.com/lists/oss-security/2015/06/01/4

Unique Alert ID: 539176 Found on: 2023-10-06 Severity: Medium

PHP Heap Use-After-Free Vulnerability - Sep19 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 6.8
Cvss Score: 6.8

Description:

PHP is prone to a heap-based use-after-free vulnerability. PHP is prone to a heap use-after-free in pcrelib (cmb).

Solution:

VendorFix Update to version 7.1.32 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.1.32 Installation path / port: 443/tcp

References:

- http://bugs.php.net/75457,https://www.php.net/ChangeLog-7.php#7.1.32

Unique Alert ID: 539177 Found on: 2023-10-06 Severity: Medium

PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-7804,CVE-2015-7803		
Cvss Base:	6.8		
Cvss Score:	6.8		

Description:

PHP is prone to multiple denial of service (DoS) vulnerabilities. Multiple flaws are due to: - An Off-by-one error in the 'phar_parse_zipfile' function within ext/phar/zip.c script. - An error in the 'phar_get_entry_data' function in ext/phar/util.c script. Successfully exploiting this issue allow remote attackers to cause a denial of service (NULL pointer dereference and application crash).

Solution:

VendorFix Update to PHP 5.5.30 or 5.6.14 or later.

Result:

Installed Version: 5.4.16 Fixed Version: 5.5.30

References:

- http://www.php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=70433,http://www.openwall.com/lists/oss-security/2015/10/05/8

Unique Alert ID: 919552 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server Multiple Vulnerabilities (Sep 2014) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2013-5704,CVE-2014-0118,CVE-2014-0226,CVE-2014-0231		
Cvss Base:	6.8		
Cvss Score:	6.8		

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2013-5704: HTTP trailers could be used to replace HTTP headers late during request processing, potentially undoing or otherwise confusing modules that examined or modified request headers earlier. This fix adds the 'MergeTrailers' directive to restore legacy behavior. - CVE-2014-0118: A resource consumption flaw was found in mod_deflate. If request body decompression was configured (using the 'DEFLATE' input filter), a remote attacker could cause the server to consume significant memory and/or CPU resources. The use of request body decompression is not a common configuration. - CVE-2014-0226: A race condition was found in mod_status. An attacker able to access a public server status page on a server using a threaded MPM could

send a carefully crafted request which could lead to a heap buffer overflow. Note that it is not a default or recommended configuration to have a public accessible server status page. - CVE-2014-0231: A flaw was found in mod_cgid. If a server using mod_cgid hosted CGI scripts which did not consume standard input, a remote attacker could cause child processes to hang indefinitely, leading to denial of service.

Solution:

VendorFix Update to version 2.2.29, 2.4.12 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.12 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_22.html,https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 1050985 Found on: 2023-10-06 Severity: Medium

PHP Sessions Subsystem Session Fixation Vulnerability (Aug 2013) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-11-05
CVE ID:	CVE-2011-4718		
Cvss Base:	6.8		
Cvss Score:	6.8		

Description:

PHP is prone to a session fixation vulnerability. Session fixation vulnerability in the Sessions subsystem in PHP allows rem ote attackers to hijack web sessions by specifying a session ID.

Solution:

VendorFix - Update to PHP version 5.5.2 or later and set 'session.use_strict_mode' in php.ini to 'On' - make adoptive session with user land code as described in the referenced PHP strict_sessions document

Result:

Installed version: 5.4.16 Fixed version: 5.5.2 Installation path / port: 80/tcp

References:

- https://wiki.php.net/rfc/strict_sessions,https://wiki.php.net/rfc/strict_sessions#current_solution,https://access.redhat.com/security/cve/cve-2011-4718,http://secunia.com/advisories/54562,http://cxsecurity.com/cveshow/CVE-2011-4718

Unique Alert ID: 539188 Found on: 2023-10-06 Severity: Medium

PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-7804,CVE-2015-7803		
Cvss Base:	6.8		
Cvss Score:	6.8		

Description:

PHP is prone to multiple denial of service (DoS) vulnerabilities. Multiple flaws are due to: - An Off-by-one error in the 'ph ar_parse_zipfile' function within ext/phar/zip.c script. - An error in the 'phar_get_entry_data' function in ext/phar/util.c sc ript. Successfully exploiting this issue allow remote attackers to cause a denial of service (NULL pointer dereference and application crash).

Solution:

VendorFix Update to PHP 5.5.30 or 5.6.14 or later.

Result:

Installed Version: 5.4.16 Fixed Version: 5.5.30

References:

- http://www.php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=70433,http://www.openwall.com/lists/oss-security/2015/10/05/8

Unique Alert ID: 1050987 Found on: 2023-10-06 Severity: Medium

PHP < 7.4.31, 8.0.x < 8.0.24, 8.1.x < 8.1.11 Security Update - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-11-05
CVE ID: CVE-2022-31628,CVE-2022-31629
Cvss Base: 6.5
Cvss Score: 6.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

Description:

PHP is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2022-31628: The phar uncompressor code would recursively uncompress 'quines' gzip files, resulting in an infinite loop. - CVE-2022-31629: The vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a '__Host-' or '__Secure-' cookie by PHP applications.

Solution:

VendorFix Update to version 7.4.31, 8.0.24, 8.1.11 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.4.31 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.4.31,https://www.php.net/ChangeLog-8.php#8.0.24,https://www.php.net/ChangeLog-8.php#8.1.11,https://bugs.php.net/bug.php?id=81726,https://bugs.php.net/bug.php?id=81727

Unique Alert ID: 539184 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities - 04 - Jun15 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-3330
Cvss Base: 6.8
Cvss Score: 6.8

Description:

PHP is prone to multiple vulnerabilities. The flaw is due to vulnerability in 'php_handler' function in sapi/apache2handler/sapi_apache2.c script in PHP. Successfully exploiting this issue allow remote attackers to cause a denial of service or possibly execute arbitrary code via pipelined HTTP requests.

Solution:

VendorFix Update to PHP 5.4.40 or 5.5.24 or 5.6.8 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.40 Installation path / port: 443/tcp

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=69085,http://openwall.com/lists/oss-security/2015/06/01/4

Unique Alert ID: 539173 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server Multiple Vulnerabilities May15 (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2014-3523,CVE-2014-0118,CVE-2014-0226,CVE-2014-0231	
Cvss Base:	6.8	
Cvss Score:	6.8	

Description:

Apache HTTP Server is prone to a denial of service vulnerability. Multiple flaws are due to: - Vulnerability in the WinNT MPM component within the 'winnt_accept' function in server/mpm/winnt/child.c script that is triggered when the default AcceptFilter is used. - Vulnerability in the mod_deflate module that is triggered when handling highly compressed bodies. - A race condition in the mod_status module that is triggered as user-supplied input is not properly validated when handling the scoreboard. - Vulnerability in the mod_cgid module that is triggered when used to host CGI scripts that do not consume standard input. Successful exploitation will allow a remote attacker to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives.

Solution:

VendorFix Update to version 2.4.10 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.10 Installation path / port: 443/tcp

References:

- http://httpd.apache.org/security/vulnerabilities_24.html,http://www.rapid7.com/db/vulnerabilities/apache-httpd-cve-2014-8109

Unique Alert ID: 539182 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server Multiple Vulnerabilities May15 (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2014-3523,CVE-2014-0118,CVE-2014-0226,CVE-2014-0231	
Cvss Base:	6.8	
Cvss Score:	6.8	

Description:

Apache HTTP Server is prone to a denial of service vulnerability. Multiple flaws are due to: - Vulnerability in the WinNT MPM component within the 'winnt_accept' function in server/mpm/winnt/child.c script that is triggered when the default AcceptFilter is used. - Vulnerability in the mod_deflate module that is triggered when handling highly compressed bodies. - A race condition in the mod_status module that is triggered as user-supplied input is not properly validated when handling the scoreboard. - Vulnerability in the mod_cgid module that is triggered when used to host CGI scripts that do not consume standard input. Successful exploitation will allow a remote attacker to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives.

Solution:

VendorFix Update to version 2.4.10 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.10 Installation path / port: 80/tcp

References:

- http://httpd.apache.org/security/vulnerabilities_24.html,http://www.rapid7.com/db/vulnerabilities/apache-httpd-cve-2014-8109

Unique Alert ID: 1050984 Found on: 2023-10-06 Severity: Medium

PHP Sessions Subsystem Session Fixation Vulnerability (Aug 2013) (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-11-05
CVE ID: CVE-2011-4718
Cvss Base: 6.8
Cvss Score: 6.8

Description:

PHP is prone to a session fixation vulnerability. Session fixation vulnerability in the Sessions subsystem in PHP allows rem ote attackers to hijack web sessions by specifying a session ID.

Solution:

VendorFix - Update to PHP version 5.5.2 or later and set 'session.use_strict_mode' in php.ini to 'On' - make adoptive session with user land code as described in the referenced PHP strict_sessions document

Result:

Installed version: 5.4.16 Fixed version: 5.5.2 Installation path / port: 443/tcp

References:

- https://wiki.php.net/rfc/strict_sessions,https://wiki.php.net/rfc/strict_sessions#current_solution,https://access.redhat.com/security/cve/cve-2011-4718,http://secunia.com/advisories/54562,http://cxsecurity.com/cveshow/CVE-2011-4718

Unique Alert ID: 539183 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities - Sep19 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 6.8
Cvss Score: 6.8

Description:

PHP is prone to multiple vulnerabilities. PHP is prone to multiple vulnerabilities: - Buffer overflow in zendparse - Cast to o bject confuses GC, causes crash - Exif crash (bus error) due to wrong alignment and invalid cast - Use-after-free in FPM master event handling

Solution:

VendorFix Update to version 7.2.22, 7.3.9 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.22 Installation path / port: 80/tcp

References:

- http://bugs.php.net/78363,http://bugs.php.net/78379,http://bugs.php.net/78333,http://bugs.php.net/77185,https://www.php.net/ChangeLog-7.php#7.3.9,https://www.php.net/ChangeLog-7.php#7.2.22

Unique Alert ID: 539175 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities - 01 - Aug14 (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-3597,CVE-2014-3587,CVE-2014-5120		
Cvss Base:	6.8		
Cvss Score:	6.8		

Description:

PHP is prone to multiple vulnerabilities. The flaws exist due to: - Multiple overflow conditions in the 'php_parserr' function within ext/standard/dns.c script. - Integer overflow in the 'cdf_read_property_info' function in cdf.c within the Fileinfo com ponent. - An error in the '_php_image_output_ctx' function within ext/gd/gd_ctx.c script as NULL bytes in paths to various image handling functions are not stripped. Successful exploitation will allow remote attackers to overwrite arbitrary files, conduct denial of service attacks or potentially execute arbitrary code.

Solution:

VendorFix Update to PHP version 5.4.32 or 5.5.16 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.32/5.5.16

References:

- http://php.net/ChangeLog-5.php,http://secunia.com/advisories/59709,http://secunia.com/advisories/57349

Unique Alert ID: 1050986 Found on: 2023-10-06 Severity: Medium

PHP < 7.4.31, 8.0.x < 8.0.24, 8.1.x < 8.1.11 Security Update - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-11-05
CVE ID:	CVE-2022-31628,CVE-2022-31629		
Cvss Base:	6.5		
Cvss Score:	6.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N		

Description:

PHP is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2022-31628: The phar uncompressor co de would recursively uncompress 'quines' gzip files, resulting in an infinite loop. - CVE-2022-31629: The vulnerability ena bles network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a '__H ost-' or '__Secure-' cookie by PHP applications.

Solution:

VendorFix Update to version 7.4.31, 8.0.24, 8.1.11 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.4.31 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.4.31,https://www.php.net/ChangeLog-8.php#8.0.24,https://www.php.net/ChangeLog-8.php#8.1.11,https://bugs.php.net/bug.php?id=81726,https://bugs.php.net/bug.php?id=81727

Unique Alert ID: 539181 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities - 01 - Aug14 (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-3597,CVE-2014-3587,CVE-2014-5120		
Cvss Base:	6.8		
Cvss Score:	6.8		

Description:

PHP is prone to multiple vulnerabilities. The flaws exist due to: - Multiple overflow conditions in the 'php_parserr' function within ext/standard/dns.c script. - Integer overflow in the 'cdf_read_property_info' function in cdf.c within the Fileinfo com ponent. - An error in the '_php_image_output_ctx' function within ext/gd/gd_ctx.c script as NULL bytes in paths to various image handling functions are not stripped. Successful exploitation will allow remote attackers to overwrite arbitrary files, conduct denial of service attacks or potentially execute arbitrary code.

Solution:

VendorFix Update to PHP version 5.4.32 or 5.5.16 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.32/5.5.16

References:

- http://php.net/ChangeLog-5.php,http://secunia.com/advisories/59709,http://secunia.com/advisories/57349

Unique Alert ID: 539169 Found on: 2023-10-06 Severity: Medium

PHP Heap Use-After-Free Vulnerability - Sep19 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
Cvss Base:	6.8		
Cvss Score:	6.8		

Description:

PHP is prone to a heap-based use-after-free vulnerability. PHP is prone to a heap use-after-free in pcrelib (cmb).

Solution:

VendorFix Update to version 7.1.32 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.1.32 Installation path / port: 80/tcp

References:

- http://bugs.php.net/75457,https://www.php.net/ChangeLog-7.php#7.1.32

Unique Alert ID: 919553 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server Multiple Vulnerabilities (Sep 2014) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2013-5704,CVE-2014-0118,CVE-2014-0226,CVE-2014-0231
Cvss Base: 6.8
Cvss Score: 6.8

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2013-5704: HTTP trailers could be used to replace HTTP headers late during request processing, potentially undoing or otherwise confusing modules that examined or modified request headers earlier. This fix adds the 'MergeTrailers' directive to restore legacy behavior. - CVE-2014-0118: A resource consumption flaw was found in mod_deflate. If request body decompression was configured (using the 'DEFLATE' input filter), a remote attacker could cause the server to consume significant memory and/or CPU resources. The use of request body decompression is not a common configuration. - CVE-2014-0226: A race condition was found in mod_status. An attacker able to access a public server status page on a server using a threaded MPM could send a carefully crafted request which could lead to a heap buffer overflow. Note that it is not a default or recommended configuration to have a public accessible server status page. - CVE-2014-0231: A flaw was found in mod_cgid. If a server using mod_cgid hosted CGI scripts which did not consume standard input, a remote attacker could cause child processes to hang indefinitely, leading to denial of service.

Solution:

VendorFix Update to version 2.2.29, 2.4.12 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.12 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_22.html,https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539168 Found on: 2023-10-06 Severity: Medium

PHP 'PHP-FPM' Denial of Service Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-9253
Cvss Base: 6.5
Cvss Score: 6.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw exists due to the php-fpm master process restarts a child process in an endless loop when using program execution functions with a non-blocking STDIN stream. Successfully exploitation will allow an attacker to consume 100% of the CPU, and consume disk space with a large volume of error logs, as demonstrated by an attack by a customer of a shared-hosting facility.

Solution:

VendorFix Update to PHP 7.1.20, 7.2.8 or 7.3.0alpha3.

Result:

Installed version: 5.4.16 Fixed version: 7.1.20 Installation path / port: 80/tcp

References:

- https://bugs.php.net/bug.php?id=73342,https://bugs.php.net/bug.php?id=70185,https://github.com/php/php-src/pull/3287,https://www.futureweb.at/security/CVE-2015-9253

Unique Alert ID: 539170 Found on: 2023-10-06 Severity: Medium

PHP 'PHP-FPM' Denial of Service Vulnerability (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-9253		
Cvss Base:	6.5		
Cvss Score:	6.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw exists due to the php-fpm master process restarts a child process in an endless loop when using program execution functions with a non-blocking STDIN stream. Successfully exploitation will allow an attacker to consume 100% of the CPU, and consume disk space with a large volume of error logs, as demonstrated by an attack by a customer of a shared-hosting facility.

Solution:

VendorFix Update to PHP 7.1.20, 7.2.8 or 7.3.0alpha3.

Result:

Installed version: 5.4.16 Fixed version: 7.1.20 Installation path / port: 443/tcp

References:

- https://bugs.php.net/bug.php?id=73342,https://bugs.php.net/bug.php?id=70185,https://github.com/php/php-src/pull/3287,https://www.futureweb.at/security/CVE-2015-9253

Unique Alert ID: 919554 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.31, 7.4.x < 7.4.24, 8.0.x < 8.0.11 Security Update (Sep 2021) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2021-21706		
Cvss Base:	6.5		
Cvss Score:	6.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N		

Description:

PHP released new versions which includes a security fix. Fixed bug #81420 (ZipArchive::extractTo extracts outside of destination).

Solution:

VendorFix Update to version 7.3.31, 7.4.24, 8.0.11 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.31 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.31,https://www.php.net/ChangeLog-7.php#7.4.24,https://www.php.net/ChangeLog-8.php#8.0.11,http://bugs.php.net/81420

Unique Alert ID: 919559 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.31, 7.4.x < 7.4.24, 8.0.x < 8.0.11 Security Update (Sep 2021) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2021-21706		
Cvss Base:	6.5		
Cvss Score:	6.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N		

Description:

PHP released new versions which includes a security fix. Fixed bug #81420 (ZipArchive::extractTo extracts outside of des tination).

Solution:

VendorFix Update to version 7.3.31, 7.4.24, 8.0.11 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.31 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.31,https://www.php.net/ChangeLog-7.php#7.4.24,https://www.php.net/ChangeLog-8.php#8.0.11,http://bugs.php.net/81420

Unique Alert ID: 539196 Found on: 2023-10-06 Severity: Medium

PHP < 7.2.26 Multiple Vulnerabilities - Dec19 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2019-11046,CVE-2019-11045,CVE-2019-11050,CVE-2019-11047		
Cvss Base:	6.5		
Cvss Score:	6.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L		

Description:

PHP is prone to multiple vulnerabilities. PHP is prone to multiple vulnerabilities: - Buffer underflow in bc_shift_addsub (CV E-2019-11046) - DirectoryIterator class silently truncates after a null byte (CVE-2019-11045) - Use-after-free in exif pars ing under memory sanitizer (CVE-2019-11050) - Heap-buffer-overflow READ in exif (CVE-2019-11047)

Solution:

VendorFix Update to version 7.2.26 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.26 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.26

Unique Alert ID: 919558 Found on: 2023-10-06 Severity: Medium

PHP < 7.2.34, 7.3 < 7.3.23, 7.4 < 7.4.11 Multiple Vulnerabilities - October20 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2020-7069,CVE-2020-7070		
Cvss Base:	5.3		
Cvss Score:	5.3		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N		

Description:

PHP is prone to multiple vulnerabilities. The following vulnerabilities exist: - Wrong ciphertext/tag in AES-CCM encryption for a 12 bytes IV (CVE-2020-7069) - PHP parses encoded cookie names so malicious '__Host-' cookies can be sent (CVE-2020-7070)

Solution:

VendorFix Update to version 7.2.34, 7.3.23, 7.4.11 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.34 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.34,https://www.php.net/ChangeLog-7.php#7.3.23,https://www.php.net/ChangeLog-7.php#7.4.11

Unique Alert ID: 919555 Found on: 2023-10-06 Severity: Medium

PHP < 7.2.34, 7.3 < 7.3.23, 7.4 < 7.4.11 Multiple Vulnerabilities - October20 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2020-7069,CVE-2020-7070		
Cvss Base:	5.3		
Cvss Score:	5.3		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N		

Description:

PHP is prone to multiple vulnerabilities. The following vulnerabilities exist: - Wrong ciphertext/tag in AES-CCM encryption for a 12 bytes IV (CVE-2020-7069) - PHP parses encoded cookie names so malicious '__Host-' cookies can be sent (CVE-2020-7070)

Solution:

VendorFix Update to version 7.2.34, 7.3.23, 7.4.11 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.34 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.34,https://www.php.net/ChangeLog-7.php#7.3.23,https://www.php.net/ChangeLog-7.php#7.4.11

Unique Alert ID: 919556 Found on: 2023-10-06 Severity: Medium

OpenSSL DoS Vulnerability (20180327) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2018-0739		
Cvss Base:	6.5		
Cvss Score:	6.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H		

Description:

OpenSSL is prone to a denial of service (DoS) vulnerability. Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could resu lt in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so t his is considered safe. Reported by OSS-fuzz.

Solution:

VendorFix Update to version 1.0.2o, 1.1.0h or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2o Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20180327.txt

Unique Alert ID: 539194 Found on: 2023-10-06 Severity: Medium

PHP < 7.2.26 Multiple Vulnerabilities - Dec19 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2019-11046,CVE-2019-11045,CVE-2019-11050,CVE-2019-11047	
Cvss Base:	6.5	
Cvss Score:	6.5	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L	

Description:

PHP is prone to multiple vulnerabilities. PHP is prone to multiple vulnerabilities: - Buffer underflow in bc_shift_addsub (CVE-2019-11046) - DirectoryIterator class silently truncates after a null byte (CVE-2019-11045) - Use-after-free in exif parsing under memory sanitizer (CVE-2019-11050) - Heap-buffer-overflow READ in exif (CVE-2019-11047)

Solution:

VendorFix Update to version 7.2.26 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.26 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.26

Unique Alert ID: 919557 Found on: 2023-10-06 Severity: Medium

OpenSSL DoS Vulnerability (20180327) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2018-0739	
Cvss Base:	6.5	
Cvss Score:	6.5	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	

Description:

OpenSSL is prone to a denial of service (DoS) vulnerability. Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Reported by OSS-fuzz.

Solution:

VendorFix Update to version 1.0.2o, 1.1.0h or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2o Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20180327.txt

Unique Alert ID: 1533215 Found on: 2023-10-06 Severity: Medium

OpenSSL DoS Vulnerability (20230719) - Linux (tcp/80)

Open Status: NEW **First Found:** 2023-10-06
CVE ID: CVE-2023-3446

Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Description:

OpenSSL is prone to a denial of service (DoS) vulnerability. Checking excessively long DH keys or parameters may be v ery slow. Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH ke y or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtain ed from an untrusted source this may lead to a Denial of Service.

Solution:

NoneAvailable No known solution is available as of 19th July, 2023. Information regarding this issue will be updated once solution details are available. Vendor info: Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available. The fix is also available in commit fc9867c1 (for 3.1), commit 1fa20cf2 (for 3.0) and commit 8780a896 (for 1.1.1) in the OpenSSL git repository. It is available to premium support customer in commit 9a0a4d3c (for 1.0.2).

Result:

Installed version: 1.0.2k Fixed version: None Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20230719.txt

Unique Alert ID: 539216 Found on: 2023-10-06 Severity: Medium

OpenSSH <= 7.2p1 - Xauth Injection (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-3115
Cvss Base: 6.4
Cvss Score: 6.4
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

Description:

openssh xauth command injection may lead to forced-command and /bin/false bypass An authenticated user may inject arbitrary xauth commands by sending an x11 channel request that includes a newline character in the x11 cookie. The ne wline acts as a command separator to the xauth binary. This attack requires the server to have 'X11Forwarding yes' ena bled. Disabling it, mitigates this vector. By injecting xauth commands one gains limited* read/write arbitrary files, inform ation leakage or xauth-connect capabilities.

Solution:

VendorFix Upgrade to OpenSSH version 7.2p2 or later.

Result:

Installed version: 6.6.1 Fixed version: 7.2p2 Installation path / port: 22/tcp

References:

- http://www.openssh.com/txt/release-7.2p2

Unique Alert ID: 1533216 Found on: 2023-10-06 Severity: Medium

OpenSSL DoS Vulnerability (20230719) - Linux (tcp/443)

Open Status:	NEW	**First Found:**	2023-10-06
CVE ID:	CVE-2023-3446		
Cvss Base:	5.3		
Cvss Score:	5.3		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L		

Description:

OpenSSL is prone to a denial of service (DoS) vulnerability. Checking excessively long DH keys or parameters may be v ery slow. Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH ke y or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtain ed from an untrusted source this may lead to a Denial of Service.

Solution:

NoneAvailable No known solution is available as of 19th July, 2023. Information regarding this issue will be updated once solution details are available. Vendor info: Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available. The fix is also available in commit fc9867c1 (for 3.1), commit 1fa20cf2 (for 3.0) and commit 8780a896 (for 1.1.1) in the OpenSSL git repository. It is available to premium support customer in commit 9a0a4d3c (for 1.0.2).

Result:

Installed version: 1.0.2k Fixed version: None Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20230719.txt

Unique Alert ID: 919561 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server CRLF Injection Vulnerability (Dec 2016) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2016-4975		
Cvss Base:	6.1		
Cvss Score:	6.1		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N		

Description:

Apache HTTP Server is prone to a CRLF injection vulnerability. Possible CRLF injection allowing HTTP response splitting at tacks for sites which use mod_userdir. This issue was mitigated to prohibit CR or LF injection into the 'Location' or other o utbound header key or value.

Solution:

VendorFix Update to version 2.2.32, 2.4.25 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.25 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_22.html,https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539215 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 2.4.0 < 2.4.42 Multiple Vulnerabilities (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2020-1927,CVE-2020-1934
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Apache HTTP Server is prone to multiple vulnerabilities: - mod_rewrite CWE-601 open redirect (CVE-2020-1927) - mod_proxy_ftp use of uninitialized value (CVE-2020-1934)

Solution:

VendorFix Update to version 2.4.42 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.42 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539213 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 2.4.0 < 2.4.42 Multiple Vulnerabilities (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2020-1927,CVE-2020-1934
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Apache HTTP Server is prone to multiple vulnerabilities: - mod_rewrite CWE-601 open redirect (CVE-2020-1927) - mod_proxy_ftp use of uninitialized value (CVE-2020-1934)

Solution:

VendorFix Update to version 2.4.42 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.42 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539211 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 2.4.0 - 2.4.40 Multiple Vulnerabilities (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2019-10092,CVE-2019-10098
Cvss Base: 6.1
Cvss Score: 6.1
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Apache HTTP server is prone to multiple vulnerabilities: - A limite

d cross-site scripting issue affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed. (CVE-2019-10092) - Redirects co nfigured with mod_rewrite that were intended to be self referential might be fooled by encoded newlines and redirect inst ead to an unexpected URL within the request URL. (CVE-2019-10098)

Solution:

VendorFix Update to version 2.4.41 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.41 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 919560 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server CRLF Injection Vulnerability (Dec 2016) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2016-4975		
Cvss Base:	6.1		
Cvss Score:	6.1		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N		

Description:

Apache HTTP Server is prone to a CRLF injection vulnerability. Possible CRLF injection allowing HTTP response splitting at tacks for sites which use mod_userdir. This issue was mitigated to prohibit CR or LF injection into the 'Location' or other o utbound header key or value.

Solution:

VendorFix Update to version 2.2.32, 2.4.25 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.25 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_22.html,https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539209 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 2.4.0 - 2.4.40 Multiple Vulnerabilities (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2019-10092,CVE-2019-10098		
Cvss Base:	6.1		
Cvss Score:	6.1		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N		

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Apache HTTP server is prone to multiple vulnerabilities: - A limite d cross-site scripting issue affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed. (CVE-2019-10092) - Redirects co nfigured with mod_rewrite that were intended to be self referential might be fooled by encoded newlines and redirect inst ead to an unexpected URL within the request URL. (CVE-2019-10098)

Solution:

VendorFix Update to version 2.4.41 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.41 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539296 Found on: 2023-10-06 Severity: Medium

PHP 'PHAR' Error Page Reflected XSS And DoS Vulnerabilities (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2018-5712,CVE-2018-5711		
Cvss Base:	5.5		
Cvss Score:	5.5		
Cvss Vector:	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H		

Description:

PHP is prone to cross site scripting (XSS) and denial of service (DoS) vulnerabilities. Multiple flaws are due to: - An input validation error on the PHAR 404 error page via the URI of a request for a .phar file. - An integer signedness error in gd_gif_in.c in the GD Graphics Library (aka libgd). Successfully exploiting this issue allows attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks and will also lead to a denial of service and exhausting the server resources.

Solution:

VendorFix Update to PHP version 5.6.33, 7.0.27, 7.1.13 or 7.2.1 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.33 Installation path / port: 80/tcp

References:

- http://php.net/ChangeLog-5.php,http://php.net/ChangeLog-7.php,https://bugs.php.net/bug.php?id=74782,https://bugs.php.net/bug.php?id=75571

Unique Alert ID: 539300 Found on: 2023-10-06 Severity: Medium

PHP 'PHAR' Error Page Reflected XSS And DoS Vulnerabilities (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2018-5712,CVE-2018-5711		
Cvss Base:	5.5		
Cvss Score:	5.5		
Cvss Vector:	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H		

Description:

PHP is prone to cross site scripting (XSS) and denial of service (DoS) vulnerabilities. Multiple flaws are due to: - An input validation error on the PHAR 404 error page via the URI of a request for a .phar file. - An integer signedness error in gd_gif_in.c in the GD Graphics Library (aka libgd). Successfully exploiting this issue allows attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks and will also lead to a denial of service and exhausting the server resources.

Solution:

VendorFix Update to PHP version 5.6.33, 7.0.27, 7.1.13 or 7.2.1 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.33 Installation path / port: 443/tcp

References:

- http://php.net/ChangeLog-5.php,http://php.net/ChangeLog-7.php,https://bugs.php.net/bug.php?id=74782,https://bugs.php.net/bug.php?id=75571

Unique Alert ID: 539298 Found on: 2023-10-06 Severity: Medium

PHP Cross-Site Scripting Vulnerability - Aug16 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-8935
Cvss Base: 6.1
Cvss Score: 6.1
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Description:

PHP is prone to a cross-site scripting (XSS) vulnerability. The flaw is due to the 'sapi_header_op' function in 'main/SAPI.c' script supports deprecated line folding without considering browser compatibility. Successfully exploiting this issue allows remote attackers to conduct cross-site scripting (XSS) attacks against Internet Explorer by leveraging '%0A%20' or '%0 D%0A%20' mishandling in the header function.

Solution:

VendorFix Update to PHP version 5.4.38, or 5.5.22, or 5.6.6, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.38

References:

- https://bugs.php.net/bug.php?id=68978

Unique Alert ID: 539299 Found on: 2023-10-06 Severity: Medium

PHP Cross-Site Scripting Vulnerability - Aug16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-8935
Cvss Base: 6.1
Cvss Score: 6.1
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Description:

PHP is prone to a cross-site scripting (XSS) vulnerability. The flaw is due to the 'sapi_header_op' function in 'main/SAPI.c' script supports deprecated line folding without considering browser compatibility. Successfully exploiting this issue allows remote attackers to conduct cross-site scripting (XSS) attacks against Internet Explorer by leveraging '%0A%20' or '%0 D%0A%20' mishandling in the header function.

Solution:

VendorFix Update to PHP version 5.4.38, or 5.5.22, or 5.6.6, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.38

References:

- https://bugs.php.net/bug.php?id=68978

Unique Alert ID: 539167 Found on: 2023-10-06 Severity: Medium

PHP Denial of Service Vulnerability - 01 - Jul16 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-8878		
Cvss Base:	5.9		
Cvss Score:	5.9		
Cvss Vector:	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to script 'main/php_open_temporary_file.c' does n ot ensure thread safety. Successfully exploiting this issue allow remote attackers to cause a denial of service (race condit ion and heap memory corruption) by leveraging an application that performs many temporary-file accesses.

Solution:

VendorFix Update to PHP version 5.5.28, or 5.6.12, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.28

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 919562 Found on: 2023-10-06 Severity: Medium

OpenSSL: Null pointer deref in X509_issuer_and_serial_hash() (CVE-2021-23841) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2021-23841		
Cvss Base:	5.9		
Cvss Score:	5.9		
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

OpenSSL is prone to a denial of service (DoS) vulnerability. The OpenSSL public API function X509_issuer_and_serial_ha sh() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certific ate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This vulnerability may subsequently result in a NULL pointer deref and a crash lea ding to a potential denial of service attack.

Solution:

VendorFix Update to version 1.0.2y, 1.1.1j or later. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2y / 1.1.1j Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20210216.txt

Unique Alert ID: 539166 Found on: 2023-10-06 Severity: Medium

PHP Denial of Service Vulnerability - 01 - Jul16 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-8878
Cvss Base: 5.9
Cvss Score: 5.9
Cvss Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to script 'main/php_open_temporary_file.c' does n ot ensure thread safety. Successfully exploiting this issue allow remote attackers to cause a denial of service (race condit ion and heap memory corruption) by leveraging an application that performs many temporary-file accesses.

Solution:

VendorFix Update to PHP version 5.5.28, or 5.6.12, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.28

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 919565 Found on: 2023-10-06 Severity: Medium

OpenSSL: Null pointer deref in X509_issuer_and_serial_hash() (CVE-2021-23841) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-23841
Cvss Base: 5.9
Cvss Score: 5.9
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

OpenSSL is prone to a denial of service (DoS) vulnerability. The OpenSSL public API function X509_issuer_and_serial_ha sh() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certific ate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This vulnerability may subsequently result in a NULL pointer deref and a crash lea ding to a potential denial of service attack.

Solution:

VendorFix Update to version 1.0.2y, 1.1.1j or later. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2y / 1.1.1j Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20210216.txt

Unique Alert ID: 607311 Found on: 2023-10-06 Severity: Medium

OpenSSL Security Bypass Vulnerability - DEC 2017 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-12-18
CVE ID: CVE-2017-3737
Cvss Base: 5.9
Cvss Score: 5.9
Cvss Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

OpenSSL is prone to a security bypass vulnerability. When SSL_read()/SSL_write() is subsequently called by the applicati on for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from th e SSL/TLS record layer. Successfully exploiting this issue will allow attackers to bypass security restrictions and perform unauthorized actions. This may aid in launching further attacks.

Solution:

VendorFix OpenSSL 1.0.2 users should upgrade to 1.0.2n.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2n Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20171207.txt

Unique Alert ID: 607313 Found on: 2023-10-06 Severity: Medium

OpenSSL: 0-byte record padding oracle (CVE-2019-1559) (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-12-18
CVE ID:	CVE-2019-1559		
Cvss Base:	5.9		
Cvss Score:	5.9		
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N		

Description:

OpenSSL is prone to a padding oracle attack. If an application encounters a fatal protocol error and then calls SSL_shutd own() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling a pplication if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MA C. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amou nts to a padding oracle that could be used to decrypt data. In order for this to be exploitable 'non-stitched' ciphersuites m ust be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the applic ation must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do a nyway). AEAD ciphersuites are not impacted.

Solution:

VendorFix Upgrade OpenSSL to version 1.0.2r or later. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2r Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20190226.txt,https://github.com/RUB-NDS/TLS-Padding-Oracles#openssl-cv e-2019-1559

Unique Alert ID: 539302 Found on: 2023-10-06 Severity: Medium

OpenSSL: 0-byte record padding oracle (CVE-2019-1559) (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2019-1559		
Cvss Base:	5.9		
Cvss Score:	5.9		
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N		

Description:

OpenSSL is prone to a padding oracle attack. If an application encounters a fatal protocol error and then calls SSL_shutd own() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling a pplication if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MA C. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amou

nts to a padding oracle that could be used to decrypt data. In order for this to be exploitable 'non-stitched' ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). AEAD ciphersuites are not impacted.

Solution:

VendorFix Upgrade OpenSSL to version 1.0.2r or later. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2r Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20190226.txt,https://github.com/RUB-NDS/TLS-Padding-Oracles#openssl-cve-2019-1559

Unique Alert ID: 1010826 Found on: 2023-10-06 Severity: Medium

OpenSSL: BN_mod_exp may produce incorrect results on MIPS (CVE-2021-4160) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2022-08-27
CVE ID:	CVE-2021-4160	
Cvss Base:	5.9	
Cvss Score:	5.9	
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	

Description:

OpenSSL is prone to a carry propagation vulnerability. There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701.

Solution:

VendorFix Update to version 1.1.1m, 3.0.1 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.1.1m Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20220128.txt

Unique Alert ID: 1010827 Found on: 2023-10-06 Severity: Medium

OpenSSL: BN_mod_exp may produce incorrect results on MIPS (CVE-2021-4160) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2022-08-27
CVE ID:	CVE-2021-4160	
Cvss Base:	5.9	
Cvss Score:	5.9	
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	

Description:

OpenSSL is prone to a carry propagation vulnerability. There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce in

formation about a private key may be performed offline. The amount of resources required for such an attack would be s ignificant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among mu ltiple clients, which is no longer an option since CVE-2016-0701.

Solution:

VendorFix Update to version 1.1.1m, 3.0.1 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.1.1m Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20220128.txt

Unique Alert ID: 919566 Found on: 2023-10-06 Severity: Medium

OpenBSD OpenSSH Information Disclosure Vulnerability (CVE-2020-14145) (tcp/22)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2020-14145	
Cvss Base:	5.9	
Cvss Score:	5.9	
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	

Description:

OpenBSD OpenSSH is prone to an information disclosure vulnerability. The client side in OpenSSH has an Observable Dis crepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target ini tial connection attempts (where no host key for the server has been cached by the client).

Solution:

VendorFix Update to version 8.5 or later.

Result:

Installed version: 6.6.1 Fixed version: 8.5 Installation path / port: 22/tcp

References:

- http://www.openwall.com/lists/oss-security/2020/12/02/1

Unique Alert ID: 539285 Found on: 2023-10-06 Severity: Medium

OpenSSL: Timing vulnerability in DSA signature generation (CVE-2018-0734) (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2018-0734	
Cvss Base:	5.9	
Cvss Score:	5.9	
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	

Description:

OpenSSL is prone to an information disclosure vulnerability. The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the privat e key.

Solution:

VendorFix Upgrade OpenSSL to version 1.1.0j-dev, 1.1.1a-dev, 1.0.2q-dev or manually apply the fixes via Github. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2q-dev Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20181030.txt,https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=

43e6a58d4991a451daf4891ff05a48735df871ac,https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=8abfe72e8c1de1b95f50aa0d9134803b4d00070f,https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=ef11e19d1365eea2b1851e6f540a0bf365d303e7

Unique Alert ID: 607314 Found on: 2023-10-06 Severity: Medium

OpenSSL: Timing vulnerability in DSA signature generation (CVE-2018-0734) (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-12-18
CVE ID:	CVE-2018-0734	
Cvss Base:	5.9	
Cvss Score:	5.9	
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	

Description:

OpenSSL is prone to an information disclosure vulnerability. The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key.

Solution:

VendorFix Upgrade OpenSSL to version 1.1.0j-dev, 1.1.1a-dev, 1.0.2q-dev or manually apply the fixes via Github. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2q-dev Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20181030.txt,https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=43e6a58d4991a451daf4891ff05a48735df871ac,https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=8abfe72e8c1de1b95f50aa0d9134803b4d00070f,https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=ef11e19d1365eea2b1851e6f540a0bf365d303e7

Unique Alert ID: 607312 Found on: 2023-10-06 Severity: Medium

OpenSSL Overflow Vulnerability (20171207, 20180327) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-12-18
CVE ID:	CVE-2017-3738	
Cvss Base:	5.9	
Cvss Score:	5.9	
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	

Description:

OpenSSL is prone to an overflow bug. The overflow bug is in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. Successfully exploiting this issue would allow an attacker to derive information about the private key.

Solution:

VendorFix Update to version 1.0.2n, 1.1.0h or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2n Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20171207.txt,https://www.openssl.org/news/secadv/20180327.txt

Unique Alert ID: 919567 Found on: 2023-10-06 Severity: Medium

OpenBSD OpenSSH <= 7.9 Multiple Vulnerabilities (tcp/22)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2018-20685,CVE-2019-6109,CVE-2019-6110,CVE-2019-6111	
Cvss Base:	5.9	
Cvss Score:	5.9	
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	

Description:

OpenBSD OpenSSH is prone to multiple vulnerabilities. The following flaws exist: - CVE-2018-20685: bypass of intended access restrictions in the scp client - CVE-2019-6109, CVE-2019-6110: manipulation of the output in the scp client by a malicious server - CVE-2019-6111: overwrite of arbitrary files in the scp client by a malicious server

Solution:

VendorFix Update to version 8.0 or later.

Result:

Installed version: 6.6.1 Fixed version: 8.0 Installation path / port: 22/tcp

References:

- https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt,http://www.openwall.com/lists/oss-security/2019/04/18/1

Unique Alert ID: 539297 Found on: 2023-10-06 Severity: Medium

OpenSSL Security Bypass Vulnerability - DEC 2017 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2017-3737	
Cvss Base:	5.9	
Cvss Score:	5.9	
Cvss Vector:	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	

Description:

OpenSSL is prone to a security bypass vulnerability. When SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. Successfully exploiting this issue will allow attackers to bypass security restrictions and perform unauthorized actions. This may aid in launching further attacks.

Solution:

VendorFix OpenSSL 1.0.2 users should upgrade to 1.0.2n.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2n Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20171207.txt

Unique Alert ID: 919564 Found on: 2023-10-06 Severity: Medium

OpenSSL: EDIPARTYNAME NULL Pointer De-reference Vulnerability (CVE-2020-1971) (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2020-1971
Cvss Base: 5.9
Cvss Score: 5.9
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

OpenSSL is prone to a Denial-of-Service (DoS) vulnerability. The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the '-crl_download' option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. An attacker may trigger a crash and cause a DoS.

Solution:

VendorFix OpenSSL 1.1.1 users should upgrade to 1.1.1i. OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2x. Other users should upgrade to OpenSSL 1.1.1i.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2x / 1.1.1i Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20201208.txt

Unique Alert ID: 919563 Found on: 2023-10-06 Severity: Medium

OpenSSL: EDIPARTYNAME NULL Pointer De-reference Vulnerability (CVE-2020-1971) (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2020-1971
Cvss Base: 5.9
Cvss Score: 5.9
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

OpenSSL is prone to a Denial-of-Service (DoS) vulnerability. The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X50

9 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being c ompared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CR Ls based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL bei ng verified. OpenSSL's s_server, s_client and verify tools have support for the '-crl_download' option which implements a utomatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is p ossible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. An atta cker may trigger a crash and cause a DoS.

Solution:

VendorFix OpenSSL 1.1.1 users should upgrade to 1.1.1i. OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2x. Other users should upgrade to OpenSSL 1.1.1i.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2x / 1.1.1i Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20201208.txt

Unique Alert ID: 539301 Found on: 2023-10-06 Severity: Medium

OpenSSL Overflow Vulnerability (20171207, 20180327) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2017-3738	
Cvss Base:	5.9	
Cvss Score:	5.9	
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	

Description:

OpenSSL is prone to an overflow bug. The overflow bug is in the AVX2 Montgomery multiplication procedure used in expo nentiation with 1024-bit moduli. Successfully exploiting this issue would allow an attacker to derive information about the private key.

Solution:

VendorFix Update to version 1.0.2n, 1.1.0h or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2n Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20171207.txt,https://www.openssl.org/news/secadv/20180327.txt

Unique Alert ID: 539214 Found on: 2023-10-06 Severity: Medium

PHP < 7.2.29 Multiple Vulnerabilities - Mar20 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2020-7064,CVE-2020-7066	
Cvss Base:	4.3	
Cvss Score:	4.3	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N	

Description:

PHP is prone to multiple vulnerabilities. PHP is prone to multiple vulnerabilities: - Use-of-uninitialized-value in exif (CVE-2 020-7064) - get_headers() silently truncates after a null byte (CVE-2020-7066)

Solution:

VendorFix Update to version 7.2.29 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.29 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.29

Unique Alert ID: 539212 Found on: 2023-10-06 Severity: Medium

PHP < 7.2.29 Multiple Vulnerabilities - Mar20 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2020-7064,CVE-2020-7066	
Cvss Base:	4.3	
Cvss Score:	4.3	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N	

Description:

PHP is prone to multiple vulnerabilities. PHP is prone to multiple vulnerabilities: - Use-of-uninitialized-value in exif (CVE-2020-7064) - get_headers() silently truncates after a null byte (CVE-2020-7066)

Solution:

VendorFix Update to version 7.2.29 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.29 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.29

Unique Alert ID: 919569 Found on: 2023-10-06 Severity: Medium

OpenSSH Information Disclosure Vulnerability (CVE-2016-20012) (tcp/22)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2016-20012	
Cvss Base:	5.3	
Cvss Score:	5.3	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	

Description:

OpenBSD OpenSSH is prone to an information disclosure vulnerability. OpenSSH allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session.

Solution:

WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Result:

Installed version: 6.6.1 Fixed version: None Installation path / port: 22/tcp

References:

- https://github.com/openssh/openssh-portable/pull/270,https://rushter.com/blog/public-ssh-keys/,https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak

Unique Alert ID: 539235 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2019-0220
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Description:

When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch a nd RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will impli citly collapse them.

Solution:

VendorFix Update to version 2.4.39 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.39 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539272 Found on: 2023-10-06 Severity: Medium

OpenSSH < 7.8 User Enumeration Vulnerability - Linux (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-15473
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Description:

OpenSSH is prone to a user enumeration vulnerability. The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and a uth2-pubkey.c Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

Solution:

VendorFix Update to version 7.8 or later.

Result:

Installed version: 6.6.1 Fixed version: 7.8 Installation path / port: 22/tcp

References:

- https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d1e0

Unique Alert ID: 539273 Found on: 2023-10-06 Severity: Medium

OpenSSH 'sftp-server' Security Bypass Vulnerability (Linux) (tcp/22)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2017-15906		
Cvss Base:	5.3		
Cvss Score:	5.3		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N		

Description:

openssh is prone to a security bypass vulnerability. The flaw exists in the 'process_open' function in sftp-server.c script w hich does not properly prevent write operations in readonly mode. Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.

Solution:

VendorFix Upgrade to OpenSSH version 7.6 or later.

Result:

Installed version: 6.6.1 Fixed version: 7.6 Installation path / port: 22/tcp

References:

- https://www.openssh.com/txt/release-7.6,https://github.com/openbsd/src/commit/a6981567e8e

Unique Alert ID: 919568 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 2.4.6 - 2.4.46 Tunneling Misconfiguration Vulnerability - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2019-17567		
Cvss Base:	5.3		
Cvss Score:	5.3		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N		

Description:

Apache HTTP Server is prone to a tunneling misconfiguration vulnerability. mod_proxy_wstunnel configured on an URL th at is not necessarily upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subs equent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

Solution:

VendorFix Update to version 2.4.48 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.48 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539237 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2019-0220

Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Description:

When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch a nd RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will impli citly collapse them.

Solution:

VendorFix Update to version 2.4.39 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.39 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539274 Found on: 2023-10-06 Severity: Medium

OpenSSH 'auth2-gss.c' User Enumeration Vulnerability - Linux (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-15919
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Description:

OpenSSH is prone to a user enumeration vulnerability. The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) c omponent is used on an affected system. Successfully exploitation will allow a remote attacker to harvest valid user acco unts, which may aid in brute-force attacks.

Solution:

WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Result:

Installed version: 6.6.1 Fixed version: None Installation path / port: 22/tcp

References:

- https://bugzilla.novell.com/show_bug.cgi?id=1106163,https://seclists.org/oss-sec/2018/q3/180

Unique Alert ID: 607308 Found on: 2023-10-06 Severity: Medium

OpenSSL Multiple Vulnerabilities - Nov 2017 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-12-18
CVE ID:	CVE-2017-3735,CVE-2017-3736		
Cvss Base:	6.5		
Cvss Score:	6.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N		

Description:

OpenSSL is prone to multiple vulnerabilities. Multiple flaws exist due to: - A carry propagating bug in the x86_64 Montgomery squaring procedure. - Malformed X.509 IPAddressFamily which could cause OOB read. Successful exploitation will allow a remote attacker to recover keys (private or secret keys) or to cause a buffer overread which lead to erroneous display of the certificate in text format.

Solution:

VendorFix Upgrade to OpenSSL version 1.1.0g or 1.0.2m or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2m Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20171102.txt

Unique Alert ID: 919573 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 2.4.6 - 2.4.46 Tunneling Misconfiguration Vulnerability - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2019-17567		
Cvss Base:	5.3		
Cvss Score:	5.3		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N		

Description:

Apache HTTP Server is prone to a tunneling misconfiguration vulnerability. mod_proxy_wstunnel configured on an URL that is not necessarily upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

Solution:

VendorFix Update to version 2.4.48 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.48 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539264 Found on: 2023-10-06 Severity: Medium

PHP < 7.2.28 Multiple Vulnerabilities - Feb20 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2020-7062,CVE-2020-7063		
Cvss Base:	5.3		
Cvss Score:	5.3		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N		

Description:

PHP is prone to multiple vulnerabilities. PHP is prone to multiple vulnerabilities: - Null Pointer Dereference in PHP Session Upload Progress (CVE-2020-7062) - Files added to tar with Phar::buildFromIterator have all-access permissions (CVE-2020-7063)

Solution:

VendorFix Update to version 7.2.28 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.28 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.28

Unique Alert ID: 539263 Found on: 2023-10-06 Severity: Medium

PHP < 7.2.28 Multiple Vulnerabilities - Feb20 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2020-7062,CVE-2020-7063		
Cvss Base:	5.3		
Cvss Score:	5.3		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N		

Description:

PHP is prone to multiple vulnerabilities. PHP is prone to multiple vulnerabilities: - Null Pointer Dereference in PHP Session Upload Progress (CVE-2020-7062) - Files added to tar with Phar::buildFromIterator have all-access permissions (CVE-2020-7063)

Solution:

VendorFix Update to version 7.2.28 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.28 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.28

Unique Alert ID: 919571 Found on: 2023-10-06 Severity: Medium

OpenSSL Information Disclosure Vulnerability (20191206) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2019-1551
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Description:

OpenSSL is prone to an information disclosure vulnerability. There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME.

Solution:

VendorFix Update to version 1.0.2u, 1.1.1e or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2u Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20191206.txt

Unique Alert ID: 539261 Found on: 2023-10-06 Severity: Medium

PHP < 7.2.31, 7.3 < 7.3.18, 7.4 < 7.4.6 Multiple DoS Vulnerabilities - May20 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2019-11048
Cvss Base: 5.3
Cvss Score: 5.3

Description:

PHP is prone to two Denial-of-Service vulnerabilities. The following flaws exist: - Long filenames cause OOM and temp files to not be cleaned - Long variables in multipart/form-data cause OOM and temp files are not cleaned leading to a Denial-of-Service condition (CVE-2019-11048).

Solution:

VendorFix Update to version 7.2.31, 7.3.18, 7.4.6 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.31 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.31,https://www.php.net/ChangeLog-7.php#7.3.18,https://www.php.net/ChangeLog-7.php#7.4.6,https://bugs.php.net/bug.php?id=78875,https://bugs.php.net/bug.php?id=78876

Unique Alert ID: 539259 Found on: 2023-10-06 Severity: Medium

PHP < 7.2.31, 7.3 < 7.3.18, 7.4 < 7.4.6 Multiple DoS Vulnerabilities - May20 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2019-11048		
Cvss Base:	5.3		
Cvss Score:	5.3		

Description:

PHP is prone to two Denial-of-Service vulnerabilities. The following flaws exist: - Long filenames cause OOM and temp file s to not be cleaned - Long variables in multipart/form-data cause OOM and temp files are not cleaned leading to a Denial -of-Service condition (CVE-2019-11048).

Solution:

VendorFix Update to version 7.2.31, 7.3.18, 7.4.6 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.31 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.31,https://www.php.net/ChangeLog-7.php#7.3.18,https://www.php.net/ChangeLog-7.php#7.4.6,https://bugs.php.net/bug.php?id=78875,https://bugs.php.net/bug.php?id=78876

Unique Alert ID: 919574 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.26, 7.4.x < 7.4.14, 8.0.x < 8.0.1 Filter Vulnerability (Jan 2021) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2020-7071		
Cvss Base:	5.3		
Cvss Score:	5.3		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N		

Description:

PHP is prone to a vulnerability where FILTER_VALIDATE_URL accepts URLs with invalid userinfo.

Solution:

VendorFix Update to version 7.3.26, 7.4.14, 8.0.1 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.26 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.26,https://www.php.net/ChangeLog-7.php#7.4.14,https://www.php.net/ChangeLog-8.php#8.0.1

Unique Alert ID: 919575 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.26, 7.4.x < 7.4.14, 8.0.x < 8.0.1 Filter Vulnerability (Jan 2021) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2020-7071
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description:

PHP is prone to a vulnerability where FILTER_VALIDATE_URL accepts URLs with invalid userinfo.

Solution:

VendorFix Update to version 7.3.26, 7.4.14, 8.0.1 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.26 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.26,https://www.php.net/ChangeLog-7.php#7.4.14,https://www.php.net/ChangeLog-8.php#8.0.1

Unique Alert ID: 919576 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.29 Multiple Vulnerabilities (Jul 2021) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-21704,CVE-2021-21705
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - CVE-2021-21705: SSRF bypass in FILTER_VALIDATE_URL. - CVE-2021-21704: Stack buffer overflow in firebird_info_cb. - CVE-2021-21704: SIGSEGV in firebird_handle_doer. - CVE-2021-21704: SIGSEGV in firebird_stmt_execute. - CVE-2021-21704: Crash while parsing blob data in firebird_fetch_blob.

Solution:

VendorFix Update to version 7.3.29 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.29 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.29,http://bugs.php.net/81122,http://bugs.php.net/76448,http://bugs.php.net/76449,http://bugs.php.net/76450,http://bugs.php.net/76452

Unique Alert ID: 919577 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.29 Multiple Vulnerabilities (Jul 2021) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17

CVE ID: CVE-2021-21704,CVE-2021-21705
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - CVE-2021-21705: SSRF bypass in FILTER_VALIDATE_URL. - CVE-2021-21704: Stack buffer overflow in firebird_info_cb. - CVE-2021-21704: SIGSEGV in firebird_handle_doer. - CVE-2021-21704: SIGSEGV in firebird_stmt_execute. - CVE-2021-21704: Crash while parsing blob data in firebird_fetch_blob.

Solution:

VendorFix Update to version 7.3.29 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.29 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.29,http://bugs.php.net/81122,http://bugs.php.net/76448,http://bugs.php.net/76449,http://bugs.php.net/76450,http://bugs.php.net/76452

Unique Alert ID: 539265 Found on: 2023-10-06 Severity: Medium

OpenSSL 'OOB read' Security Bypass Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2017-3735
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description:

OpenSSL is prone to an 'OOB read' security bypass vulnerability. The flaw exists as OpenSSL could do a one-byte buffer overread if an X.509 certificate has a malformed IPAddressFamily extension. Successfully exploiting this issue will allow attackers to bypass security restrictions and perform unauthorized actions, this may aid in launching further attacks.

Solution:

VendorFix Upgrade to OpenSSL version 1.1.0g-dev or 1.0.2m-dev or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2m-dev Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20170828.txt,https://www.openssl.org/news/vulnerabilities.html#y2017

Unique Alert ID: 607307 Found on: 2023-10-06 Severity: Medium

OpenSSL 'OOB read' Security Bypass Vulnerability (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-12-18
CVE ID: CVE-2017-3735
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description:

OpenSSL is prone to an 'OOB read' security bypass vulnerability. The flaw exists as OpenSSL could do a one-byte buffer overread if an X.509 certificate has a malformed IPAddressFamily extension. Successfully exploiting this issue will allow a ttackers to bypass security restrictions and perform unauthorized actions, this may aid in launching further attacks.

Solution:

VendorFix Upgrade to OpenSSL version 1.1.0g-dev or 1.0.2m-dev or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2m-dev Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20170828.txt,https://www.openssl.org/news/vulnerabilities.html#y2017

Unique Alert ID: 919578 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.33, 7.4.x < 7.4.26, 8.0.x < 8.0.13 Security Update (Nov 2021) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-21707
Cvss Base: 5.3
Cvss Score: 5.3

Description:

PHP released new versions which include a security fix. Fixed bug #79971 (special character is breaking the path in xml f unction).

Solution:

VendorFix Update to version 7.3.33, 7.4.26, 8.0.13 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.33 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.33,https://www.php.net/ChangeLog-7.php#7.4.26,https://www.php.net/ChangeLog-8.php#8.0.13,http://bugs.php.net/79971

Unique Alert ID: 919579 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.33, 7.4.x < 7.4.26, 8.0.x < 8.0.13 Security Update (Nov 2021) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-21707
Cvss Base: 5.3
Cvss Score: 5.3

Description:

PHP released new versions which include a security fix. Fixed bug #79971 (special character is breaking the path in xml function).

Solution:

VendorFix Update to version 7.3.33, 7.4.26, 8.0.13 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.33 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.33,https://www.php.net/ChangeLog-7.php#7.4.26,https://www.php.net/ChangeLog-8.php#8.0.13,http://bugs.php.net/79971

Unique Alert ID: 919572 Found on: 2023-10-06 Severity: Medium

OpenSSL Information Disclosure Vulnerability (20191206) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2019-1551
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Description:

OpenSSL is prone to an information disclosure vulnerability. There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME.

Solution:

VendorFix Update to version 1.0.2u, 1.1.1e or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2u Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20191206.txt

Unique Alert ID: 539270 Found on: 2023-10-06 Severity: Medium

OpenSSL Multiple Vulnerabilities - Nov 2017 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2017-3735,CVE-2017-3736

Cvss Base: 6.5
Cvss Score: 6.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

Description:

OpenSSL is prone to multiple vulnerabilities. Multiple flaws exist due to: - A carry propagating bug in the x86_64 Montgo mery squaring procedure. - Malformed X.509 IPAddressFamily which could cause OOB read. Successful exploitation will a llow a remote attacker to recover keys (private or secret keys) or to cause a buffer overread which lead to erroneous dis play of the certificate in text format.

Solution:

VendorFix Upgrade to OpenSSL version 1.1.0g or 1.0.2m or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2m Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20171102.txt

Unique Alert ID: 539283 Found on: 2023-10-06 Severity: Medium

OpenSSH Denial of Service Vulnerability - Jan16 (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-1907
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Description:

openssh is prone to a denial of service (DoS) vulnerability. The flaw exists due to an error in 'ssh_packet_read_poll2' fun ction within 'packet.c' script. Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read and application crash).

Solution:

VendorFix Upgrade to OpenSSH version 7.1p2 or later.

Result:

Installed version: 6.6.1 Fixed version: 7.1p2 Installation path / port: 22/tcp

References:

- http://www.openssh.com/txt/release-7.1p2,https://anongit.mindrot.org/openssh.git/commit/?id=2fecfd486bdba9f51b3a789277bb0733ca36e1c0

Unique Alert ID: 919570 Found on: 2023-10-06 Severity: Medium

Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) (tcp/22)

Open Status: Re-OPEN **First Found:** 2022-05-17
Cvss Base: 5.3
Cvss Score: 5.3

Description:

The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s). - 1024-bit MODP group / prime KEX algorithms: Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key e xchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connecti on. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection -is dependent only on this prime. A nation-state can break a 1024-bit prime. An attacker can quickly break individual con nections.

Solution:

Mitigation Disable the reported weak KEX algorithm(s) - 1024-bit MODP group / prime KEX algorithms: Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Result:

The remote SSH server supports the following weak KEX algorithm(s): KEX algorithm | Reason ---------- ---------- diffie-hellman-group-exchange-sha1 | Using SHA-1 diffie-hellman-group1-sha1 | Using Oakley Group 2 (a 1024-bit MODP group) and SHA-1

References:

- https://weakdh.org/sysadmin.html,https://www.rfc-editor.org/rfc/rfc9142.html,https://www.rfc-editor.org/rfc/rfc914 2.html#name-summary-guidance-for-implem,https://datatracker.ietf.org/doc/html/rfc6194

Unique Alert ID: 539293 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 2.4.1 < 2.4.24 IP Spoofing Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2020-11985
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description:

Apache HTTP Server is prone to an IP address spoofing vulnerability when proxying using mod_remoteip and mod_rewrit e.

Solution:

VendorFix Update to version 2.4.24 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.24 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539304 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 2.4.1 < 2.4.24 IP Spoofing Vulnerability (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2020-11985
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description:

Apache HTTP Server is prone to an IP address spoofing vulnerability when proxying using mod_remoteip and mod_rewrite.

Solution:

VendorFix Update to version 2.4.24 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.24 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539217 Found on: 2023-10-06 Severity: Medium

PHP 'php_parserr' Heap Based Buffer Overflow Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-4049
Cvss Base: 5.1
Cvss Score: 5.1

Description:

PHP is prone to a heap-based buffer overflow vulnerability. The flaw is due to buffer overflow error in the 'php_parserr' function in ext/standard/dns.c script. Successfully exploiting this issue allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code on the affected system.

Solution:

VendorFix Update to PHP version 5.6.0 or 5.5.14 or 5.4.30 or 5.3.29 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.30

References:

- http://php.net/ChangeLog-5.php,http://www.openwall.com/lists/oss-security/2014/06/13/4

Unique Alert ID: 539219 Found on: 2023-10-06 Severity: Medium

PHP 'php_parserr' Heap Based Buffer Overflow Vulnerability (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-4049
Cvss Base: 5.1
Cvss Score: 5.1

Description:

PHP is prone to a heap-based buffer overflow vulnerability. The flaw is due to buffer overflow error in the 'php_parserr' function in ext/standard/dns.c script. Successfully exploiting this issue allows remote attackers to cause a denial of servic

e (crash) and possibly execute arbitrary code on the affected system.

Solution:

VendorFix Update to PHP version 5.6.0 or 5.5.14 or 5.4.30 or 5.3.29 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.30

References:

- http://php.net/ChangeLog-5.php,http://www.openwall.com/lists/oss-security/2014/06/13/4

Unique Alert ID: 539269 Found on: 2023-10-06 Severity: Medium

SSL/TLS: Certificate Expired (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 5.0
Cvss Score: 5.0

Description:

The remote server's SSL/TLS certificate has already expired. This script checks expiry dates of certificates associated wit h SSL/TLS-enabled services on the target and reports whether any have already expired.

Solution:

Mitigation Replace the SSL/TLS certificate by a new one.

Result:

The certificate of the remote service expired on 2019-03-13 13:40:08. Certificate details: fingerprint (SHA-1) | 81C5AB98A9E8BECAEEB849E97EF47D7A14DCF936 fingerprint (SHA-256) | 635269291BDF6067EEDB2D40DB10B25C354D9FEA326F43779AE51D6C3FEB0FAB issued by | CN=Let's Encrypt Authority X3,O=Let's Encrypt,C=US public key algorithm | RSA public key size (bits) | 2048 serial | 0342FA98D61F9F34FD44E05EE95726E89BB3 signature algorithm | sha256WithRSAEncryption subject | CN=*.testapptrana.com subject alternative names (SAN) | *.testapptrana.com valid from | 2018-12-13 13:40:08 UTC valid until | 2019-03-13 13:40:08 UTC

Unique Alert ID: 539266 Found on: 2023-10-06 Severity: Medium

Missing 'HttpOnly' Cookie Attribute (HTTP) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 5.0
Cvss Score: 5.0

Description:

The remote HTTP web server / application is missing to set the 'HttpOnly' cookie attribute for one or more sent HTTP coo kie. The flaw exists if a session cookie is not using the 'HttpOnly' cookie attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Solution:

Mitigation Set the 'HttpOnly' attribute for any session cookie.

Result:

The cookies: Set-Cookie: PHPSESSID=***replaced***; path=/ Set-Cookie: PHPSESSID=***replaced***; path=/ Set-Cookie: security=low are missing the "HttpOnly" attribute.

References:

- https://www.rfc-editor.org/rfc/rfc6265#section-5.2.6,https://owasp.org/www-community/HttpOnly,https://wiki.owasp.org/index.php/Testing_for_cookies_attributes

Unique Alert ID: 919585 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server DoS Vulnerability (Sep 2014) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2014-3581
Cvss Base: 5.0
Cvss Score: 5.0

Description:

Apache HTTP Server is prone to a denial of service (DoS) vulnerability. A NULL pointer deference was found in mod_cach e. A malicious HTTP server could cause a crash in a caching forward proxy configuration. This crash would only be a deni al of service if using a threaded MPM.

Solution:

VendorFix Update to version 2.4.12 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.12 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 919584 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server DoS Vulnerability (Sep 2014) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2014-3581
Cvss Base: 5.0
Cvss Score: 5.0

Description:

Apache HTTP Server is prone to a denial of service (DoS) vulnerability. A NULL pointer deference was found in mod_cach e. A malicious HTTP server could cause a crash in a caching forward proxy configuration. This crash would only be a deni al of service if using a threaded MPM.

Solution:

VendorFix Update to version 2.4.12 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.12 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539252 Found on: 2023-10-06 Severity: Medium

PHP 'donate' function Denial of Service Vulnerability - Nov14 (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-3710
Cvss Base: 5.0
Cvss Score: 5.0

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to an out-of-bounds read error in the 'donote' func tion in readelf.c script. Successful exploitation will allow a local attacker to conduct a denial of service attack.

Solution:

VendorFix Update to PHP version 5.4.35 or 5.5.19 or 5.6.3 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.35/5.5.19/5.6.3

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=68283

Unique Alert ID: 539251 Found on: 2023-10-06 Severity: Medium

PHP 'donate' function Denial of Service Vulnerability - Nov14 (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-3710
Cvss Base: 5.0
Cvss Score: 5.0

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to an out-of-bounds read error in the 'donote' func tion in readelf.c script. Successful exploitation will allow a local attacker to conduct a denial of service attack.

Solution:

VendorFix Update to PHP version 5.4.35 or 5.5.19 or 5.6.3 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.35/5.5.19/5.6.3

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=68283

Unique Alert ID: 539244 Found on: 2023-10-06 Severity: Medium

PHP 'open_basedir' Security Bypass Vulnerability (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2012-1171
Cvss Base: 5.0
Cvss Score: 5.0

Description:

PHP is prone to a security bypass vulnerability. The flaw is in libxml RSHUTDOWN function which allows to bypass open_b asedir protection mechanism through stream_close method call. Successful exploitation will allow remote attackers to rea d arbitrary files.

Solution:

WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Result:

Installed version: 5.4.16 Fixed version: N/A

References:

- https://bugzilla.redhat.com/show_bug.cgi?id=802591

Unique Alert ID: 539243 Found on: 2023-10-06 Severity: Medium

PHP 'open_basedir' Security Bypass Vulnerability (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2012-1171
Cvss Base: 5.0
Cvss Score: 5.0

Description:

PHP is prone to a security bypass vulnerability. The flaw is in libxml RSHUTDOWN function which allows to bypass open_basedir protection mechanism through stream_close method call. Successful exploitation will allow remote attackers to read arbitrary files.

Solution:

WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Result:

Installed version: 5.4.16 Fixed version: N/A

References:

- https://bugzilla.redhat.com/show_bug.cgi?id=802591

Unique Alert ID: 1533218 Found on: 2023-10-06 Severity: Medium

OpenSSL DoS Vulnerability (20230731) - Linux (tcp/443)

Open Status: NEW **First Found:** 2023-10-06
CVE ID: CVE-2023-3817
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Description:

OpenSSL is prone to a denial of service (DoS) vulnerability. Checking excessively long DH keys or parameters may be very slow. Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service.

Solution:

NoneAvailable No known solution is available as of 01st August, 2023. Information regarding this issue will be updated once solution details are available. Vendor info: Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available. The fix is also available in commit 6a1eb62c2 (for 3.1), commit 9002fd073 (for 3.0) and commit 91ddeba0f (for 1.1.1) in the OpenSSL git repository. It is available to premium support customer in commit 869ad69a (for 1.0.2).

Result:

Installed version: 1.0.2k Fixed version: None Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20230731.txt

Unique Alert ID: 1533219 Found on: 2023-10-06 Severity: Medium

OpenBSD OpenSSH < 9.3 Unspecified Vulnerability (tcp/22)

Open Status: NEW **First Found:** 2023-10-06
Cvss Base: 5.0
Cvss Score: 5.0

Description:

OpenBSD OpenSSH is prone to an unspecified vulnerability. ssh(1): Portable OpenSSH provides an implementation of the getrrsetbyname(3) function if the standard library does not provide it, for use by the VerifyHostKeyDNS feature. A specifi cally crafted DNS response could cause this function to perform an out-of-bounds read of adjacent stack data, but this co ndition does not appear to be exploitable beyond denial-of-service to the ssh(1) client. The getrrsetbyname(3) replaceme nt is only included if the system's standard library lacks this function and portable OpenSSH was not compiled with the ld ns library (--with-ldns). getrrsetbyname(3) is only invoked if using VerifyHostKeyDNS to fetch SSHFP records.This proble m was found by the Coverity static analyzer.

Solution:

VendorFix Update to version 9.3 or later.

Result:

Installed version: 6.6.1 Fixed version: 9.3 Installation path / port: 22/tcp

References:

- https://www.openssh.com/releasenotes.html#9.3,https://www.openwall.com/lists/oss-security/2023/03/15/8

Unique Alert ID: 1533220 Found on: 2023-10-06 Severity: Medium

OpenBSD OpenSSH < 9.2 Unspecified Vulnerability (tcp/22)

Open Status: NEW **First Found:** 2023-10-06
Cvss Base: 5.0
Cvss Score: 5.0

Description:

OpenBSD OpenSSH is prone to an unspecified vulnerability. If the CanonicalizeHostname and CanonicalizePermittedCNA MEs options were enabled, and the system/libc resolver did not check that names in DNS responses were valid, then use of these options could allow an attacker with control of DNS to include invalid characters (possibly including wildcards) in names added to known_hosts files when they were updated. These names would still have to match the CanonicalizePer mittedCNAMEs allow-list, so practical exploitation appears unlikely.

Solution:

VendorFix Update to version 9.2 or later.

Result:

Installed version: 6.6.1 Fixed version: 9.2 Installation path / port: 22/tcp

References:

- https://www.openssh.com/releasenotes.html#9.2,https://www.openwall.com/lists/oss-security/2023/02/02/3

Unique Alert ID: 919583 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.28, 7.4.x < 7.4.18 IMAP Header Injection Vulnerability (Apr 2021) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
Cvss Base: 5.0
Cvss Score: 5.0

Description:

PHP is prone to an IMAP header injection vulnerability.

Solution:

VendorFix Update to version 7.3.28, 7.4.18 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.28 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.28,https://www.php.net/ChangeLog-7.php#7.4.18

Unique Alert ID: 919581 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.28, 7.4.x < 7.4.18 IMAP Header Injection Vulnerability (Apr 2021) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
Cvss Base: 5.0
Cvss Score: 5.0

Description:

PHP is prone to an IMAP header injection vulnerability.

Solution:

VendorFix Update to version 7.3.28, 7.4.18 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.28 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.28,https://www.php.net/ChangeLog-7.php#7.4.18

Unique Alert ID: 919582 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.30, 7.4.x < 7.4.23, 8.0.x < 8.0.10 Security Update (Aug 2021) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
Cvss Base: 5.0
Cvss Score: 5.0

Description:

PHP released new versions which include security fixes.

Solution:

VendorFix Update to version 7.3.30, 7.4.23, 8.0.10 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.30 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.30,https://www.php.net/ChangeLog-7.php#7.4.23,https://www.php.net/ChangeLog-8.php#8.0.10

Unique Alert ID: 919580 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.30, 7.4.x < 7.4.23, 8.0.x < 8.0.10 Security Update (Aug 2021) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
Cvss Base: 5.0
Cvss Score: 5.0

Description:

PHP released new versions which include security fixes.

Solution:

VendorFix Update to version 7.3.30, 7.4.23, 8.0.10 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.30 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.30,https://www.php.net/ChangeLog-7.php#7.4.23,https://www.php.net/ChangeLog-8.php#8.0.10

Unique Alert ID: 1533221 Found on: 2023-10-06 Severity: Medium

OpenSSL DoS Vulnerability (20230731) - Linux (tcp/80)

Open Status: NEW **First Found:** 2023-10-06
CVE ID: CVE-2023-3817
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Description:

OpenSSL is prone to a denial of service (DoS) vulnerability. Checking excessively long DH keys or parameters may be very slow. Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service.

Solution:

NoneAvailable No known solution is available as of 01st August, 2023. Information regarding this issue will be updated once solution details are available. Vendor info: Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available. The fix is also available in commit 6a1eb62c2 (for 3.1), commit 9002fd073 (for 3.0) and commit 91ddeba0f (for 1.1.1) in the OpenSSL git repository. It is available to premium support customer in commit 869ad69a (for 1.0.2).

Result:

Installed version: 1.0.2k Fixed version: None Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20230731.txt

Unique Alert ID: 1533224 Found on: 2023-10-06 Severity: Medium

PHP < 8.0.29, 8.1.x < 8.1.20, 8.2.x < 8.2.7 Security Update - Linux (tcp/80)

Open Status: NEW **First Found:** 2023-10-06
CVE ID: CVE-2023-3247
Cvss Base: 4.3
Cvss Score: 4.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

Description:

PHP is prone to a missing error check and insufficient random bytes in HTTP Digest authentication for SOAP vulnerability.

Solution:

VendorFix Update to version 8.0.29, 8.1.10, 8.2.7 or later.

Result:

Installed version: 5.4.16 Fixed version: 8.0.29 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-8.php#8.0.29,https://www.php.net/ChangeLog-8.php#8.1.20,https://www.php.net/ChangeLog-8.php#8.2.7,https://github.com/php/php-src/security/advisories/GHSA-76gg-c692-v2mw

Unique Alert ID: 1533225 Found on: 2023-10-06 Severity: Medium

PHP < 8.0.29, 8.1.x < 8.1.20, 8.2.x < 8.2.7 Security Update - Linux (tcp/443)

Open Status: NEW **First Found:** 2023-10-06
CVE ID: CVE-2023-3247
Cvss Base: 4.3
Cvss Score: 4.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

Description:

PHP is prone to a missing error check and insufficient random bytes in HTTP Digest authentication for SOAP vulnerability.

Solution:

VendorFix Update to version 8.0.29, 8.1.10, 8.2.7 or later.

Result:

Installed version: 5.4.16 Fixed version: 8.0.29 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-8.php#8.0.29,https://www.php.net/ChangeLog-8.php#8.1.20,https://www.php.net/ChangeLog-8.php#8.2.7,https://github.com/php/php-src/security/advisories/GHSA-76gg-c692-v2mw

Unique Alert ID: 539258 Found on: 2023-10-06 Severity: Medium

PHP CDF File Parsing Denial of Service Vulnerabilities - 01 - Jun14 (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-0237,CVE-2014-0238
Cvss Base: 5.0
Cvss Score: 5.0

Description:

PHP is prone to multiple denial of service vulnerabilities. The flaw is due to - An error due to an infinite loop within the 'unpack_summary_info' function in src/cdf.c script. - An error within the 'cdf_read_property_info' function in src/cdf.c script. Successful exploitation will allow remote attackers to conduct denial of service attacks.

Solution:

VendorFix Update to PHP version 5.4.29 or 5.5.13 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.29/5.5.13

References:

- http://www.php.net/ChangeLog-5.php,http://secunia.com/advisories/58804,https://www.hkcert.org/my_url/en/alert/14060401

Unique Alert ID: 539257 Found on: 2023-10-06 Severity: Medium

PHP CDF File Parsing Denial of Service Vulnerabilities - 01 - Jun14 (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-0237,CVE-2014-0238		
Cvss Base:	5.0		
Cvss Score:	5.0		

Description:

PHP is prone to multiple denial of service vulnerabilities. The flaw is due to - An error due to an infinite loop within the 'unpack_summary_info' function in src/cdf.c script. - An error within the 'cdf_read_property_info' function in src/cdf.c script. Successful exploitation will allow remote attackers to conduct denial of service attacks.

Solution:

VendorFix Update to PHP version 5.4.29 or 5.5.13 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.29/5.5.13

References:

- http://www.php.net/ChangeLog-5.php,http://secunia.com/advisories/58804,https://www.hkcert.org/my_url/en/alert/14060401

Unique Alert ID: 1533226 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server < 2.4.55 Multiple Vulnerabilities (Linux) (tcp/443)

Open Status:	NEW	**First Found:**	2023-10-06
CVE ID:	CVE-2006-20001,CVE-2022-36760,CVE-2022-37436		
Cvss Base:	5.3		
Cvss Score:	5.3		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N		

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2006-20001: mod_dav out of bounds read, or write of zero byte - CVE-2022-36760: Possible request smuggling in mod_proxy_ajp - CVE-2022-37436: mod_proxy allows a backend to trigger HTTP response splitting

Solution:

VendorFix Update to version 2.4.55 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.55 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 1533227 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server < 2.4.55 Multiple Vulnerabilities (Linux) (tcp/80)

Open Status:	NEW	**First Found:**	2023-10-06
CVE ID:	CVE-2006-20001,CVE-2022-36760,CVE-2022-37436		
Cvss Base:	5.3		
Cvss Score:	5.3		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N		

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2006-20001: mod_dav out of bounds read, or write of zero byte - CVE-2022-36760: Possible request smuggling in mod_proxy_ajp - CVE-2022-37436: mod_proxy allows a backend to trigger HTTP response splitting

Solution:

VendorFix Update to version 2.4.55 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.55 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539230 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 'mod_lua' Denial of Service Vulnerability -01 May15 (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18

CVE ID: CVE-2015-0228
Cvss Base: 5.0
Cvss Score: 5.0

Description:

Apache HTTP Server is prone to a denial of service vulnerability. Flaw is due to vulnerability in lua_websocket_read functi on in lua_request.c in the mod_lua module. Successful exploitation will allow a remote attacker to cause a denial of servi ce via some crafted dimension.

Solution:

VendorFix Update to version 2.4.13 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.13 Installation path / port: 443/tcp

References:

- https://bugs.mageia.org/show_bug.cgi?id=15428,http://svn.apache.org/repos/asf/httpd/httpd/branches/2.4.x/CHAN GES

Unique Alert ID: 539228 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server Multiple Vulnerabilities August15 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-3185,CVE-2015-3183
Cvss Base: 5.0
Cvss Score: 5.0

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Multiple flaws are due to: - an error in 'ap_some_auth_required' function in 'server/request.c' script which does not consider that a Require directive may be associated with an authorizat ion setting rather than an authentication setting. - an error in chunked transfer coding implementation. Successful exploit ation will allow remote attackers to bypass intended access restrictions in opportunistic circumstances and to cause cache poisoning or credential hijacking if an intermediary proxy is in use.

Solution:

VendorFix Update to version 2.4.14 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.14 Installation path / port: 443/tcp

References:

- http://www.apache.org/dist/httpd/CHANGES_2.4,http://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539229 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server Multiple Vulnerabilities August15 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-3185,CVE-2015-3183		
Cvss Base:	5.0		
Cvss Score:	5.0		

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Multiple flaws are due to: - an error in 'ap_some_auth_required' function in 'server/request.c' script which does not consider that a Require directive may be associated with an authorizat ion setting rather than an authentication setting. - an error in chunked transfer coding implementation. Successful exploit ation will allow remote attackers to bypass intended access restrictions in opportunistic circumstances and to cause cache poisoning or credential hijacking if an intermediary proxy is in use.

Solution:

VendorFix Update to version 2.4.14 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.14 Installation path / port: 80/tcp

References:

- http://www.apache.org/dist/httpd/CHANGES_2.4,http://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 656889 Found on: 2023-10-06 Severity: Medium

SSL/TLS: Certificate In Chain Expired (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2021-03-18
Cvss Base:	5.0		
Cvss Score:	5.0		

Description:

The remote service is using a SSL/TLS certificate chain where one or multiple CA certificates have expired. Checks if the CA certificates in the SSL/TLS certificate chain have expired.

Solution:

Mitigation Sign your server certificate with a valid CA certificate.

Result:

The following certificates which are part of the certificate chain have expired: Subject: CN=Let's Encrypt Authority X3,O=Let's Encrypt,C=US Expired on: 2021-03-17 16:40:46

Unique Alert ID: 539231 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 'mod_lua' Denial of Service Vulnerability -01 May15 (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-0228
Cvss Base: 5.0
Cvss Score: 5.0

Description:

Apache HTTP Server is prone to a denial of service vulnerability. Flaw is due to vulnerability in lua_websocket_read functi on in lua_request.c in the mod_lua module. Successful exploitation will allow a remote attacker to cause a denial of servi ce via some crafted dimension.

Solution:

VendorFix Update to version 2.4.13 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.13 Installation path / port: 80/tcp

References:

- https://bugs.mageia.org/show_bug.cgi?id=15428,http://svn.apache.org/repos/asf/httpd/httpd/branches/2.4.x/CHAN GES

Unique Alert ID: 1533230 Found on: 2023-10-06 Severity: Medium

OpenSSL Multiple Vulnerabilities (20230322, 20230328, 20230530) - Linux (tcp/80)

Open Status: NEW **First Found:** 2023-10-06
CVE ID: CVE-2023-0464,CVE-2023-0465,CVE-2023-0466,CVE-2023-2650
Cvss Base: 6.5
Cvss Score: 6.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Description:

OpenSSL is prone to multiple vulnerabilities. The following flaws exist: - CVE-2023-0464: Excessive Resource Usage Verif ying X.509 Policy Constraints - CVE-2023-0465: Invalid certificate policies in leaf certificates are silently ignored - CVE-2 023-0466: Certificate policy check not enabled - CVE-2023-2650: Possible DoS translating ASN.1 object identifiers

Solution:

VendorFix Update to version 1.0.2zh, 1.1.1u, 3.0.9, 3.1.1 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2zh Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20230322.txt,https://www.openssl.org/news/secadv/20230328.txt,https://ww w.openssl.org/news/secadv/20230530.txt

Unique Alert ID: 1533231 Found on: 2023-10-06 Severity: Medium

OpenSSL Multiple Vulnerabilities (20230322, 20230328, 20230530) - Linux (tcp/443)

Open Status:	NEW	**First Found:**	2023-10-06
CVE ID:	CVE-2023-0464,CVE-2023-0465,CVE-2023-0466,CVE-2023-2650		
Cvss Base:	6.5		
Cvss Score:	6.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H		

Description:

OpenSSL is prone to multiple vulnerabilities. The following flaws exist: - CVE-2023-0464: Excessive Resource Usage Verifying X.509 Policy Constraints - CVE-2023-0465: Invalid certificate policies in leaf certificates are silently ignored - CVE-2023-0466: Certificate policy check not enabled - CVE-2023-2650: Possible DoS translating ASN.1 object identifiers

Solution:

VendorFix Update to version 1.0.2zh, 1.1.1u, 3.0.9, 3.1.1 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2zh Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20230322.txt,https://www.openssl.org/news/secadv/20230328.txt,https://www.openssl.org/news/secadv/20230530.txt

Unique Alert ID: 919587 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server Multiple Vulnerabilities (Mar 2014) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2013-6438,CVE-2014-0098		
Cvss Base:	5.0		
Cvss Score:	5.0		

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2013-6438: XML parsing code in mod_dav incorrectly calculates the end of the string when removing leading spaces and places a NUL character outside the buffer, causing random crashes. This XML parsing code is only used with DAV provider modules that support DeltaV, of which the only publicly released provider is mod_dav_svn. - CVE-2014-0098: A flaw was found in mod_log_config. A remote attacker could send a specific truncated cookie causing a crash. This crash would only be a denial of service if using a threaded MPM.

Solution:

VendorFix Update to version 2.2.27, 2.4.9 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.9 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_22.html,https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 919586 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server Multiple Vulnerabilities (Mar 2014) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2013-6438,CVE-2014-0098
Cvss Base: 5.0
Cvss Score: 5.0

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2013-6438: XML parsing code in mod_dav incorrectly calculates the end of the string when removing leading spaces and places a NUL character outside the buffer, causing random crashes. This XML parsing code is only used with DAV provider modules that support DeltaV, of which the only publicly released provider is mod_dav_svn. - CVE-2014-0098: A flaw was found in mod_log_config. A remote attacker could send a specific truncated cookie causing a crash. This crash would only be a denial of service if using a threaded MPM.

Solution:

VendorFix Update to version 2.2.27, 2.4.9 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.9 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_22.html,https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539315 Found on: 2023-10-06 Severity: Medium

OpenSSL: Microarchitecture timing vulnerability in ECC scalar multiplication (CVE-2018-5407) (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-5407
Cvss Base: 4.7
Cvss Score: 4.7
Cvss Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

Description:

OpenSSL is prone to an information disclosure vulnerability. OpenSSL ECC scalar multiplication, used in e.g. ECDSA and ECDH, has been shown to be vulnerable to a microarchitecture timing side channel attack. An attacker with sufficient access to mount local timing attacks during ECDSA signature generation could recover the private key.

Solution:

VendorFix Upgrade OpenSSL to version 1.0.2q, 1.1.0i or later. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2q Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20181112.txt,https://www.openssl.org/news/vulnerabilities.html,https://github.com/openssl/openssl/commit/aab7c770353b1dc4ba045938c8fb446dd1c4531e,https://eprint.iacr.org/2018/1060.pdf,https://github.com/bbbrumley/portsmash,https://www.exploit-db.com/exploits/45785/

Unique Alert ID: 539314 Found on: 2023-10-06 Severity: Medium

PHP Security Bypass Vulnerability May18 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-10545
Cvss Base: 4.7
Cvss Score: 4.7
Cvss Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

Description:

PHP is prone to a security bypass vulnerability. The flaw exists as the dumpable FPM child processes allow bypassing opc ache access controls Successful exploitation will allow an attacker to bypass security restrictions and access sensitive con figuration data for other accounts directly in the PHP worker process's memory.

Solution:

VendorFix Update to version 7.2.4 or 7.0.29 or 5.6.35 or 7.1.16 or later. Please see the references for more information.

Result:

Installed version: 5.4.16 Fixed version: 5.6.35 Installation path / port: 443/tcp

References:

- http://www.php.net/ChangeLog-5.php#5.6.35,http://www.php.net/ChangeLog-7.php#7.0.29,http://www.php.net/Ch angeLog-7.php#7.1.16,http://www.php.net/ChangeLog-7.php#7.2.4

Unique Alert ID: 539316 Found on: 2023-10-06 Severity: Medium

PHP Security Bypass Vulnerability May18 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-10545
Cvss Base: 4.7
Cvss Score: 4.7
Cvss Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

Description:

PHP is prone to a security bypass vulnerability. The flaw exists as the dumpable FPM child processes allow bypassing opc ache access controls Successful exploitation will allow an attacker to bypass security restrictions and access sensitive con figuration data for other accounts directly in the PHP worker process's memory.

Solution:

VendorFix Update to version 7.2.4 or 7.0.29 or 5.6.35 or 7.1.16 or later. Please see the references for more information.

Result:

Installed version: 5.4.16 Fixed version: 5.6.35 Installation path / port: 80/tcp

References:

- http://www.php.net/ChangeLog-5.php#5.6.35,http://www.php.net/ChangeLog-7.php#7.0.29,http://www.php.net/Ch angeLog-7.php#7.1.16,http://www.php.net/ChangeLog-7.php#7.2.4

Unique Alert ID: 607315 Found on: 2023-10-06 Severity: Medium

OpenSSL: Microarchitecture timing vulnerability in ECC scalar multiplication (CVE-2018-5407) (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-12-18
CVE ID: CVE-2018-5407
Cvss Base: 4.7
Cvss Score: 4.7
Cvss Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

Description:

OpenSSL is prone to an information disclosure vulnerability. OpenSSL ECC scalar multiplication, used in e.g. ECDSA and ECDH, has been shown to be vulnerable to a microarchitecture timing side channel attack. An attacker with sufficient acc ess to mount local timing attacks during ECDSA signature generation could recover the private key.

Solution:

VendorFix Upgrade OpenSSL to version 1.0.2q, 1.1.0i or later. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2q Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20181112.txt,https://www.openssl.org/news/vulnerabilities.html,https://github.com/openssl/openssl/commit/aab7c770353b1dc4ba045938c8fb446dd1c4531e,https://eprint.iacr.org/2018/1060.pdf,https://github.com/bbbrumley/portsmash,https://www.exploit-db.com/exploits/45785/

Unique Alert ID: 539292 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 'mod_lua' Denial of Service Vulnerability May15 (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-8109
Cvss Base: 4.3
Cvss Score: 4.3

Description:

Apache HTTP Server is prone to a denial of service vulnerability. Flaw is due to a vulnerability in LuaAuthzProvider that is triggered if a user-supplied LUA script is supplied more than once with different arguments. Successful exploitation will all ow a remote attacker to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Requir e directives.

Solution:

VendorFix Update to version 2.4.12 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.12 Installation path / port: 443/tcp

References:

- http://httpd.apache.org/security/vulnerabilities_24.html,http://www.rapid7.com/db/vulnerabilities/apache-httpd-cve-2014-8109

Unique Alert ID: 539305 Found on: 2023-10-06 Severity: Medium

PHP 'LibGD' Denial of Service Vulnerability (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-2497
Cvss Base: 4.3
Cvss Score: 4.3

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to a NULL pointer dereference error in 'gdImageCreateFromXpm' function within LibGD. Successful exploitation will allow remote attackers to conduct denial of service attacks.

Solution:

VendorFix Update to PHP version 5.4.32 or 5.5.16 or 5.6.0 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.32/5.5.16/5.6.0

References:

- https://bugs.php.net/bug.php?id=66901

Unique Alert ID: 539287 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 'mod_cache' Denial of Service Vulnerability -01 May15 (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-0117
Cvss Base: 4.3
Cvss Score: 4.3

Description:

Apache HTTP Server is prone to a denial of service vulnerability. Flaw is due to vulnerability in mod_proxy module in the Apache HTTP Server. Successful exploitation will allow a remote attacker to cause a denial of service via a crafted HTTP Connection header when a reverse proxy is enabled.

Solution:

VendorFix Update to version 2.4.10 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.10 Installation path / port: 80/tcp

References:

- http://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539286 Found on: 2023-10-06 Severity: Medium

OpenSSH Security Bypass Vulnerability (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-5352
Cvss Base: 4.3
Cvss Score: 4.3

Description:

OpenSSH is prone to a security bypass vulnerability. The flaw is due to the refusal deadline was not checked within the x11_open_helper function. Successful exploitation will allow remote attackers to bypass intended access restrictions.

Solution:

VendorFix Upgrade to OpenSSH version 6.9 or later.

Result:

Installed version: 6.6.1 Fixed version: 6.9 Installation path / port: 22/tcp

References:

- http://openwall.com/lists/oss-security/2015/07/01/10

Unique Alert ID: 539290 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 'mod_cache' Denial of Service Vulnerability -01 May15 (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-0117
Cvss Base: 4.3
Cvss Score: 4.3

Description:

Apache HTTP Server is prone to a denial of service vulnerability. Flaw is due to vulnerability in mod_proxy module in the Apache HTTP Server. Successful exploitation will allow a remote attacker to cause a denial of service via a crafted HTTP Connection header when a reverse proxy is enabled.

Solution:

VendorFix Update to version 2.4.10 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.10 Installation path / port: 443/tcp

References:

- http://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539291 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 'mod_lua' Denial of Service Vulnerability May15 (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-8109
Cvss Base: 4.3
Cvss Score: 4.3

Description:

Apache HTTP Server is prone to a denial of service vulnerability. Flaw is due to a vulnerability in LuaAuthzProvider that is triggered if a user-supplied LUA script is supplied more than once with different arguments. Successful exploitation will all ow a remote attacker to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Requir e directives.

Solution:

VendorFix Update to version 2.4.12 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.12 Installation path / port: 80/tcp

References:

- http://httpd.apache.org/security/vulnerabilities_24.html,http://www.rapid7.com/db/vulnerabilities/apache-httpd-cve-2014-8109

Unique Alert ID: 539288 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 'mod_cache' Denial of Service Vulnerability May15 (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2013-4352		
Cvss Base:	4.3		
Cvss Score:	4.3		

Description:

Apache HTTP Server is prone to a denial of service vulnerability. Flaw is due to vulnerability in 'cache_invalidate' function in modules/cache/cache_storage.c script in the mod_cache module in the Apache HTTP Server. Successful exploitation wi ll allow a remote attacker to cause a denial of service via specially crafted request.

Solution:

VendorFix Update to version 2.4.7 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.7 Installation path / port: 80/tcp

References:

- https://bugzilla.redhat.com/show_bug.cgi?id=1120604,http://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 919588 Found on: 2023-10-06 Severity: Medium

SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2011-3389,CVE-2015-0204		
Cvss Base:	4.3		
Cvss Score:	4.3		

Description:

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system. The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK) An a ttacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service t o get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in t his protocols won't receive security updates anymore.

Solution:

Mitigation It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Result:

In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

References:

- https://ssl-config.mozilla.org/,https://bettercrypto.org/,https://datatracker.ietf.org/doc/rfc8996/,https://vnhacker.bl ogspot.com/2011/09/beast.html,https://web.archive.org/web/20201108095603/https://censys.io/blog/freak,https:// www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014

Unique Alert ID: 539294 Found on: 2023-10-06 Severity: Medium

PHP 'LibGD' Denial of Service Vulnerability (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-2497
Cvss Base: 4.3
Cvss Score: 4.3

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to a NULL pointer dereference error in 'gdImageCreateFromXpm' function within LibGD. Successful exploitation will allow remote attackers to conduct denial of service attacks.

Solution:

VendorFix Update to PHP version 5.4.32 or 5.5.16 or 5.6.0 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.32/5.5.16/5.6.0

References:

- https://bugs.php.net/bug.php?id=66901

Unique Alert ID: 539303 Found on: 2023-10-06 Severity: Medium

Weak Encryption Algorithm(s) Supported (SSH) (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 4.3
Cvss Score: 4.3

Description:

The remote SSH server is configured to allow / support weak encryption algorithm(s). - The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore. - The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it. - A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Solution:

Mitigation Disable the reported weak encryption algorithm(s).

Result:

The remote SSH server supports the following weak client-to-server encryption algorithm(s): 3des-cbc aes128-cbc aes192-cbc aes256-cbc arcfour arcfour128 arcfour256 blowfish-cbc cast128-cbc rijndael-cbc@lysator.liu.se The remote SSH server supports the following weak server-to-client encryption algorithm(s): 3des-cbc aes128-cbc aes192-cbc aes256-cbc arcfour arcfour128 arcfour256 blowfish-cbc cast128-cbc rijndael-cbc@lysator.liu.se

References:

- https://www.rfc-editor.org/rfc/rfc4253#section-6.3

Unique Alert ID: 539289 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 'mod_cache' Denial of Service Vulnerability May15 (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2013-4352
Cvss Base: 4.3
Cvss Score: 4.3

Description:

Apache HTTP Server is prone to a denial of service vulnerability. Flaw is due to vulnerability in 'cache_invalidate' function in modules/cache/cache_storage.c script in the mod_cache module in the Apache HTTP Server. Successful exploitation wi ll allow a remote attacker to cause a denial of service via specially crafted request.

Solution:

VendorFix Update to version 2.4.7 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.7 Installation path / port: 443/tcp

References:

- https://bugzilla.redhat.com/show_bug.cgi?id=1120604,http://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 1533232 Found on: 2023-10-06 Severity: Medium

OpenBSD OpenSSH < 9.1 Multiple Vulnerabilities (tcp/22)

Open Status: NEW **First Found:** 2023-10-06
Cvss Base: 4.0
Cvss Score: 4.0

Description:

OpenBSD OpenSSH is prone to multiple vulnerabilities. The following vulnerabilities exist: - A one-byte overflow in SSH-banner processing in ssh-keyscan. - A double free() in error path of file hashing step in signing/verify code in ssh-keygen . - A double-free in error path in ssh-keysign.

Solution:

VendorFix Update to version 9.1 or later.

Result:

Installed version: 6.6.1 Fixed version: 9.1 Installation path / port: 22/tcp

Unique Alert ID: 539116 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities - 05 - Aug16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-4644,CVE-2015-4643,CVE-2015-4598
Cvss Base: 6.5
Cvss Score: 6.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws exist due to: - Improper validation of token extraction for table na mes, in the php_pgsql_meta_data function in pgsql.c in the PostgreSQL extension. - Integer overflow in the ftp_genlist fu nction in ext/ftp/ftp.c - PHP does not ensure that pathnames lack %00 sequences. Successfully exploiting this issue allow

remote attackers to cause a denial of service, to read or write to arbitrary files, also execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow.

Solution:

VendorFix Update to PHP version 5.4.42, or 5.5.26, or 5.6.10, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.42

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539118 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities - 05 - Aug16 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2015-4644,CVE-2015-4643,CVE-2015-4598	
Cvss Base:	6.5	
Cvss Score:	6.5	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws exist due to: - Improper validation of token extraction for table names, in the php_pgsql_meta_data function in pgsql.c in the PostgreSQL extension. - Integer overflow in the ftp_genlist function in ext/ftp/ftp.c - PHP does not ensure that pathnames lack %00 sequences. Successfully exploiting this issue allow remote attackers to cause a denial of service, to read or write to arbitrary files, also execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow.

Solution:

VendorFix Update to PHP version 5.4.42, or 5.5.26, or 5.6.10, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.42

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 539052 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities - 03 - Jun15 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2015-3329,CVE-2015-3307,CVE-2015-2783,CVE-2015-1352,CVE-2015-4599,CVE-2015-4600,CVE-2015-4602,CVE-2015-4603,CVE-2015-4604,CVE-2015-4605,CVE-2015-3411,CVE-2015-3412	
Cvss Base:	5.3	
Cvss Score:	5.3	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Multiple stack-based buffer overflows in the 'phar_set_inode' function in phar_internal.h script in PHP. - Vulnerabilities in 'phar_parse_metadata' and 'phar_parse_pharfile' functions in ext/phar/phar.c script in PHP. - A NULL pointer dereference flaw in the 'build_tablename' function in 'ext/pgsql/pgsql.c' script that is triggered when handling NULL return values for 'token'. Successfully exploiting this issue allow remote attackers to cause a denial of service, to obtain sensitive information from process memory and to execute arbitrary code via crafted dimensions.

Solution:

VendorFix Update to PHP 5.4.40 or 5.5.24 or 5.6.8 or later.

Result:

Installed Version: 5.4.16 Fixed Version: 5.4.40

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=69085,http://openwall.com/lists/oss-security/2015/06/01/4

Unique Alert ID: 539180 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server Multiple Vulnerabilities Apr18 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2018-1312,CVE-2018-1283,CVE-2017-15715,CVE-2017-15710,CVE-2018-1301	
Cvss Base:	5.9	
Cvss Score:	5.9	
Cvss Vector:	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Multiple flaws exist due to: - Apache HTTP Server fails to correctly generate the nonce sent to prevent reply attacks. - Misconfigured mod_session variable, HTTP_SESSION. - Apache HTTP Server fails to sanitize the expression specified in ''. - An error in Apache HTTP Server 'mod_authnz_ldap' when configured with AuthLDAPCharsetConfig. - Apache HTTP Server fails to sanitize against a specially crafted request. Successful exploitation will allow an attacker to replay HTTP requests across servers without detection, influence the user content, upload a malicious file, crash the Apache HTTP Server and perform denial of service attack.

Solution:

VendorFix Update to version 2.4.30 or later. Please see the references for more information.

Result:

Installed version: 2.4.6 Fixed version: 2.4.30 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539171 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server Multiple Vulnerabilities Apr18 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2018-1312,CVE-2018-1283,CVE-2017-15715,CVE-2017-15710,CVE-2018-1301	
Cvss Base:	5.9	
Cvss Score:	5.9	
Cvss Vector:	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Multiple flaws exist due to: - Apache HTTP Server fails to correctly generate the nonce sent to prevent reply attacks. - Misconfigured mod_session variable, HTTP_SESSION. - Apache HTTP Server fails to sanitize the expression specified in ''. - An error in Apache HTTP Server 'mod_authnz_ldap' when configured with AuthLDAPCharsetConfig. - Apache HTTP Server fails to sanitize against a specially crafted request. Successful exploitation will allow an attacker to replay HTTP requests across servers without detection, influence the user content, upload a malicious file, crash the Apache HTTP Server and perform denial of service attack.

Solution:

VendorFix Update to version 2.4.30 or later. Please see the references for more information.

Result:

Installed version: 2.4.6 Fixed version: 2.4.30 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539071 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities - 03 - Jun15 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2015-3329,CVE-2015-3307,CVE-2015-2783,CVE-2015-1352,CVE-2015-4599,CVE-2015-4600,CVE-2015-4602,CVE-2015-4603,CVE-2015-4604,CVE-2015-4605,CVE-2015-3411,CVE-2015-3412	
Cvss Base:	5.3	
Cvss Score:	5.3	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws are due to: - Multiple stack-based buffer overflows in the 'phar_set_inode' function in phar_internal.h script in PHP. - Vulnerabilities in 'phar_parse_metadata' and 'phar_parse_pharfile' functions in ext/phar/phar.c script in PHP. - A NULL pointer dereference flaw in the 'build_tablename' function in 'ext/pgsql/pgsql.c' script that is triggered when handling NULL return values for 'token'. Successfully exploiting this issue allow remote attackers to cause a denial of service, to obtain sensitive information from process memory and to execute arbitrary code via crafted dimensions.

Solution:

VendorFix Update to PHP 5.4.40 or 5.5.24 or 5.6.8 or later.

Result:

Installed Version: 5.4.16 Fixed Version: 5.4.40

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=69085,http://openwall.com/lists/oss-security/2015/06/01/4

Unique Alert ID: 539186 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities May18 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2018-10549,CVE-2018-10546,CVE-2018-10548,CVE-2018-10547	
Cvss Base:	6.1	
Cvss Score:	6.1	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws exist due to - An out of bounds read error in 'exif_read_data' function while processing crafted JPG data. - An error in stream filter 'convert.iconv' which leads to infinite loop on invalid sequence. - An error in the LDAP module of PHP which allows a malicious LDAP server or man-in-the-middle attacker to crash PHP. - An error in the 'phar_do_404()' function in 'ext/phar/phar_object.c' script which returns parts of the request unfiltered, leading to another XSS vector. This is due to incomplete fix for CVE-2018-5712. Successful exploitation will allow an attacker to conduct XSS attacks, crash PHP, conduct denial-of-service condition and execute arbitrary code in the context of the affected application.

Solution:

VendorFix Update to version 7.2.5 or 7.0.30 or 5.6.36 or 7.1.17 or later. Please see the references for more information.

Result:

Installed version: 5.4.16 Fixed version: 5.6.36 Installation path / port: 443/tcp

References:

- http://www.php.net/ChangeLog-5.php#5.6.36,http://www.php.net/ChangeLog-7.php#7.0.30,http://www.php.net/ChangeLog-7.php#7.1.17,http://www.php.net/ChangeLog-7.php#7.2.5

Unique Alert ID: 539174 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities May18 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2018-10549,CVE-2018-10546,CVE-2018-10548,CVE-2018-10547	
Cvss Base:	6.1	
Cvss Score:	6.1	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	

Description:

PHP is prone to multiple vulnerabilities. Multiple flaws exist due to - An out of bounds read error in 'exif_read_data' function while processing crafted JPG data. - An error in stream filter 'convert.iconv' which leads to infinite loop on invalid sequence. - An error in the LDAP module of PHP which allows a malicious LDAP server or man-in-the-middle attacker to crash PHP. - An error in the 'phar_do_404()' function in 'ext/phar/phar_object.c' script which returns parts of the request unfiltered, leading to another XSS vector. This is due to incomplete fix for CVE-2018-5712. Successful exploitation will allow an attacker to conduct XSS attacks, crash PHP, conduct denial-of-service condition and execute arbitrary code in the context of the affected application.

Solution:

VendorFix Update to version 7.2.5 or 7.0.30 or 5.6.36 or 7.1.17 or later. Please see the references for more information.

Result:

Installed version: 5.4.16 Fixed version: 5.6.36 Installation path / port: 80/tcp

References:

- http://www.php.net/ChangeLog-5.php#5.6.36,http://www.php.net/ChangeLog-7.php#7.0.30,http://www.php.net/ChangeLog-7.php#7.1.17,http://www.php.net/ChangeLog-7.php#7.2.5

Unique Alert ID: 539083 Found on: 2023-10-06 Severity: Medium

OpenSSH Denial of Service And User Enumeration Vulnerabilities (Linux) (tcp/22)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-6515,CVE-2016-6210	
Cvss Base:	5.9	
Cvss Score:	5.9	
Cvss Vector:	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	

Description:

openssh is prone to denial of service and user enumeration vulnerabilities. Multiple flaws exist due to: - The auth_password function in 'auth-passwd.c' script does not limit password lengths for password authentication. - The sshd in OpenSSH, when SHA256 or SHA512 are used for user password hashing uses BLOWFISH hashing on a static password when the username does not exist and it takes much longer to calculate SHA256/SHA512 hash than BLOWFISH hash. Successfully exploiting this issue allows remote attackers to cause a denial of service (crypt CPU consumption) and to enumerate users by leveraging the timing difference between responses when a large password is provided.

Solution:

VendorFix Upgrade to OpenSSH version 7.3 or later.

Result:

Installed version: 6.6.1 Fixed version: 7.3 Installation path / port: 22/tcp

References:

- http://www.openssh.com/txt/release-7.3,http://seclists.org/fulldisclosure/2016/Jul/51,https://security-tracker.debian.org/tracker/CVE-2016-6210,http://openwall.com/lists/oss-security/2016/08/01/2

Unique Alert ID: 539271 Found on: 2023-10-06 Severity: Medium

OpenSSL: 1.0.2 < 1.0.2p / 1.1.0 < 1.1.0i Multiple Vulnerabilities (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-0732,CVE-2018-0737
Cvss Base: 5.9
Cvss Score: 5.9
Cvss Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

OpenSSL is prone to multiple vulnerabilities. The flaws exist due to: - During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client (CVE-2018-0732). - The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack (CVE-2018-0737). Successful exploitation will allow a remote attacker: - to cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack (CVE-2018-0732). - with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key (CVE-2018-0737).

Solution:

VendorFix Upgrade to OpenSSL version 1.1.0i or 1.0.2p or later. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2p Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20180416.txt,https://www.openssl.org/news/secadv/20180612.txt,http://seclists.org/oss-sec/2018/q2/50,https://github.com/openssl/openssl/commit/ea7abeeabf92b7aca160bdd0208636d4da69f4f4,https://github.com/openssl/openssl/commit/3984ef0b72831da8b3ece4745cac4f8575b19098,https://github.com/openssl/openssl/commit/6939eab03a6e23d2bd2c3f5e34fe1d48e542e787,https://github.com/openssl/openssl/commit/349a41da1ad88ad87825414752a8ff5fdd6a6c3f

Unique Alert ID: 607309 Found on: 2023-10-06 Severity: Medium

OpenSSL: 1.0.2 < 1.0.2p / 1.1.0 < 1.1.0i Multiple Vulnerabilities (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-12-18
CVE ID: CVE-2018-0732,CVE-2018-0737
Cvss Base: 5.9
Cvss Score: 5.9
Cvss Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

OpenSSL is prone to multiple vulnerabilities. The flaws exist due to: - During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client (CVE-2018-0732). - The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack (CVE-2018-0737). Successful exploitation will allow a remote attacker: - to cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack (CVE-2018-0732). - with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key (CVE-2018-0737).

Solution:

VendorFix Upgrade to OpenSSL version 1.1.0i or 1.0.2p or later. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2p Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20180416.txt,https://www.openssl.org/news/secadv/20180612.txt,http://seclists.org/oss-sec/2018/q2/50,https://github.com/openssl/openssl/commit/ea7abeeabf92b7aca160bdd0208636d4da69f4f4,https://github.com/openssl/openssl/commit/3984ef0b72831da8b3ece4745cac4f8575b19098,https://github.com/openssl/openssl/commit/6939eab03a6e23d2bd2c3f5e34fe1d48e542e787,https://github.com/openssl/openssl/commit/349a41da1ad88ad87825414752a8ff5fdd6a6c3f

Unique Alert ID: 539187 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities - Sep19 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 6.8
Cvss Score: 6.8

Description:

PHP is prone to multiple vulnerabilities. PHP is prone to multiple vulnerabilities: - Buffer overflow in zendparse - Cast to object confuses GC, causes crash - Exif crash (bus error) due to wrong alignment and invalid cast - Use-after-free in FPM master event handling

Solution:

VendorFix Update to version 7.2.22, 7.3.9 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.22 Installation path / port: 443/tcp

References:

- http://bugs.php.net/78363,http://bugs.php.net/78379,http://bugs.php.net/78333,http://bugs.php.net/77185,https://www.php.net/ChangeLog-7.php#7.3.9,https://www.php.net/ChangeLog-7.php#7.2.22

Unique Alert ID: 539190 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities - 04 - Jun15 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-3330
Cvss Base: 6.8
Cvss Score: 6.8

Description:

PHP is prone to multiple vulnerabilities. The flaw is due to vulnerability in 'php_handler' function in sapi/apache2handler/sapi_apache2.c script in PHP. Successfully exploiting this issue allow remote attackers to cause a denial of service or possibly execute arbitrary code via pipelined HTTP requests.

Solution:

VendorFix Update to PHP 5.4.40 or 5.5.24 or 5.6.8 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.40 Installation path / port: 80/tcp

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=69085,http://openwall.com/lists/oss-security/2015/06/01/4

Unique Alert ID: 539176 Found on: 2023-10-06 Severity: Medium

PHP Heap Use-After-Free Vulnerability - Sep19 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 6.8
Cvss Score: 6.8

Description:

PHP is prone to a heap-based use-after-free vulnerability. PHP is prone to a heap use-after-free in pcrelib (cmb).

Solution:

VendorFix Update to version 7.1.32 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.1.32 Installation path / port: 443/tcp

References:

- http://bugs.php.net/75457,https://www.php.net/ChangeLog-7.php#7.1.32

Unique Alert ID: 539177 Found on: 2023-10-06 Severity: Medium

PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-7804,CVE-2015-7803
Cvss Base: 6.8
Cvss Score: 6.8

Description:

PHP is prone to multiple denial of service (DoS) vulnerabilities. Multiple flaws are due to: - An Off-by-one error in the 'phar_parse_zipfile' function within ext/phar/zip.c script. - An error in the 'phar_get_entry_data' function in ext/phar/util.c script. Successfully exploiting this issue allow remote attackers to cause a denial of service (NULL pointer dereference and application crash).

Solution:

VendorFix Update to PHP 5.5.30 or 5.6.14 or later.

Result:

Installed Version: 5.4.16 Fixed Version: 5.5.30

References:

- http://www.php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=70433,http://www.openwall.com/lists/oss-security/2015/10/05/8

Unique Alert ID: 919552 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server Multiple Vulnerabilities (Sep 2014) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2013-5704,CVE-2014-0118,CVE-2014-0226,CVE-2014-0231	
Cvss Base:	6.8	
Cvss Score:	6.8	

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2013-5704: HTTP trailers could be used to replace HTTP headers late during request processing, potentially undoing or otherwise confusing modules that examined or modified request headers earlier. This fix adds the 'MergeTrailers' directive to restore legacy behavior. - CVE-2014-0118: A resource consumption flaw was found in mod_deflate. If request body decompression was configured (using the 'DEFLATE' input filter), a remote attacker could cause the server to consume significant memory and/or CPU resources. The use of request body decompression is not a common configuration. - CVE-2014-0226: A race condition was found in mod_status. An attacker able to access a public server status page on a server using a threaded MPM could send a carefully crafted request which could lead to a heap buffer overflow. Note that it is not a default or recommended configuration to have a public accessible server status page. - CVE-2014-0231: A flaw was found in mod_cgid. If a server using mod_cgid hosted CGI scripts which did not consume standard input, a remote attacker could cause child processes to hang indefinitely, leading to denial of service.

Solution:

VendorFix Update to version 2.2.29, 2.4.12 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.12 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_22.html,https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 1050985 Found on: 2023-10-06 Severity: Medium

PHP Sessions Subsystem Session Fixation Vulnerability (Aug 2013) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2022-11-05
CVE ID:	CVE-2011-4718	
Cvss Base:	6.8	
Cvss Score:	6.8	

Description:

PHP is prone to a session fixation vulnerability. Session fixation vulnerability in the Sessions subsystem in PHP allows remote attackers to hijack web sessions by specifying a session ID.

Solution:

VendorFix - Update to PHP version 5.5.2 or later and set 'session.use_strict_mode' in php.ini to 'On' - make adoptive session with user land code as described in the referenced PHP strict_sessions document

Result:

Installed version: 5.4.16 Fixed version: 5.5.2 Installation path / port: 80/tcp

References:

- https://wiki.php.net/rfc/strict_sessions,https://wiki.php.net/rfc/strict_sessions#current_solution,https://access.redhat.com/security/cve/cve-2011-4718,http://secunia.com/advisories/54562,http://cxsecurity.com/cveshow/CVE-2011-4718

Unique Alert ID: 539188 Found on: 2023-10-06 Severity: Medium

PHP Multiple Denial of Service Vulnerabilities - 01 - Dec15 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2015-7804,CVE-2015-7803		
Cvss Base:	6.8		
Cvss Score:	6.8		

Description:

PHP is prone to multiple denial of service (DoS) vulnerabilities. Multiple flaws are due to: - An Off-by-one error in the 'phar_parse_zipfile' function within ext/phar/zip.c script. - An error in the 'phar_get_entry_data' function in ext/phar/util.c script. Successfully exploiting this issue allow remote attackers to cause a denial of service (NULL pointer dereference and application crash).

Solution:

VendorFix Update to PHP 5.5.30 or 5.6.14 or later.

Result:

Installed Version: 5.4.16 Fixed Version: 5.5.30

References:

- http://www.php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=70433,http://www.openwall.com/lists/oss-security/2015/10/05/8

Unique Alert ID: 1050987 Found on: 2023-10-06 Severity: Medium

PHP < 7.4.31, 8.0.x < 8.0.24, 8.1.x < 8.1.11 Security Update - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-11-05
CVE ID:	CVE-2022-31628,CVE-2022-31629		
Cvss Base:	6.5		
Cvss Score:	6.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N		

Description:

PHP is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2022-31628: The phar uncompressor code would recursively uncompress 'quines' gzip files, resulting in an infinite loop. - CVE-2022-31629: The vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a '__Host-' or '__Secure-' cookie by PHP applications.

Solution:

VendorFix Update to version 7.4.31, 8.0.24, 8.1.11 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.4.31 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.4.31,https://www.php.net/ChangeLog-8.php#8.0.24,https://www.php.net/ChangeLog-8.php#8.1.11,https://bugs.php.net/bug.php?id=81726,https://bugs.php.net/bug.php?id=81727

Unique Alert ID: 539184 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities - 04 - Jun15 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-3330
Cvss Base: 6.8
Cvss Score: 6.8

Description:

PHP is prone to multiple vulnerabilities. The flaw is due to vulnerability in 'php_handler' function in sapi/apache2handler/sapi_apache2.c script in PHP. Successfully exploiting this issue allow remote attackers to cause a denial of service or possibly execute arbitrary code via pipelined HTTP requests.

Solution:

VendorFix Update to PHP 5.4.40 or 5.5.24 or 5.6.8 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.40 Installation path / port: 443/tcp

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=69085,http://openwall.com/lists/oss-security/2015/06/01/4

Unique Alert ID: 539173 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server Multiple Vulnerabilities May15 (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-3523,CVE-2014-0118,CVE-2014-0226,CVE-2014-0231
Cvss Base: 6.8
Cvss Score: 6.8

Description:

Apache HTTP Server is prone to a denial of service vulnerability. Multiple flaws are due to: - Vulnerability in the WinNT MPM component within the 'winnt_accept' function in server/mpm/winnt/child.c script that is triggered when the default AcceptFilter is used. - Vulnerability in the mod_deflate module that is triggered when handling highly compressed bodies. - A race condition in the mod_status module that is triggered as user-supplied input is not properly validated when handling the scoreboard. - Vulnerability in the mod_cgid module that is triggered when used to host CGI scripts that do not consume standard input. Successful exploitation will allow a remote attacker to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives.

Solution:

VendorFix Update to version 2.4.10 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.10 Installation path / port: 443/tcp

References:

- http://httpd.apache.org/security/vulnerabilities_24.html,http://www.rapid7.com/db/vulnerabilities/apache-httpd-cve-2014-8109

Unique Alert ID: 539182 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server Multiple Vulnerabilities May15 (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-3523,CVE-2014-0118,CVE-2014-0226,CVE-2014-0231		
Cvss Base:	6.8		
Cvss Score:	6.8		

Description:

Apache HTTP Server is prone to a denial of service vulnerability. Multiple flaws are due to: - Vulnerability in the WinNT MPM component within the 'winnt_accept' function in server/mpm/winnt/child.c script that is triggered when the default AcceptFilter is used. - Vulnerability in the mod_deflate module that is triggered when handling highly compressed bodies. - A race condition in the mod_status module that is triggered as user-supplied input is not properly validated when handling the scoreboard. - Vulnerability in the mod_cgid module that is triggered when used to host CGI scripts that do not consume standard input. Successful exploitation will allow a remote attacker to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives.

Solution:

VendorFix Update to version 2.4.10 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.10 Installation path / port: 80/tcp

References:

- http://httpd.apache.org/security/vulnerabilities_24.html,http://www.rapid7.com/db/vulnerabilities/apache-httpd-cve-2014-8109

Unique Alert ID: 1050984 Found on: 2023-10-06 Severity: Medium

PHP Sessions Subsystem Session Fixation Vulnerability (Aug 2013) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-11-05
CVE ID:	CVE-2011-4718		
Cvss Base:	6.8		
Cvss Score:	6.8		

Description:

PHP is prone to a session fixation vulnerability. Session fixation vulnerability in the Sessions subsystem in PHP allows remote attackers to hijack web sessions by specifying a session ID.

Solution:

VendorFix - Update to PHP version 5.5.2 or later and set 'session.use_strict_mode' in php.ini to 'On' - make adoptive session with user land code as described in the referenced PHP strict_sessions document

Result:

Installed version: 5.4.16 Fixed version: 5.5.2 Installation path / port: 443/tcp

References:

- https://wiki.php.net/rfc/strict_sessions,https://wiki.php.net/rfc/strict_sessions#current_solution,https://access.redhat.com/security/cve/cve-2011-4718,http://secunia.com/advisories/54562,http://cxsecurity.com/cveshow/CVE-2011-4718

Unique Alert ID: 539183 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities - Sep19 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 6.8
Cvss Score: 6.8

Description:

PHP is prone to multiple vulnerabilities. PHP is prone to multiple vulnerabilities: - Buffer overflow in zendparse - Cast to o bject confuses GC, causes crash - Exif crash (bus error) due to wrong alignment and invalid cast - Use-after-free in FPM master event handling

Solution:

VendorFix Update to version 7.2.22, 7.3.9 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.22 Installation path / port: 80/tcp

References:

- http://bugs.php.net/78363,http://bugs.php.net/78379,http://bugs.php.net/78333,http://bugs.php.net/77185,https://www.php.net/ChangeLog-7.php#7.3.9,https://www.php.net/ChangeLog-7.php#7.2.22

Unique Alert ID: 539175 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities - 01 - Aug14 (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-3597,CVE-2014-3587,CVE-2014-5120
Cvss Base: 6.8
Cvss Score: 6.8

Description:

PHP is prone to multiple vulnerabilities. The flaws exist due to: - Multiple overflow conditions in the 'php_parserr' function within ext/standard/dns.c script. - Integer overflow in the 'cdf_read_property_info' function in cdf.c within the Fileinfo com ponent. - An error in the '_php_image_output_ctx' function within ext/gd/gd_ctx.c script as NULL bytes in paths to various image handling functions are not stripped. Successful exploitation will allow remote attackers to overwrite arbitrary files, conduct denial of service attacks or potentially execute arbitrary code.

Solution:

VendorFix Update to PHP version 5.4.32 or 5.5.16 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.32/5.5.16

References:

- http://php.net/ChangeLog-5.php,http://secunia.com/advisories/59709,http://secunia.com/advisories/57349

Unique Alert ID: 1050986 Found on: 2023-10-06 Severity: Medium

PHP < 7.4.31, 8.0.x < 8.0.24, 8.1.x < 8.1.11 Security Update - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-11-05
CVE ID: CVE-2022-31628,CVE-2022-31629

Cvss Base: 6.5
Cvss Score: 6.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

Description:

PHP is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2022-31628: The phar uncompressor co de would recursively uncompress 'quines' gzip files, resulting in an infinite loop. - CVE-2022-31629: The vulnerability ena bles network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a '__H ost-' or '__Secure-' cookie by PHP applications.

Solution:

VendorFix Update to version 7.4.31, 8.0.24, 8.1.11 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.4.31 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.4.31,https://www.php.net/ChangeLog-8.php#8.0.24,https://www.php.net/ChangeLog-8.php#8.1.11,https://bugs.php.net/bug.php?id=81726,https://bugs.php.net/bug.php?id=81727

Unique Alert ID: 539181 Found on: 2023-10-06 Severity: Medium

PHP Multiple Vulnerabilities - 01 - Aug14 (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-3597,CVE-2014-3587,CVE-2014-5120
Cvss Base: 6.8
Cvss Score: 6.8

Description:

PHP is prone to multiple vulnerabilities. The flaws exist due to: - Multiple overflow conditions in the 'php_parserr' function within ext/standard/dns.c script. - Integer overflow in the 'cdf_read_property_info' function in cdf.c within the Fileinfo com ponent. - An error in the '_php_image_output_ctx' function within ext/gd/gd_ctx.c script as NULL bytes in paths to various image handling functions are not stripped. Successful exploitation will allow remote attackers to overwrite arbitrary files, conduct denial of service attacks or potentially execute arbitrary code.

Solution:

VendorFix Update to PHP version 5.4.32 or 5.5.16 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.32/5.5.16

References:

- http://php.net/ChangeLog-5.php,http://secunia.com/advisories/59709,http://secunia.com/advisories/57349

Unique Alert ID: 539169 Found on: 2023-10-06 Severity: Medium

PHP Heap Use-After-Free Vulnerability - Sep19 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 6.8
Cvss Score: 6.8

Description:

PHP is prone to a heap-based use-after-free vulnerability. PHP is prone to a heap use-after-free in pcrelib (cmb).

Solution:

VendorFix Update to version 7.1.32 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.1.32 Installation path / port: 80/tcp

References:

- http://bugs.php.net/75457,https://www.php.net/ChangeLog-7.php#7.1.32

Unique Alert ID: 919553 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server Multiple Vulnerabilities (Sep 2014) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2013-5704,CVE-2014-0118,CVE-2014-0226,CVE-2014-0231
Cvss Base: 6.8
Cvss Score: 6.8

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2013-5704: HTTP trailers could be used to replace HTTP headers late during request processing, potentially undoing or otherwise confusing modules that examined or modified request headers earlier. This fix adds the 'MergeTrailers' directive to restore legacy behavior. - CVE-2014-0118: A resource consumption flaw was found in mod_deflate. If request body decompression was configured (using the 'DEFLATE' input filter), a remote attacker could cause the server to consume significant memory and/or CPU resources. The use of request body decompression is not a common configuration. - CVE-2014-0226: A race condition was found in mod_status. An attacker able to access a public server status page on a server using a threaded MPM could send a carefully crafted request which could lead to a heap buffer overflow. Note that it is not a default or recommended configuration to have a public accessible server status page. - CVE-2014-0231: A flaw was found in mod_cgid. If a server using mod_cgid hosted CGI scripts which did not consume standard input, a remote attacker could cause child processes to hang indefinitely, leading to denial of service.

Solution:

VendorFix Update to version 2.2.29, 2.4.12 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.12 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_22.html,https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539168 Found on: 2023-10-06 Severity: Medium

PHP 'PHP-FPM' Denial of Service Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-9253
Cvss Base: 6.5
Cvss Score: 6.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw exists due to the php-fpm master process restarts a child process in an endless loop when using program execution functions with a non-blocking STDIN stream. Successfully expl oitation will allow an attacker to consume 100% of the CPU, and consume disk space with a large volume of error logs, a s demonstrated by an attack by a customer of a shared-hosting facility.

Solution:

VendorFix Update to PHP 7.1.20, 7.2.8 or 7.3.0alpha3.

Result:

Installed version: 5.4.16 Fixed version: 7.1.20 Installation path / port: 80/tcp

References:

- https://bugs.php.net/bug.php?id=73342,https://bugs.php.net/bug.php?id=70185,https://github.com/php/php-src/pul l/3287,https://www.futureweb.at/security/CVE-2015-9253

Unique Alert ID: 539170 Found on: 2023-10-06 Severity: Medium

PHP 'PHP-FPM' Denial of Service Vulnerability (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-9253
Cvss Base: 6.5
Cvss Score: 6.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw exists due to the php-fpm master process restarts a child process in an endless loop when using program execution functions with a non-blocking STDIN stream. Successfully expl oitation will allow an attacker to consume 100% of the CPU, and consume disk space with a large volume of error logs, a s demonstrated by an attack by a customer of a shared-hosting facility.

Solution:

VendorFix Update to PHP 7.1.20, 7.2.8 or 7.3.0alpha3.

Result:

Installed version: 5.4.16 Fixed version: 7.1.20 Installation path / port: 443/tcp

References:

- https://bugs.php.net/bug.php?id=73342,https://bugs.php.net/bug.php?id=70185,https://github.com/php/php-src/pul l/3287,https://www.futureweb.at/security/CVE-2015-9253

Unique Alert ID: 919554 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.31, 7.4.x < 7.4.24, 8.0.x < 8.0.11 Security Update (Sep 2021) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-21706
Cvss Base: 6.5
Cvss Score: 6.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

Description:

PHP released new versions which includes a security fix. Fixed bug #81420 (ZipArchive::extractTo extracts outside of des tination).

Solution:

VendorFix Update to version 7.3.31, 7.4.24, 8.0.11 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.31 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.31,https://www.php.net/ChangeLog-7.php#7.4.24,https://www.php.net/ChangeLog-8.php#8.0.11,http://bugs.php.net/81420

Unique Alert ID: 919559 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.31, 7.4.x < 7.4.24, 8.0.x < 8.0.11 Security Update (Sep 2021) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-21706
Cvss Base: 6.5
Cvss Score: 6.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

Description:

PHP released new versions which includes a security fix. Fixed bug #81420 (ZipArchive::extractTo extracts outside of des tination).

Solution:

VendorFix Update to version 7.3.31, 7.4.24, 8.0.11 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.31 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.31,https://www.php.net/ChangeLog-7.php#7.4.24,https://www.php.net/ChangeLog-8.php#8.0.11,http://bugs.php.net/81420

Unique Alert ID: 539196 Found on: 2023-10-06 Severity: Medium

PHP < 7.2.26 Multiple Vulnerabilities - Dec19 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2019-11046,CVE-2019-11045,CVE-2019-11050,CVE-2019-11047		
Cvss Base:	6.5		
Cvss Score:	6.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L		

Description:

PHP is prone to multiple vulnerabilities. PHP is prone to multiple vulnerabilities: - Buffer underflow in bc_shift_addsub (CVE-2019-11046) - DirectoryIterator class silently truncates after a null byte (CVE-2019-11045) - Use-after-free in exif parsing under memory sanitizer (CVE-2019-11050) - Heap-buffer-overflow READ in exif (CVE-2019-11047)

Solution:

VendorFix Update to version 7.2.26 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.26 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.26

Unique Alert ID: 919558 Found on: 2023-10-06 Severity: Medium

PHP < 7.2.34, 7.3 < 7.3.23, 7.4 < 7.4.11 Multiple Vulnerabilities - October20 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2020-7069,CVE-2020-7070		
Cvss Base:	5.3		
Cvss Score:	5.3		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N		

Description:

PHP is prone to multiple vulnerabilities. The following vulnerabilities exist: - Wrong ciphertext/tag in AES-CCM encryption for a 12 bytes IV (CVE-2020-7069) - PHP parses encoded cookie names so malicious '__Host-' cookies can be sent (CVE-2020-7070)

Solution:

VendorFix Update to version 7.2.34, 7.3.23, 7.4.11 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.34 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.34,https://www.php.net/ChangeLog-7.php#7.3.23,https://www.php.net/ChangeLog-7.php#7.4.11

Unique Alert ID: 919555 Found on: 2023-10-06 Severity: Medium

PHP < 7.2.34, 7.3 < 7.3.23, 7.4 < 7.4.11 Multiple Vulnerabilities - October20 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2020-7069,CVE-2020-7070
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description:

PHP is prone to multiple vulnerabilities. The following vulnerabilities exist: - Wrong ciphertext/tag in AES-CCM encryption for a 12 bytes IV (CVE-2020-7069) - PHP parses encoded cookie names so malicious '__Host-' cookies can be sent (CVE-2020-7070)

Solution:

VendorFix Update to version 7.2.34, 7.3.23, 7.4.11 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.34 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.34,https://www.php.net/ChangeLog-7.php#7.3.23,https://www.php.net/ChangeLog-7.php#7.4.11

Unique Alert ID: 919556 Found on: 2023-10-06 Severity: Medium

OpenSSL DoS Vulnerability (20180327) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2018-0739
Cvss Base: 6.5
Cvss Score: 6.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Description:

OpenSSL is prone to a denial of service (DoS) vulnerability. Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could resu lt in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so t his is considered safe. Reported by OSS-fuzz.

Solution:

VendorFix Update to version 1.0.2o, 1.1.0h or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2o Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20180327.txt

Unique Alert ID: 539194 Found on: 2023-10-06 Severity: Medium

PHP < 7.2.26 Multiple Vulnerabilities - Dec19 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2019-11046,CVE-2019-11045,CVE-2019-11050,CVE-2019-11047		
Cvss Base:	6.5		
Cvss Score:	6.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L		

Description:

PHP is prone to multiple vulnerabilities. PHP is prone to multiple vulnerabilities: - Buffer underflow in bc_shift_addsub (CVE-2019-11046) - DirectoryIterator class silently truncates after a null byte (CVE-2019-11045) - Use-after-free in exif parsing under memory sanitizer (CVE-2019-11050) - Heap-buffer-overflow READ in exif (CVE-2019-11047)

Solution:

VendorFix Update to version 7.2.26 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.26 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.26

Unique Alert ID: 919557 Found on: 2023-10-06 Severity: Medium

OpenSSL DoS Vulnerability (20180327) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2018-0739		
Cvss Base:	6.5		
Cvss Score:	6.5		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H		

Description:

OpenSSL is prone to a denial of service (DoS) vulnerability. Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Reported by OSS-fuzz.

Solution:

VendorFix Update to version 1.0.2o, 1.1.0h or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2o Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20180327.txt

Unique Alert ID: 1533215 Found on: 2023-10-06 Severity: Medium

OpenSSL DoS Vulnerability (20230719) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2023-10-06
CVE ID: CVE-2023-3446

Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Description:

OpenSSL is prone to a denial of service (DoS) vulnerability. Checking excessively long DH keys or parameters may be v ery slow. Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH ke y or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtain ed from an untrusted source this may lead to a Denial of Service.

Solution:

NoneAvailable No known solution is available as of 19th July, 2023. Information regarding this issue will be updated once solution details are available. Vendor info: Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available. The fix is also available in commit fc9867c1 (for 3.1), commit 1fa20cf2 (for 3.0) and commit 8780a896 (for 1.1.1) in the OpenSSL git repository. It is available to premium support customer in commit 9a0a4d3c (for 1.0.2).

Result:

Installed version: 1.0.2k Fixed version: None Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20230719.txt

Unique Alert ID: 539216 Found on: 2023-10-06 Severity: Medium

OpenSSH <= 7.2p1 - Xauth Injection (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2016-3115
Cvss Base: 6.4
Cvss Score: 6.4
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

Description:

openssh xauth command injection may lead to forced-command and /bin/false bypass An authenticated user may inject arbitrary xauth commands by sending an x11 channel request that includes a newline character in the x11 cookie. The ne wline acts as a command separator to the xauth binary. This attack requires the server to have 'X11Forwarding yes' ena bled. Disabling it, mitigates this vector. By injecting xauth commands one gains limited* read/write arbitrary files, inform ation leakage or xauth-connect capabilities.

Solution:

VendorFix Upgrade to OpenSSH version 7.2p2 or later.

Result:

Installed version: 6.6.1 Fixed version: 7.2p2 Installation path / port: 22/tcp

References:

- http://www.openssh.com/txt/release-7.2p2

Unique Alert ID: 1533216 Found on: 2023-10-06 Severity: Medium

OpenSSL DoS Vulnerability (20230719) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2023-10-06
CVE ID: CVE-2023-3446
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Description:

OpenSSL is prone to a denial of service (DoS) vulnerability. Checking excessively long DH keys or parameters may be v ery slow. Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH ke y or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtain ed from an untrusted source this may lead to a Denial of Service.

Solution:

NoneAvailable No known solution is available as of 19th July, 2023. Information regarding this issue will be updated once solution details are available. Vendor info: Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available. The fix is also available in commit fc9867c1 (for 3.1), commit 1fa20cf2 (for 3.0) and commit 8780a896 (for 1.1.1) in the OpenSSL git repository. It is available to premium support customer in commit 9a0a4d3c (for 1.0.2).

Result:

Installed version: 1.0.2k Fixed version: None Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20230719.txt

Unique Alert ID: 919561 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server CRLF Injection Vulnerability (Dec 2016) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2016-4975
Cvss Base: 6.1
Cvss Score: 6.1
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Description:

Apache HTTP Server is prone to a CRLF injection vulnerability. Possible CRLF injection allowing HTTP response splitting at tacks for sites which use mod_userdir. This issue was mitigated to prohibit CR or LF injection into the 'Location' or other o utbound header key or value.

Solution:

VendorFix Update to version 2.2.32, 2.4.25 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.25 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_22.html,https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539215 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 2.4.0 < 2.4.42 Multiple Vulnerabilities (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2020-1927,CVE-2020-1934

Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Apache HTTP Server is prone to multiple vulnerabilities: - mod_rewrite CWE-601 open redirect (CVE-2020-1927) - mod_proxy_ftp use of uninitialized value (CVE-2020-1934)

Solution:

VendorFix Update to version 2.4.42 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.42 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539213 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 2.4.0 < 2.4.42 Multiple Vulnerabilities (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2020-1927,CVE-2020-1934
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Apache HTTP Server is prone to multiple vulnerabilities: - mod_rewrite CWE-601 open redirect (CVE-2020-1927) - mod_proxy_ftp use of uninitialized value (CVE-2020-1934)

Solution:

VendorFix Update to version 2.4.42 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.42 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539211 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 2.4.0 - 2.4.40 Multiple Vulnerabilities (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2019-10092,CVE-2019-10098
Cvss Base: 6.1
Cvss Score: 6.1
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Apache HTTP server is prone to multiple vulnerabilities: - A limite d cross-site scripting issue affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed. (CVE-2019-10092) - Redirects co nfigured with mod_rewrite that were intended to be self referential might be fooled by encoded newlines and redirect inst ead to an unexpected URL within the request URL. (CVE-2019-10098)

Solution:

VendorFix Update to version 2.4.41 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.41 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 919560 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server CRLF Injection Vulnerability (Dec 2016) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2016-4975		
Cvss Base:	6.1		
Cvss Score:	6.1		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N		

Description:

Apache HTTP Server is prone to a CRLF injection vulnerability. Possible CRLF injection allowing HTTP response splitting at tacks for sites which use mod_userdir. This issue was mitigated to prohibit CR or LF injection into the 'Location' or other o utbound header key or value.

Solution:

VendorFix Update to version 2.2.32, 2.4.25 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.25 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_22.html,https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539209 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 2.4.0 - 2.4.40 Multiple Vulnerabilities (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2019-10092,CVE-2019-10098		
Cvss Base:	6.1		
Cvss Score:	6.1		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N		

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Apache HTTP server is prone to multiple vulnerabilities: - A limite d cross-site scripting issue affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed. (CVE-2019-10092) - Redirects co nfigured with mod_rewrite that were intended to be self referential might be fooled by encoded newlines and redirect inst ead to an unexpected URL within the request URL. (CVE-2019-10098)

Solution:

VendorFix Update to version 2.4.41 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.41 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539296 Found on: 2023-10-06 Severity: Medium

PHP 'PHAR' Error Page Reflected XSS And DoS Vulnerabilities (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2018-5712,CVE-2018-5711		
Cvss Base:	5.5		
Cvss Score:	5.5		
Cvss Vector:	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H		

Description:

PHP is prone to cross site scripting (XSS) and denial of service (DoS) vulnerabilities. Multiple flaws are due to: - An input validation error on the PHAR 404 error page via the URI of a request for a .phar file. - An integer signedness error in gd_gif_in.c in the GD Graphics Library (aka libgd). Successfully exploiting this issue allows attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks and will also lead to a denial of service and exhausting the server resources.

Solution:

VendorFix Update to PHP version 5.6.33, 7.0.27, 7.1.13 or 7.2.1 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.33 Installation path / port: 80/tcp

References:

- http://php.net/ChangeLog-5.php,http://php.net/ChangeLog-7.php,https://bugs.php.net/bug.php?id=74782,https://bugs.php.net/bug.php?id=75571

Unique Alert ID: 539300 Found on: 2023-10-06 Severity: Medium

PHP 'PHAR' Error Page Reflected XSS And DoS Vulnerabilities (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2018-5712,CVE-2018-5711		
Cvss Base:	5.5		
Cvss Score:	5.5		
Cvss Vector:	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H		

Description:

PHP is prone to cross site scripting (XSS) and denial of service (DoS) vulnerabilities. Multiple flaws are due to: - An input validation error on the PHAR 404 error page via the URI of a request for a .phar file. - An integer signedness error in gd_gif_in.c in the GD Graphics Library (aka libgd). Successfully exploiting this issue allows attacker to execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site. This may allow the attacker to steal cookie-based authentication credentials and to launch other attacks and will also lead to a denial of service and exhausting the server resources.

Solution:

VendorFix Update to PHP version 5.6.33, 7.0.27, 7.1.13 or 7.2.1 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.6.33 Installation path / port: 443/tcp

References:

- http://php.net/ChangeLog-5.php,http://php.net/ChangeLog-7.php,https://bugs.php.net/bug.php?id=74782,https://bugs.php.net/bug.php?id=75571

Unique Alert ID: 539298 Found on: 2023-10-06 Severity: Medium

PHP Cross-Site Scripting Vulnerability - Aug16 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-8935
Cvss Base: 6.1
Cvss Score: 6.1
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Description:

PHP is prone to a cross-site scripting (XSS) vulnerability. The flaw is due to the 'sapi_header_op' function in 'main/SAPI.c' script supports deprecated line folding without considering browser compatibility. Successfully exploiting this issue allows remote attackers to conduct cross-site scripting (XSS) attacks against Internet Explorer by leveraging '%0A%20' or '%0D%0A%20' mishandling in the header function.

Solution:

VendorFix Update to PHP version 5.4.38, or 5.5.22, or 5.6.6, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.38

References:

- https://bugs.php.net/bug.php?id=68978

Unique Alert ID: 539299 Found on: 2023-10-06 Severity: Medium

PHP Cross-Site Scripting Vulnerability - Aug16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-8935
Cvss Base: 6.1
Cvss Score: 6.1
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Description:

PHP is prone to a cross-site scripting (XSS) vulnerability. The flaw is due to the 'sapi_header_op' function in 'main/SAPI.c' script supports deprecated line folding without considering browser compatibility. Successfully exploiting this issue allows remote attackers to conduct cross-site scripting (XSS) attacks against Internet Explorer by leveraging '%0A%20' or '%0D%0A%20' mishandling in the header function.

Solution:

VendorFix Update to PHP version 5.4.38, or 5.5.22, or 5.6.6, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.38

References:

- https://bugs.php.net/bug.php?id=68978

Unique Alert ID: 539167 Found on: 2023-10-06 Severity: Medium

PHP Denial of Service Vulnerability - 01 - Jul16 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-8878
Cvss Base: 5.9
Cvss Score: 5.9
Cvss Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to script 'main/php_open_temporary_file.c' does n ot ensure thread safety. Successfully exploiting this issue allow remote attackers to cause a denial of service (race condit ion and heap memory corruption) by leveraging an application that performs many temporary-file accesses.

Solution:

VendorFix Update to PHP version 5.5.28, or 5.6.12, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.28

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 919562 Found on: 2023-10-06 Severity: Medium

OpenSSL: Null pointer deref in X509_issuer_and_serial_hash() (CVE-2021-23841) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-23841
Cvss Base: 5.9
Cvss Score: 5.9
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

OpenSSL is prone to a denial of service (DoS) vulnerability. The OpenSSL public API function X509_issuer_and_serial_ha sh() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certific ate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This vulnerability may subsequently result in a NULL pointer deref and a crash lea ding to a potential denial of service attack.

Solution:

VendorFix Update to version 1.0.2y, 1.1.1j or later. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2y / 1.1.1j Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20210216.txt

Unique Alert ID: 539166 Found on: 2023-10-06 Severity: Medium

PHP Denial of Service Vulnerability - 01 - Jul16 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-8878
Cvss Base: 5.9
Cvss Score: 5.9
Cvss Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to script 'main/php_open_temporary_file.c' does n ot ensure thread safety. Successfully exploiting this issue allow remote attackers to cause a denial of service (race condit ion and heap memory corruption) by leveraging an application that performs many temporary-file accesses.

Solution:

VendorFix Update to PHP version 5.5.28, or 5.6.12, or later.

Result:

Installed version: 5.4.16 Fixed version: 5.5.28

References:

- http://www.php.net/ChangeLog-5.php

Unique Alert ID: 919565 Found on: 2023-10-06 Severity: Medium

OpenSSL: Null pointer deref in X509_issuer_and_serial_hash() (CVE-2021-23841) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-23841
Cvss Base: 5.9
Cvss Score: 5.9
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

OpenSSL is prone to a denial of service (DoS) vulnerability. The OpenSSL public API function X509_issuer_and_serial_ha sh() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certific ate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This vulnerability may subsequently result in a NULL pointer deref and a crash lea ding to a potential denial of service attack.

Solution:

VendorFix Update to version 1.0.2y, 1.1.1j or later. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2y / 1.1.1j Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20210216.txt

Unique Alert ID: 607311 Found on: 2023-10-06 Severity: Medium

OpenSSL Security Bypass Vulnerability - DEC 2017 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-12-18
CVE ID: CVE-2017-3737

Cvss Base: 5.9
Cvss Score: 5.9
Cvss Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

OpenSSL is prone to a security bypass vulnerability. When SSL_read()/SSL_write() is subsequently called by the applicati on for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from th e SSL/TLS record layer. Successfully exploiting this issue will allow attackers to bypass security restrictions and perform unauthorized actions. This may aid in launching further attacks.

Solution:

VendorFix OpenSSL 1.0.2 users should upgrade to 1.0.2n.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2n Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20171207.txt

Unique Alert ID: 607313 Found on: 2023-10-06 Severity: Medium

OpenSSL: 0-byte record padding oracle (CVE-2019-1559) (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-12-18
CVE ID: CVE-2019-1559
Cvss Base: 5.9
Cvss Score: 5.9
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

OpenSSL is prone to a padding oracle attack. If an application encounters a fatal protocol error and then calls SSL_shutd own() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling a pplication if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MA C. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amou nts to a padding oracle that could be used to decrypt data. In order for this to be exploitable 'non-stitched' ciphersuites m ust be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the applic ation must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do a nyway). AEAD ciphersuites are not impacted.

Solution:

VendorFix Upgrade OpenSSL to version 1.0.2r or later. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2r Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20190226.txt,https://github.com/RUB-NDS/TLS-Padding-Oracles#openssl-cv e-2019-1559

Unique Alert ID: 539302 Found on: 2023-10-06 Severity: Medium

OpenSSL: 0-byte record padding oracle (CVE-2019-1559) (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2019-1559		
Cvss Base:	5.9		
Cvss Score:	5.9		
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N		

Description:

OpenSSL is prone to a padding oracle attack. If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable 'non-stitched' ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). AEAD ciphersuites are not impacted.

Solution:

VendorFix Upgrade OpenSSL to version 1.0.2r or later. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2r Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20190226.txt,https://github.com/RUB-NDS/TLS-Padding-Oracles#openssl-cve-2019-1559

Unique Alert ID: 1010826 Found on: 2023-10-06 Severity: Medium

OpenSSL: BN_mod_exp may produce incorrect results on MIPS (CVE-2021-4160) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-08-27
CVE ID:	CVE-2021-4160		
Cvss Base:	5.9		
Cvss Score:	5.9		
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N		

Description:

OpenSSL is prone to a carry propagation vulnerability. There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701.

Solution:

VendorFix Update to version 1.1.1m, 3.0.1 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.1.1m Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20220128.txt

Unique Alert ID: 1010827 Found on: 2023-10-06 Severity: Medium

OpenSSL: BN_mod_exp may produce incorrect results on MIPS (CVE-2021-4160) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-08-27
CVE ID:	CVE-2021-4160		
Cvss Base:	5.9		
Cvss Score:	5.9		
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N		

Description:

OpenSSL is prone to a carry propagation vulnerability. There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701.

Solution:

VendorFix Update to version 1.1.1m, 3.0.1 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.1.1m Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20220128.txt

Unique Alert ID: 919566 Found on: 2023-10-06 Severity: Medium

OpenBSD OpenSSH Information Disclosure Vulnerability (CVE-2020-14145) (tcp/22)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2020-14145		
Cvss Base:	5.9		
Cvss Score:	5.9		
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N		

Description:

OpenBSD OpenSSH is prone to an information disclosure vulnerability. The client side in OpenSSH has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client).

Solution:

VendorFix Update to version 8.5 or later.

Result:

Installed version: 6.6.1 Fixed version: 8.5 Installation path / port: 22/tcp

References:

- http://www.openwall.com/lists/oss-security/2020/12/02/1

Unique Alert ID: 539285 Found on: 2023-10-06 Severity: Medium

OpenSSL: Timing vulnerability in DSA signature generation (CVE-2018-0734) (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-0734
Cvss Base: 5.9
Cvss Score: 5.9
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

OpenSSL is prone to an information disclosure vulnerability. The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the privat e key.

Solution:

VendorFix Upgrade OpenSSL to version 1.1.0j-dev, 1.1.1a-dev, 1.0.2q-dev or manually apply the fixes via Github. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2q-dev Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20181030.txt,https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=43e6a58d4991a451daf4891ff05a48735df871ac,https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=8abfe72e8c1de1b95f50aa0d9134803b4d00070f,https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=ef11e19d1365eea2b1851e6f540a0bf365d303e7

Unique Alert ID: 607314 Found on: 2023-10-06 Severity: Medium

OpenSSL: Timing vulnerability in DSA signature generation (CVE-2018-0734) (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-12-18
CVE ID: CVE-2018-0734
Cvss Base: 5.9
Cvss Score: 5.9
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

OpenSSL is prone to an information disclosure vulnerability. The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the privat e key.

Solution:

VendorFix Upgrade OpenSSL to version 1.1.0j-dev, 1.1.1a-dev, 1.0.2q-dev or manually apply the fixes via Github. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2q-dev Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20181030.txt,https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=43e6a58d4991a451daf4891ff05a48735df871ac,https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=8abfe72e8c1de1b95f50aa0d9134803b4d00070f,https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=ef11e19d1365eea2b1851e6f540a0bf365d303e7

Unique Alert ID: 607312 Found on: 2023-10-06 Severity: Medium

OpenSSL Overflow Vulnerability (20171207, 20180327) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-12-18
CVE ID:	CVE-2017-3738		
Cvss Base:	5.9		
Cvss Score:	5.9		
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N		

Description:

OpenSSL is prone to an overflow bug. The overflow bug is in the AVX2 Montgomery multiplication procedure used in expo nentiation with 1024-bit moduli. Successfully exploiting this issue would allow an attacker to derive information about the private key.

Solution:

VendorFix Update to version 1.0.2n, 1.1.0h or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2n Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20171207.txt,https://www.openssl.org/news/secadv/20180327.txt

Unique Alert ID: 919567 Found on: 2023-10-06 Severity: Medium

OpenBSD OpenSSH <= 7.9 Multiple Vulnerabilities (tcp/22)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2018-20685,CVE-2019-6109,CVE-2019-6110,CVE-2019-6111		
Cvss Base:	5.9		
Cvss Score:	5.9		
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N		

Description:

OpenBSD OpenSSH is prone to multiple vulnerabilities. The following flaws exist: - CVE-2018-20685: bypass of intended access restrictions in the scp client - CVE-2019-6109, CVE-2019-6110: manipulation of the output in the scp client by a m alicious server - CVE-2019-6111: overwrite of arbitrary files in the scp client by a malicious server

Solution:

VendorFix Update to version 8.0 or later.

Result:

Installed version: 6.6.1 Fixed version: 8.0 Installation path / port: 22/tcp

References:

- https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt,http://www.openwall.com/lists/oss-security/2019/04/18/1

Unique Alert ID: 539297 Found on: 2023-10-06 Severity: Medium

OpenSSL Security Bypass Vulnerability - DEC 2017 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2017-3737		
Cvss Base:	5.9		
Cvss Score:	5.9		
Cvss Vector:	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N		

Description:

OpenSSL is prone to a security bypass vulnerability. When SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. Successfully exploiting this issue will allow attackers to bypass security restrictions and perform unauthorized actions. This may aid in launching further attacks.

Solution:

VendorFix OpenSSL 1.0.2 users should upgrade to 1.0.2n.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2n Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20171207.txt

Unique Alert ID: 919564 Found on: 2023-10-06 Severity: Medium

OpenSSL: EDIPARTYNAME NULL Pointer De-reference Vulnerability (CVE-2020-1971) (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2020-1971		
Cvss Base:	5.9		
Cvss Score:	5.9		
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H		

Description:

OpenSSL is prone to a Denial-of-Service (DoS) vulnerability. The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the '-crl_download' option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. An attacker may trigger a crash and cause a DoS.

Solution:

VendorFix OpenSSL 1.1.1 users should upgrade to 1.1.1i. OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2x. Other users should upgrade to OpenSSL 1.1.1i.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2x / 1.1.1i Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20201208.txt

Unique Alert ID: 919563 Found on: 2023-10-06 Severity: Medium

OpenSSL: EDIPARTYNAME NULL Pointer De-reference Vulnerability (CVE-2020-1971) (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2020-1971

Cvss Base: 5.9
Cvss Score: 5.9
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

Description:

OpenSSL is prone to a Denial-of-Service (DoS) vulnerability. The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the '-crl_download' option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. An attacker may trigger a crash and cause a DoS.

Solution:

VendorFix OpenSSL 1.1.1 users should upgrade to 1.1.1i. OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2x. Other users should upgrade to OpenSSL 1.1.1i.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2x / 1.1.1i Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20201208.txt

Unique Alert ID: 539301 Found on: 2023-10-06 Severity: Medium

OpenSSL Overflow Vulnerability (20171207, 20180327) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2017-3738
Cvss Base: 5.9
Cvss Score: 5.9
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

Description:

OpenSSL is prone to an overflow bug. The overflow bug is in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. Successfully exploiting this issue would allow an attacker to derive information about the private key.

Solution:

VendorFix Update to version 1.0.2n, 1.1.0h or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2n Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20171207.txt,https://www.openssl.org/news/secadv/20180327.txt

Unique Alert ID: 539214 Found on: 2023-10-06 Severity: Medium

PHP < 7.2.29 Multiple Vulnerabilities - Mar20 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2020-7064,CVE-2020-7066	
Cvss Base:	4.3	
Cvss Score:	4.3	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N	

Description:

PHP is prone to multiple vulnerabilities. PHP is prone to multiple vulnerabilities: - Use-of-uninitialized-value in exif (CVE-2020-7064) - get_headers() silently truncates after a null byte (CVE-2020-7066)

Solution:

VendorFix Update to version 7.2.29 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.29 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.29

Unique Alert ID: 539212 Found on: 2023-10-06 Severity: Medium

PHP < 7.2.29 Multiple Vulnerabilities - Mar20 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2020-7064,CVE-2020-7066	
Cvss Base:	4.3	
Cvss Score:	4.3	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N	

Description:

PHP is prone to multiple vulnerabilities. PHP is prone to multiple vulnerabilities: - Use-of-uninitialized-value in exif (CVE-2020-7064) - get_headers() silently truncates after a null byte (CVE-2020-7066)

Solution:

VendorFix Update to version 7.2.29 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.29 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.29

Unique Alert ID: 919569 Found on: 2023-10-06 Severity: Medium

OpenSSH Information Disclosure Vulnerability (CVE-2016-20012) (tcp/22)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2016-20012		
Cvss Base:	5.3		
Cvss Score:	5.3		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		

Description:

OpenBSD OpenSSH is prone to an information disclosure vulnerability. OpenSSH allows remote attackers, who have a su spicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion i s correct. This occurs because a challenge is sent only when that combination could be valid for a login session.

Solution:

WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Result:

Installed version: 6.6.1 Fixed version: None Installation path / port: 22/tcp

References:

- https://github.com/openssh/openssh-portable/pull/270,https://rushter.com/blog/public-ssh-keys/,https://utcc.utoronto.ca/~cks/space/blog/tech/SSHKeysAreInfoLeak

Unique Alert ID: 539235 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2019-0220		
Cvss Base:	5.3		
Cvss Score:	5.3		
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		

Description:

When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch a nd RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will impli citly collapse them.

Solution:

VendorFix Update to version 2.4.39 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.39 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539272 Found on: 2023-10-06 Severity: Medium

OpenSSH < 7.8 User Enumeration Vulnerability - Linux (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-15473

Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Description:

OpenSSH is prone to a user enumeration vulnerability. The flaw is due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and a uth2-pubkey.c Successfully exploitation will allow remote attacker to test whether a certain user exists or not (username enumeration) on a target OpenSSH server.

Solution:

VendorFix Update to version 7.8 or later.

Result:

Installed version: 6.6.1 Fixed version: 7.8 Installation path / port: 22/tcp

References:

- https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d1e0

Unique Alert ID: 539273 Found on: 2023-10-06 Severity: Medium

OpenSSH 'sftp-server' Security Bypass Vulnerability (Linux) (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2017-15906
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description:

openssh is prone to a security bypass vulnerability. The flaw exists in the 'process_open' function in sftp-server.c script w hich does not properly prevent write operations in readonly mode. Successfully exploiting this issue allows local users to bypass certain security restrictions and perform unauthorized actions. This may lead to further attacks.

Solution:

VendorFix Upgrade to OpenSSH version 7.6 or later.

Result:

Installed version: 6.6.1 Fixed version: 7.6 Installation path / port: 22/tcp

References:

- https://www.openssh.com/txt/release-7.6,https://github.com/openbsd/src/commit/a6981567e8e

Unique Alert ID: 919568 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 2.4.6 - 2.4.46 Tunneling Misconfiguration Vulnerability - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2019-17567
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description:

Apache HTTP Server is prone to a tunneling misconfiguration vulnerability. mod_proxy_wstunnel configured on an URL th at is not necessarily upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subs equent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

Solution:

VendorFix Update to version 2.4.48 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.48 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539237 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server < 2.4.39 URL Normalization Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2019-0220
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Description:

When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch a nd RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will impli citly collapse them.

Solution:

VendorFix Update to version 2.4.39 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.39 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539274 Found on: 2023-10-06 Severity: Medium

OpenSSH 'auth2-gss.c' User Enumeration Vulnerability - Linux (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18

CVE ID: CVE-2018-15919
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Description:

OpenSSH is prone to a user enumeration vulnerability. The flaw exists in the 'auth-gss2.c' source code file of the affected software and is due to insufficient validation of an authentication request packet when the Guide Star Server II (GSS2) c omponent is used on an affected system. Successfully exploitation will allow a remote attacker to harvest valid user acco unts, which may aid in brute-force attacks.

Solution:

WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Result:

Installed version: 6.6.1 Fixed version: None Installation path / port: 22/tcp

References:

- https://bugzilla.novell.com/show_bug.cgi?id=1106163,https://seclists.org/oss-sec/2018/q3/180

Unique Alert ID: 607308 Found on: 2023-10-06 Severity: Medium

OpenSSL Multiple Vulnerabilities - Nov 2017 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-12-18
CVE ID: CVE-2017-3735,CVE-2017-3736
Cvss Base: 6.5
Cvss Score: 6.5
Cvss Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

Description:

OpenSSL is prone to multiple vulnerabilities. Multiple flaws exist due to: - A carry propagating bug in the x86_64 Montgo mery squaring procedure. - Malformed X.509 IPAddressFamily which could cause OOB read. Successful exploitation will a llow a remote attacker to recover keys (private or secret keys) or to cause a buffer overread which lead to erroneous dis play of the certificate in text format.

Solution:

VendorFix Upgrade to OpenSSL version 1.1.0g or 1.0.2m or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2m Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20171102.txt

Unique Alert ID: 919573 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 2.4.6 - 2.4.46 Tunneling Misconfiguration Vulnerability - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2019-17567
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description:

Apache HTTP Server is prone to a tunneling misconfiguration vulnerability. mod_proxy_wstunnel configured on an URL th at is not necessarily upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subs equent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

Solution:

VendorFix Update to version 2.4.48 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.48 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539264 Found on: 2023-10-06 Severity: Medium

PHP < 7.2.28 Multiple Vulnerabilities - Feb20 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2020-7062,CVE-2020-7063
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description:

PHP is prone to multiple vulnerabilities. PHP is prone to multiple vulnerabilities: - Null Pointer Dereference in PHP Session Upload Progress (CVE-2020-7062) - Files added to tar with Phar::buildFromIterator have all-access permissions (CVE-20 20-7063)

Solution:

VendorFix Update to version 7.2.28 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.28 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.28

Unique Alert ID: 539263 Found on: 2023-10-06 Severity: Medium

PHP < 7.2.28 Multiple Vulnerabilities - Feb20 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2020-7062,CVE-2020-7063		
Cvss Base:	5.3		
Cvss Score:	5.3		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N		

Description:

PHP is prone to multiple vulnerabilities. PHP is prone to multiple vulnerabilities: - Null Pointer Dereference in PHP Session Upload Progress (CVE-2020-7062) - Files added to tar with Phar::buildFromIterator have all-access permissions (CVE-2020-7063)

Solution:

VendorFix Update to version 7.2.28 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.28 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.28

Unique Alert ID: 919571 Found on: 2023-10-06 Severity: Medium

OpenSSL Information Disclosure Vulnerability (20191206) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2019-1551		
Cvss Base:	5.3		
Cvss Score:	5.3		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		

Description:

OpenSSL is prone to an information disclosure vulnerability. There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME.

Solution:

VendorFix Update to version 1.0.2u, 1.1.1e or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2u Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20191206.txt

Unique Alert ID: 539261 Found on: 2023-10-06 Severity: Medium

PHP < 7.2.31, 7.3 < 7.3.18, 7.4 < 7.4.6 Multiple DoS Vulnerabilities - May20 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2019-11048
Cvss Base: 5.3
Cvss Score: 5.3

Description:

PHP is prone to two Denial-of-Service vulnerabilities. The following flaws exist: - Long filenames cause OOM and temp file s to not be cleaned - Long variables in multipart/form-data cause OOM and temp files are not cleaned leading to a Denial -of-Service condition (CVE-2019-11048).

Solution:

VendorFix Update to version 7.2.31, 7.3.18, 7.4.6 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.31 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.31,https://www.php.net/ChangeLog-7.php#7.3.18,https://www.php.net/ChangeLog-7.php#7.4.6,https://bugs.php.net/bug.php?id=78875,https://bugs.php.net/bug.php?id=78876

Unique Alert ID: 539259 Found on: 2023-10-06 Severity: Medium

PHP < 7.2.31, 7.3 < 7.3.18, 7.4 < 7.4.6 Multiple DoS Vulnerabilities - May20 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2019-11048
Cvss Base: 5.3
Cvss Score: 5.3

Description:

PHP is prone to two Denial-of-Service vulnerabilities. The following flaws exist: - Long filenames cause OOM and temp file s to not be cleaned - Long variables in multipart/form-data cause OOM and temp files are not cleaned leading to a Denial -of-Service condition (CVE-2019-11048).

Solution:

VendorFix Update to version 7.2.31, 7.3.18, 7.4.6 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.31 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.31,https://www.php.net/ChangeLog-7.php#7.3.18,https://www.php.net/ChangeLog-7.php#7.4.6,https://bugs.php.net/bug.php?id=78875,https://bugs.php.net/bug.php?id=78876

Unique Alert ID: 919574 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.26, 7.4.x < 7.4.14, 8.0.x < 8.0.1 Filter Vulnerability (Jan 2021) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2020-7071
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description:

PHP is prone to a vulnerability where FILTER_VALIDATE_URL accepts URLs with invalid userinfo.

Solution:

VendorFix Update to version 7.3.26, 7.4.14, 8.0.1 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.26 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.26,https://www.php.net/ChangeLog-7.php#7.4.14,https://www.php.net/ChangeLog-8.php#8.0.1

Unique Alert ID: 919575 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.26, 7.4.x < 7.4.14, 8.0.x < 8.0.1 Filter Vulnerability (Jan 2021) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2020-7071
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description:

PHP is prone to a vulnerability where FILTER_VALIDATE_URL accepts URLs with invalid userinfo.

Solution:

VendorFix Update to version 7.3.26, 7.4.14, 8.0.1 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.26 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.26,https://www.php.net/ChangeLog-7.php#7.4.14,https://www.php.net/ChangeLog-8.php#8.0.1

Unique Alert ID: 919576 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.29 Multiple Vulnerabilities (Jul 2021) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-21704,CVE-2021-21705
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - CVE-2021-21705: SSRF bypass in FILTER_VALIDATE_URL. - CVE-2021-21704: Stack buffer overflow in firebird_info_cb. - CVE-2021-21704: SIGSEGV in firebird_handle_doer. - CVE-2021-21704: SIGSEGV in firebird_stmt_execute. - CVE-2021-21704: Crash while parsing blob data in firebird_fetch_blob.

Solution:

VendorFix Update to version 7.3.29 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.29 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.29,http://bugs.php.net/81122,http://bugs.php.net/76448,http://bugs.php.net/76449,http://bugs.php.net/76450,http://bugs.php.net/76452

Unique Alert ID: 919577 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.29 Multiple Vulnerabilities (Jul 2021) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2021-21704,CVE-2021-21705
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description:

PHP is prone to multiple vulnerabilities. The following flaws exist: - CVE-2021-21705: SSRF bypass in FILTER_VALIDATE_URL. - CVE-2021-21704: Stack buffer overflow in firebird_info_cb. - CVE-2021-21704: SIGSEGV in firebird_handle_doer. - CVE-2021-21704: SIGSEGV in firebird_stmt_execute. - CVE-2021-21704: Crash while parsing blob data in firebird_fetch_blob.

Solution:

VendorFix Update to version 7.3.29 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.29 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.29,http://bugs.php.net/81122,http://bugs.php.net/76448,http://bugs.php.net/76449,http://bugs.php.net/76450,http://bugs.php.net/76452

Unique Alert ID: 539265 Found on: 2023-10-06 Severity: Medium

OpenSSL 'OOB read' Security Bypass Vulnerability (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2017-3735	
Cvss Base:	5.3	
Cvss Score:	5.3	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	

Description:

OpenSSL is prone to an 'OOB read' security bypass vulnerability. The flaw exists as OpenSSL could do a one-byte buffer overread if an X.509 certificate has a malformed IPAddressFamily extension. Successfully exploiting this issue will allow a ttackers to bypass security restrictions and perform unauthorized actions, this may aid in launching further attacks.

Solution:

VendorFix Upgrade to OpenSSL version 1.1.0g-dev or 1.0.2m-dev or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2m-dev Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20170828.txt,https://www.openssl.org/news/vulnerabilities.html#y2017

Unique Alert ID: 607307 Found on: 2023-10-06 Severity: Medium

OpenSSL 'OOB read' Security Bypass Vulnerability (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2020-12-18
CVE ID:	CVE-2017-3735	
Cvss Base:	5.3	
Cvss Score:	5.3	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	

Description:

OpenSSL is prone to an 'OOB read' security bypass vulnerability. The flaw exists as OpenSSL could do a one-byte buffer overread if an X.509 certificate has a malformed IPAddressFamily extension. Successfully exploiting this issue will allow a ttackers to bypass security restrictions and perform unauthorized actions, this may aid in launching further attacks.

Solution:

VendorFix Upgrade to OpenSSL version 1.1.0g-dev or 1.0.2m-dev or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2m-dev Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20170828.txt,https://www.openssl.org/news/vulnerabilities.html#y2017

Unique Alert ID: 919578 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.33, 7.4.x < 7.4.26, 8.0.x < 8.0.13 Security Update (Nov 2021) - Linux (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2021-21707	
Cvss Base:	5.3	
Cvss Score:	5.3	

Description:

PHP released new versions which include a security fix. Fixed bug #79971 (special character is breaking the path in xml f unction).

Solution:

VendorFix Update to version 7.3.33, 7.4.26, 8.0.13 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.33 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.33,https://www.php.net/ChangeLog-7.php#7.4.26,https://www.php.net/ChangeLog-8.php#8.0.13,http://bugs.php.net/79971

Unique Alert ID: 919579 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.33, 7.4.x < 7.4.26, 8.0.x < 8.0.13 Security Update (Nov 2021) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2021-21707	
Cvss Base:	5.3	
Cvss Score:	5.3	

Description:

PHP released new versions which include a security fix. Fixed bug #79971 (special character is breaking the path in xml f unction).

Solution:

VendorFix Update to version 7.3.33, 7.4.26, 8.0.13 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.33 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.33,https://www.php.net/ChangeLog-7.php#7.4.26,https://www.php.net/ChangeLog-8.php#8.0.13,http://bugs.php.net/79971

Unique Alert ID: 919572 Found on: 2023-10-06 Severity: Medium

OpenSSL Information Disclosure Vulnerability (20191206) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2019-1551	
Cvss Base:	5.3	
Cvss Score:	5.3	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	

Description:

OpenSSL is prone to an information disclosure vulnerability. There is an overflow bug in the x64_64 Montgomery squarin g procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks ag ainst 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN _mod_exp may be affected if they use BN_FLG_CONSTTIME.

Solution:

VendorFix Update to version 1.0.2u, 1.1.1e or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2u Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20191206.txt

Unique Alert ID: 539270 Found on: 2023-10-06 Severity: Medium

OpenSSL Multiple Vulnerabilities - Nov 2017 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2017-3735,CVE-2017-3736	
Cvss Base:	6.5	
Cvss Score:	6.5	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	

Description:

OpenSSL is prone to multiple vulnerabilities. Multiple flaws exist due to: - A carry propagating bug in the x86_64 Montgo mery squaring procedure. - Malformed X.509 IPAddressFamily which could cause OOB read. Successful exploitation will a llow a remote attacker to recover keys (private or secret keys) or to cause a buffer overread which lead to erroneous dis play of the certificate in text format.

Solution:

VendorFix Upgrade to OpenSSL version 1.1.0g or 1.0.2m or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2m Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20171102.txt

Unique Alert ID: 539283 Found on: 2023-10-06 Severity: Medium

OpenSSH Denial of Service Vulnerability - Jan16 (tcp/22)

Open Status:	Re-OPEN	**First Found:** 2020-11-18
CVE ID:	CVE-2016-1907	
Cvss Base:	5.3	
Cvss Score:	5.3	
Cvss Vector:	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	

Description:

openssh is prone to a denial of service (DoS) vulnerability. The flaw exists due to an error in 'ssh_packet_read_poll2' fun ction within 'packet.c' script. Successfully exploiting this issue allow remote attackers to cause a denial of service (out-of-bounds read and application crash).

Solution:

VendorFix Upgrade to OpenSSH version 7.1p2 or later.

Result:

Installed version: 6.6.1 Fixed version: 7.1p2 Installation path / port: 22/tcp

References:

- http://www.openssh.com/txt/release-7.1p2,https://anongit.mindrot.org/openssh.git/commit/?id=2fecfd486bdba9f51b3a789277bb0733ca36e1c0

Unique Alert ID: 919570 Found on: 2023-10-06 Severity: Medium

Weak Key Exchange (KEX) Algorithm(s) Supported (SSH) (tcp/22)

Open Status: Re-OPEN **First Found:** 2022-05-17
Cvss Base: 5.3
Cvss Score: 5.3

Description:

The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s). - 1024-bit MODP group / prime KEX algorithms: Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key e xchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connecti on. However, the first step in the number field sieve-the most efficient algorithm for breaking a Diffie-Hellman connection -is dependent only on this prime. A nation-state can break a 1024-bit prime. An attacker can quickly break individual con nections.

Solution:

Mitigation Disable the reported weak KEX algorithm(s) - 1024-bit MODP group / prime KEX algorithms: Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Result:

The remote SSH server supports the following weak KEX algorithm(s): KEX algorithm | Reason ---------- ---------- diffie-hellman-group-exchange-sha1 | Using SHA-1 diffie-hellman-group1-sha1 | Using Oakley Group 2 (a 1024-bit MODP group) and SHA-1

References:

- https://weakdh.org/sysadmin.html,https://www.rfc-editor.org/rfc/rfc9142.html,https://www.rfc-editor.org/rfc/rfc914 2.html#name-summary-guidance-for-implem,https://datatracker.ietf.org/doc/html/rfc6194

Unique Alert ID: 539293 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 2.4.1 < 2.4.24 IP Spoofing Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2020-11985
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description:

Apache HTTP Server is prone to an IP address spoofing vulnerability when proxying using mod_remoteip and mod_rewrit e.

Solution:

VendorFix Update to version 2.4.24 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.24 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539304 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 2.4.1 < 2.4.24 IP Spoofing Vulnerability (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2020-11985
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Description:

Apache HTTP Server is prone to an IP address spoofing vulnerability when proxying using mod_remoteip and mod_rewrite.

Solution:

VendorFix Update to version 2.4.24 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.24 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539217 Found on: 2023-10-06 Severity: Medium

PHP 'php_parserr' Heap Based Buffer Overflow Vulnerability (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-4049
Cvss Base: 5.1
Cvss Score: 5.1

Description:

PHP is prone to a heap-based buffer overflow vulnerability. The flaw is due to buffer overflow error in the 'php_parserr' function in ext/standard/dns.c script. Successfully exploiting this issue allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code on the affected system.

Solution:

VendorFix Update to PHP version 5.6.0 or 5.5.14 or 5.4.30 or 5.3.29 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.30

References:

- http://php.net/ChangeLog-5.php,http://www.openwall.com/lists/oss-security/2014/06/13/4

Unique Alert ID: 539219 Found on: 2023-10-06 Severity: Medium

PHP 'php_parserr' Heap Based Buffer Overflow Vulnerability (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-4049
Cvss Base: 5.1
Cvss Score: 5.1

Description:

PHP is prone to a heap-based buffer overflow vulnerability. The flaw is due to buffer overflow error in the 'php_parserr' f

unction in ext/standard/dns.c script. Successfully exploiting this issue allows remote attackers to cause a denial of servic e (crash) and possibly execute arbitrary code on the affected system.

Solution:

VendorFix Update to PHP version 5.6.0 or 5.5.14 or 5.4.30 or 5.3.29 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.30

References:

- http://php.net/ChangeLog-5.php,http://www.openwall.com/lists/oss-security/2014/06/13/4

Unique Alert ID: 539269 Found on: 2023-10-06 Severity: Medium

SSL/TLS: Certificate Expired (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 5.0
Cvss Score: 5.0

Description:

The remote server's SSL/TLS certificate has already expired. This script checks expiry dates of certificates associated wit h SSL/TLS-enabled services on the target and reports whether any have already expired.

Solution:

Mitigation Replace the SSL/TLS certificate by a new one.

Result:

The certificate of the remote service expired on 2019-03-13 13:40:08. Certificate details: fingerprint (SHA-1) | 81C5AB98A9E8BECAEEB849E97EF47D7A14DCF936 fingerprint (SHA-256) | 635269291BDF6067EEDB2D40DB10B25C354D9FEA326F43779AE51D6C3FEB0FAB issued by | CN=Let's Encrypt Authority X3,O=Let's Encrypt,C=US public key algorithm | RSA public key size (bits) | 2048 serial | 0342FA98D61F9F34FD44E05EE95726E89BB3 signature algorithm | sha256WithRSAEncryption subject | CN=*.testapptrana.com subject alternative names (SAN) | *.testapptrana.com valid from | 2018-12-13 13:40:08 UTC valid until | 2019-03-13 13:40:08 UTC

Unique Alert ID: 539266 Found on: 2023-10-06 Severity: Medium

Missing 'HttpOnly' Cookie Attribute (HTTP) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 5.0
Cvss Score: 5.0

Description:

The remote HTTP web server / application is missing to set the 'HttpOnly' cookie attribute for one or more sent HTTP coo kie. The flaw exists if a session cookie is not using the 'HttpOnly' cookie attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Solution:

Mitigation Set the 'HttpOnly' attribute for any session cookie.

Result:

The cookies: Set-Cookie: PHPSESSID=***replaced***; path=/ Set-Cookie: PHPSESSID=***replaced***; path=/ Set-Cookie: security=low are missing the "HttpOnly" attribute.

References:

- https://www.rfc-editor.org/rfc/rfc6265#section-5.2.6,https://owasp.org/www-community/HttpOnly,https://wiki.owas p.org/index.php/Testing_for_cookies_attributes

Unique Alert ID: 919585 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server DoS Vulnerability (Sep 2014) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2014-3581
Cvss Base: 5.0
Cvss Score: 5.0

Description:

Apache HTTP Server is prone to a denial of service (DoS) vulnerability. A NULL pointer deference was found in mod_cach e. A malicious HTTP server could cause a crash in a caching forward proxy configuration. This crash would only be a deni al of service if using a threaded MPM.

Solution:

VendorFix Update to version 2.4.12 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.12 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 919584 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server DoS Vulnerability (Sep 2014) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2014-3581
Cvss Base: 5.0
Cvss Score: 5.0

Description:

Apache HTTP Server is prone to a denial of service (DoS) vulnerability. A NULL pointer deference was found in mod_cach e. A malicious HTTP server could cause a crash in a caching forward proxy configuration. This crash would only be a deni al of service if using a threaded MPM.

Solution:

VendorFix Update to version 2.4.12 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.12 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539252 Found on: 2023-10-06 Severity: Medium

PHP 'donate' function Denial of Service Vulnerability - Nov14 (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-3710
Cvss Base: 5.0
Cvss Score: 5.0

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to an out-of-bounds read error in the 'donote' func tion in readelf.c script. Successful exploitation will allow a local attacker to conduct a denial of service attack.

Solution:

VendorFix Update to PHP version 5.4.35 or 5.5.19 or 5.6.3 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.35/5.5.19/5.6.3

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=68283

Unique Alert ID: 539251 Found on: 2023-10-06 Severity: Medium

PHP 'donate' function Denial of Service Vulnerability - Nov14 (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-3710
Cvss Base: 5.0
Cvss Score: 5.0

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to an out-of-bounds read error in the 'donote' function in readelf.c script. Successful exploitation will allow a local attacker to conduct a denial of service attack.

Solution:

VendorFix Update to PHP version 5.4.35 or 5.5.19 or 5.6.3 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.35/5.5.19/5.6.3

References:

- http://php.net/ChangeLog-5.php,https://bugs.php.net/bug.php?id=68283

Unique Alert ID: 539244 Found on: 2023-10-06 Severity: Medium

PHP 'open_basedir' Security Bypass Vulnerability (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2012-1171
Cvss Base: 5.0
Cvss Score: 5.0

Description:

PHP is prone to a security bypass vulnerability. The flaw is in libxml RSHUTDOWN function which allows to bypass open_basedir protection mechanism through stream_close method call. Successful exploitation will allow remote attackers to read arbitrary files.

Solution:

WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Result:

Installed version: 5.4.16 Fixed version: N/A

References:

- https://bugzilla.redhat.com/show_bug.cgi?id=802591

Unique Alert ID: 539243 Found on: 2023-10-06 Severity: Medium

PHP 'open_basedir' Security Bypass Vulnerability (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2012-1171
Cvss Base: 5.0
Cvss Score: 5.0

Description:

PHP is prone to a security bypass vulnerability. The flaw is in libxml RSHUTDOWN function which allows to bypass open_basedir protection mechanism through stream_close method call. Successful exploitation will allow remote attackers to read arbitrary files.

Solution:

WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Result:

Installed version: 5.4.16 Fixed version: N/A

References:

- https://bugzilla.redhat.com/show_bug.cgi?id=802591

Unique Alert ID: 1533218 Found on: 2023-10-06 Severity: Medium

OpenSSL DoS Vulnerability (20230731) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2023-10-06
CVE ID: CVE-2023-3817
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Description:

OpenSSL is prone to a denial of service (DoS) vulnerability. Checking excessively long DH keys or parameters may be very slow. Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service.

Solution:

NoneAvailable No known solution is available as of 01st August, 2023. Information regarding this issue will be updated once solution details are available. Vendor info: Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available. The fix is also available in commit 6a1eb62c2 (for 3.1), commit 9002fd073 (for 3.0) and commit 91ddeba0f (for 1.1.1) in the OpenSSL git repository. It is available to premium support customer in commit 869ad69a (for 1.0.2).

Result:

Installed version: 1.0.2k Fixed version: None Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20230731.txt

Unique Alert ID: 1533219 Found on: 2023-10-06 Severity: Medium

OpenBSD OpenSSH < 9.3 Unspecified Vulnerability (tcp/22)

Open Status: Re-OPEN **First Found:** 2023-10-06
Cvss Base: 5.0
Cvss Score: 5.0

Description:

OpenBSD OpenSSH is prone to an unspecified vulnerability. ssh(1): Portable OpenSSH provides an implementation of the getrrsetbyname(3) function if the standard library does not provide it, for use by the VerifyHostKeyDNS feature. A specifi cally crafted DNS response could cause this function to perform an out-of-bounds read of adjacent stack data, but this co ndition does not appear to be exploitable beyond denial-of-service to the ssh(1) client. The getrrsetbyname(3) replaceme nt is only included if the system's standard library lacks this function and portable OpenSSH was not compiled with the ld ns library (--with-ldns). getrrsetbyname(3) is only invoked if using VerifyHostKeyDNS to fetch SSHFP records.This proble m was found by the Coverity static analyzer.

Solution:

VendorFix Update to version 9.3 or later.

Result:

Installed version: 6.6.1 Fixed version: 9.3 Installation path / port: 22/tcp

References:

- https://www.openssh.com/releasenotes.html#9.3,https://www.openwall.com/lists/oss-security/2023/03/15/8

Unique Alert ID: 1533220 Found on: 2023-10-06 Severity: Medium

OpenBSD OpenSSH < 9.2 Unspecified Vulnerability (tcp/22)

Open Status: Re-OPEN **First Found:** 2023-10-06
Cvss Base: 5.0
Cvss Score: 5.0

Description:

OpenBSD OpenSSH is prone to an unspecified vulnerability. If the CanonicalizeHostname and CanonicalizePermittedCNA MEs options were enabled, and the system/libc resolver did not check that names in DNS responses were valid, then use of these options could allow an attacker with control of DNS to include invalid characters (possibly including wildcards) in names added to known_hosts files when they were updated. These names would still have to match the CanonicalizePer mittedCNAMEs allow-list, so practical exploitation appears unlikely.

Solution:

VendorFix Update to version 9.2 or later.

Result:

Installed version: 6.6.1 Fixed version: 9.2 Installation path / port: 22/tcp

References:

- https://www.openssh.com/releasenotes.html#9.2,https://www.openwall.com/lists/oss-security/2023/02/02/3

Unique Alert ID: 919583 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.28, 7.4.x < 7.4.18 IMAP Header Injection Vulnerability (Apr 2021) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
Cvss Base: 5.0
Cvss Score: 5.0

Description:

PHP is prone to an IMAP header injection vulnerability.

Solution:

VendorFix Update to version 7.3.28, 7.4.18 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.28 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.28,https://www.php.net/ChangeLog-7.php#7.4.18

Unique Alert ID: 919581 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.28, 7.4.x < 7.4.18 IMAP Header Injection Vulnerability (Apr 2021) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
Cvss Base: 5.0
Cvss Score: 5.0

Description:

PHP is prone to an IMAP header injection vulnerability.

Solution:

VendorFix Update to version 7.3.28, 7.4.18 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.28 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.28,https://www.php.net/ChangeLog-7.php#7.4.18

Unique Alert ID: 919582 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.30, 7.4.x < 7.4.23, 8.0.x < 8.0.10 Security Update (Aug 2021) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
Cvss Base: 5.0
Cvss Score: 5.0

Description:

PHP released new versions which include security fixes.

Solution:

VendorFix Update to version 7.3.30, 7.4.23, 8.0.10 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.30 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.30,https://www.php.net/ChangeLog-7.php#7.4.23,https://www.php.net/ChangeLog-8.php#8.0.10

Unique Alert ID: 919580 Found on: 2023-10-06 Severity: Medium

PHP < 7.3.30, 7.4.x < 7.4.23, 8.0.x < 8.0.10 Security Update (Aug 2021) - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
Cvss Base: 5.0
Cvss Score: 5.0

Description:

PHP released new versions which include security fixes.

Solution:

VendorFix Update to version 7.3.30, 7.4.23, 8.0.10 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.3.30 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.3.30,https://www.php.net/ChangeLog-7.php#7.4.23,https://www.php.net/ChangeLog-8.php#8.0.10

Unique Alert ID: 1533221 Found on: 2023-10-06 Severity: Medium

OpenSSL DoS Vulnerability (20230731) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2023-10-06
CVE ID: CVE-2023-3817
Cvss Base: 5.3
Cvss Score: 5.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Description:

OpenSSL is prone to a denial of service (DoS) vulnerability. Checking excessively long DH keys or parameters may be very slow. Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service.

Solution:

NoneAvailable No known solution is available as of 01st August, 2023. Information regarding this issue will be updated once solution details are available. Vendor info: Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available. The fix is also available in commit 6a1eb62c2 (for 3.1), commit 9002fd073 (for 3.0) and commit 91ddeba0f (for 1.1.1) in the OpenSSL git repository. It is available to premium support customer in commit 869ad69a (for 1.0.2).

Result:

Installed version: 1.0.2k Fixed version: None Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20230731.txt

Unique Alert ID: 1533224 Found on: 2023-10-06 Severity: Medium

PHP < 8.0.29, 8.1.x < 8.1.20, 8.2.x < 8.2.7 Security Update - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2023-10-06
CVE ID: CVE-2023-3247
Cvss Base: 4.3
Cvss Score: 4.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

Description:

PHP is prone to a missing error check and insufficient random bytes in HTTP Digest authentication for SOAP vulnerability.

Solution:

VendorFix Update to version 8.0.29, 8.1.10, 8.2.7 or later.

Result:

Installed version: 5.4.16 Fixed version: 8.0.29 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-8.php#8.0.29,https://www.php.net/ChangeLog-8.php#8.1.20,https://www.php.net/ChangeLog-8.php#8.2.7,https://github.com/php/php-src/security/advisories/GHSA-76gg-c692-v2mw

Unique Alert ID: 1533225 Found on: 2023-10-06 Severity: Medium

PHP < 8.0.29, 8.1.x < 8.1.20, 8.2.x < 8.2.7 Security Update - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2023-10-06
CVE ID: CVE-2023-3247
Cvss Base: 4.3
Cvss Score: 4.3
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

Description:

PHP is prone to a missing error check and insufficient random bytes in HTTP Digest authentication for SOAP vulnerability.

Solution:

VendorFix Update to version 8.0.29, 8.1.10, 8.2.7 or later.

Result:

Installed version: 5.4.16 Fixed version: 8.0.29 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-8.php#8.0.29,https://www.php.net/ChangeLog-8.php#8.1.20,https://www.php.net/ChangeLog-8.php#8.2.7,https://github.com/php/php-src/security/advisories/GHSA-76gg-c692-v2mw

Unique Alert ID: 539258 Found on: 2023-10-06 Severity: Medium

PHP CDF File Parsing Denial of Service Vulnerabilities - 01 - Jun14 (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-0237,CVE-2014-0238
Cvss Base: 5.0
Cvss Score: 5.0

Description:

PHP is prone to multiple denial of service vulnerabilities. The flaw is due to - An error due to an infinite loop within the 'unpack_summary_info' function in src/cdf.c script. - An error within the 'cdf_read_property_info' function in src/cdf.c script. Successful exploitation will allow remote attackers to conduct denial of service attacks.

Solution:

VendorFix Update to PHP version 5.4.29 or 5.5.13 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.29/5.5.13

References:

- http://www.php.net/ChangeLog-5.php,http://secunia.com/advisories/58804,https://www.hkcert.org/my_url/en/alert/14060401

Unique Alert ID: 539257 Found on: 2023-10-06 Severity: Medium

PHP CDF File Parsing Denial of Service Vulnerabilities - 01 - Jun14 (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2014-0237,CVE-2014-0238		
Cvss Base:	5.0		
Cvss Score:	5.0		

Description:

PHP is prone to multiple denial of service vulnerabilities. The flaw is due to - An error due to an infinite loop within the 'unpack_summary_info' function in src/cdf.c script. - An error within the 'cdf_read_property_info' function in src/cdf.c script. Successful exploitation will allow remote attackers to conduct denial of service attacks.

Solution:

VendorFix Update to PHP version 5.4.29 or 5.5.13 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.29/5.5.13

References:

- http://www.php.net/ChangeLog-5.php,http://secunia.com/advisories/58804,https://www.hkcert.org/my_url/en/alert/14060401

Unique Alert ID: 1533226 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server < 2.4.55 Multiple Vulnerabilities (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2023-10-06
CVE ID:	CVE-2006-20001,CVE-2022-36760,CVE-2022-37436	
Cvss Base:	5.3	
Cvss Score:	5.3	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2006-20001: mod_dav out of bounds read, or write of zero byte - CVE-2022-36760: Possible request smuggling in mod_proxy_ajp - CVE-2022-37436: mod_proxy allows a backend to trigger HTTP response splitting

Solution:

VendorFix Update to version 2.4.55 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.55 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 1533227 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server < 2.4.55 Multiple Vulnerabilities (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2023-10-06
CVE ID:	CVE-2006-20001,CVE-2022-36760,CVE-2022-37436	
Cvss Base:	5.3	
Cvss Score:	5.3	
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2006-20001: mod_dav out of bounds read, or write of zero byte - CVE-2022-36760: Possible request smuggling in mod_proxy_ajp - CVE-2022-37436: mod_proxy allows a backend to trigger HTTP response splitting

Solution:

VendorFix Update to version 2.4.55 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.55 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539230 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 'mod_lua' Denial of Service Vulnerability -01 May15 (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18

CVE ID: CVE-2015-0228
Cvss Base: 5.0
Cvss Score: 5.0

Description:

Apache HTTP Server is prone to a denial of service vulnerability. Flaw is due to vulnerability in lua_websocket_read functi on in lua_request.c in the mod_lua module. Successful exploitation will allow a remote attacker to cause a denial of servi ce via some crafted dimension.

Solution:

VendorFix Update to version 2.4.13 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.13 Installation path / port: 443/tcp

References:

- https://bugs.mageia.org/show_bug.cgi?id=15428,http://svn.apache.org/repos/asf/httpd/httpd/branches/2.4.x/CHAN GES

Unique Alert ID: 539228 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server Multiple Vulnerabilities August15 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-3185,CVE-2015-3183
Cvss Base: 5.0
Cvss Score: 5.0

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Multiple flaws are due to: - an error in 'ap_some_auth_required' function in 'server/request.c' script which does not consider that a Require directive may be associated with an authorizat ion setting rather than an authentication setting. - an error in chunked transfer coding implementation. Successful exploit ation will allow remote attackers to bypass intended access restrictions in opportunistic circumstances and to cause cache poisoning or credential hijacking if an intermediary proxy is in use.

Solution:

VendorFix Update to version 2.4.14 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.14 Installation path / port: 443/tcp

References:

- http://www.apache.org/dist/httpd/CHANGES_2.4,http://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539229 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server Multiple Vulnerabilities August15 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-3185,CVE-2015-3183
Cvss Base: 5.0
Cvss Score: 5.0

Description:

Apache HTTP Server is prone to multiple vulnerabilities. Multiple flaws are due to: - an error in 'ap_some_auth_required' function in 'server/request.c' script which does not consider that a Require directive may be associated with an authorizat ion setting rather than an authentication setting. - an error in chunked transfer coding implementation. Successful exploit ation will allow remote attackers to bypass intended access restrictions in opportunistic circumstances and to cause cache poisoning or credential hijacking if an intermediary proxy is in use.

Solution:

VendorFix Update to version 2.4.14 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.14 Installation path / port: 80/tcp

References:

- http://www.apache.org/dist/httpd/CHANGES_2.4,http://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 656889 Found on: 2023-10-06 Severity: Medium

SSL/TLS: Certificate In Chain Expired (tcp/443)

Open Status: Re-OPEN **First Found:** 2021-03-18
Cvss Base: 5.0
Cvss Score: 5.0

Description:

The remote service is using a SSL/TLS certificate chain where one or multiple CA certificates have expired. Checks if the CA certificates in the SSL/TLS certificate chain have expired.

Solution:

Mitigation Sign your server certificate with a valid CA certificate.

Result:

The following certificates which are part of the certificate chain have expired: Subject: CN=Let's Encrypt Authority X3,O=Let's Encrypt,C=US Expired on: 2021-03-17 16:40:46

Unique Alert ID: 539231 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 'mod_lua' Denial of Service Vulnerability -01 May15 (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-0228
Cvss Base: 5.0
Cvss Score: 5.0

Description:

Apache HTTP Server is prone to a denial of service vulnerability. Flaw is due to vulnerability in lua_websocket_read functi on in lua_request.c in the mod_lua module. Successful exploitation will allow a remote attacker to cause a denial of servi ce via some crafted dimension.

Solution:

VendorFix Update to version 2.4.13 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.13 Installation path / port: 80/tcp

References:

- https://bugs.mageia.org/show_bug.cgi?id=15428,http://svn.apache.org/repos/asf/httpd/httpd/branches/2.4.x/CHAN GES

Unique Alert ID: 1533230 Found on: 2023-10-06 Severity: Medium

OpenSSL Multiple Vulnerabilities (20230322, 20230328, 20230530) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2023-10-06
CVE ID: CVE-2023-0464,CVE-2023-0465,CVE-2023-0466,CVE-2023-2650
Cvss Base: 6.5
Cvss Score: 6.5
Cvss Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Description:

OpenSSL is prone to multiple vulnerabilities. The following flaws exist: - CVE-2023-0464: Excessive Resource Usage Verif ying X.509 Policy Constraints - CVE-2023-0465: Invalid certificate policies in leaf certificates are silently ignored - CVE-2 023-0466: Certificate policy check not enabled - CVE-2023-2650: Possible DoS translating ASN.1 object identifiers

Solution:

VendorFix Update to version 1.0.2zh, 1.1.1u, 3.0.9, 3.1.1 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2zh Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20230322.txt,https://www.openssl.org/news/secadv/20230328.txt,https://ww w.openssl.org/news/secadv/20230530.txt

Unique Alert ID: 1533231 Found on: 2023-10-06 Severity: Medium

OpenSSL Multiple Vulnerabilities (20230322, 20230328, 20230530) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2023-10-06
CVE ID:	CVE-2023-0464,CVE-2023-0465,CVE-2023-0466,CVE-2023-2650		
Cvss Base:	6.5		
Cvss Score:	6.5		
Cvss Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H		

Description:

OpenSSL is prone to multiple vulnerabilities. The following flaws exist: - CVE-2023-0464: Excessive Resource Usage Verifying X.509 Policy Constraints - CVE-2023-0465: Invalid certificate policies in leaf certificates are silently ignored - CVE-2023-0466: Certificate policy check not enabled - CVE-2023-2650: Possible DoS translating ASN.1 object identifiers

Solution:

VendorFix Update to version 1.0.2zh, 1.1.1u, 3.0.9, 3.1.1 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2zh Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20230322.txt,https://www.openssl.org/news/secadv/20230328.txt,https://www.openssl.org/news/secadv/20230530.txt

Unique Alert ID: 919587 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server Multiple Vulnerabilities (Mar 2014) - Linux (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2013-6438,CVE-2014-0098		
Cvss Base:	5.0		
Cvss Score:	5.0		

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2013-6438: XML parsing code in mod_dav incorrectly calculates the end of the string when removing leading spaces and places a NUL character outside the buffer, causing random crashes. This XML parsing code is only used with DAV provider modules that support DeltaV, of which the only publicly released provider is mod_dav_svn. - CVE-2014-0098: A flaw was found in mod_log_config. A remote attacker could send a specific truncated cookie causing a crash. This crash would only be a denial of service if using a threaded MPM.

Solution:

VendorFix Update to version 2.2.27, 2.4.9 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.9 Installation path / port: 443/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_22.html,https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 919586 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server Multiple Vulnerabilities (Mar 2014) - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2013-6438,CVE-2014-0098
Cvss Base: 5.0
Cvss Score: 5.0

Description:

Apache HTTP Server is prone to multiple vulnerabilities. The following vulnerabilities exist: - CVE-2013-6438: XML parsing code in mod_dav incorrectly calculates the end of the string when removing leading spaces and places a NUL character outside the buffer, causing random crashes. This XML parsing code is only used with DAV provider modules that support DeltaV, of which the only publicly released provider is mod_dav_svn. - CVE-2014-0098: A flaw was found in mod_log_config. A remote attacker could send a specific truncated cookie causing a crash. This crash would only be a denial of service if using a threaded MPM.

Solution:

VendorFix Update to version 2.2.27, 2.4.9 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.9 Installation path / port: 80/tcp

References:

- https://httpd.apache.org/security/vulnerabilities_22.html,https://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539315 Found on: 2023-10-06 Severity: Medium

OpenSSL: Microarchitecture timing vulnerability in ECC scalar multiplication (CVE-2018-5407) (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2018-5407
Cvss Base: 4.7
Cvss Score: 4.7
Cvss Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

Description:

OpenSSL is prone to an information disclosure vulnerability. OpenSSL ECC scalar multiplication, used in e.g. ECDSA and ECDH, has been shown to be vulnerable to a microarchitecture timing side channel attack. An attacker with sufficient access to mount local timing attacks during ECDSA signature generation could recover the private key.

Solution:

VendorFix Upgrade OpenSSL to version 1.0.2q, 1.1.0i or later. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2q Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20181112.txt,https://www.openssl.org/news/vulnerabilities.html,https://github.com/openssl/openssl/commit/aab7c770353b1dc4ba045938c8fb446dd1c4531e,https://eprint.iacr.org/2018/1060.pdf,https://github.com/bbbrumley/portsmash,https://www.exploit-db.com/exploits/45785/

Unique Alert ID: 539314 Found on: 2023-10-06 Severity: Medium

PHP Security Bypass Vulnerability May18 (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2018-10545		
Cvss Base:	4.7		
Cvss Score:	4.7		
Cvss Vector:	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N		

Description:

PHP is prone to a security bypass vulnerability. The flaw exists as the dumpable FPM child processes allow bypassing opc ache access controls Successful exploitation will allow an attacker to bypass security restrictions and access sensitive con figuration data for other accounts directly in the PHP worker process's memory.

Solution:

VendorFix Update to version 7.2.4 or 7.0.29 or 5.6.35 or 7.1.16 or later. Please see the references for more information.

Result:

Installed version: 5.4.16 Fixed version: 5.6.35 Installation path / port: 443/tcp

References:

- http://www.php.net/ChangeLog-5.php#5.6.35,http://www.php.net/ChangeLog-7.php#7.0.29,http://www.php.net/Ch angeLog-7.php#7.1.16,http://www.php.net/ChangeLog-7.php#7.2.4

Unique Alert ID: 539316 Found on: 2023-10-06 Severity: Medium

PHP Security Bypass Vulnerability May18 (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2018-10545		
Cvss Base:	4.7		
Cvss Score:	4.7		
Cvss Vector:	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N		

Description:

PHP is prone to a security bypass vulnerability. The flaw exists as the dumpable FPM child processes allow bypassing opc ache access controls Successful exploitation will allow an attacker to bypass security restrictions and access sensitive con figuration data for other accounts directly in the PHP worker process's memory.

Solution:

VendorFix Update to version 7.2.4 or 7.0.29 or 5.6.35 or 7.1.16 or later. Please see the references for more information.

Result:

Installed version: 5.4.16 Fixed version: 5.6.35 Installation path / port: 80/tcp

References:

- http://www.php.net/ChangeLog-5.php#5.6.35,http://www.php.net/ChangeLog-7.php#7.0.29,http://www.php.net/Ch angeLog-7.php#7.1.16,http://www.php.net/ChangeLog-7.php#7.2.4

Unique Alert ID: 607315 Found on: 2023-10-06 Severity: Medium

OpenSSL: Microarchitecture timing vulnerability in ECC scalar multiplication (CVE-2018-5407) (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-12-18
CVE ID: CVE-2018-5407
Cvss Base: 4.7
Cvss Score: 4.7
Cvss Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

Description:

OpenSSL is prone to an information disclosure vulnerability. OpenSSL ECC scalar multiplication, used in e.g. ECDSA and ECDH, has been shown to be vulnerable to a microarchitecture timing side channel attack. An attacker with sufficient acc ess to mount local timing attacks during ECDSA signature generation could recover the private key.

Solution:

VendorFix Upgrade OpenSSL to version 1.0.2q, 1.1.0i or later. See the references for more details.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2q Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20181112.txt,https://www.openssl.org/news/vulnerabilities.html,https://github.com/openssl/openssl/commit/aab7c770353b1dc4ba045938c8fb446dd1c4531e,https://eprint.iacr.org/2018/1060.pdf,https://github.com/bbbrumley/portsmash,https://www.exploit-db.com/exploits/45785/

Unique Alert ID: 539292 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 'mod_lua' Denial of Service Vulnerability May15 (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-8109
Cvss Base: 4.3
Cvss Score: 4.3

Description:

Apache HTTP Server is prone to a denial of service vulnerability. Flaw is due to a vulnerability in LuaAuthzProvider that is triggered if a user-supplied LUA script is supplied more than once with different arguments. Successful exploitation will all ow a remote attacker to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Requir e directives.

Solution:

VendorFix Update to version 2.4.12 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.12 Installation path / port: 443/tcp

References:

- http://httpd.apache.org/security/vulnerabilities_24.html,http://www.rapid7.com/db/vulnerabilities/apache-httpd-cve-2014-8109

Unique Alert ID: 539305 Found on: 2023-10-06 Severity: Medium

PHP 'LibGD' Denial of Service Vulnerability (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-2497
Cvss Base: 4.3
Cvss Score: 4.3

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to a NULL pointer dereference error in 'gdImageCreateFromXpm' function within LibGD. Successful exploitation will allow remote attackers to conduct denial of service attacks.

Solution:

VendorFix Update to PHP version 5.4.32 or 5.5.16 or 5.6.0 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.32/5.5.16/5.6.0

References:

- https://bugs.php.net/bug.php?id=66901

Unique Alert ID: 539287 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 'mod_cache' Denial of Service Vulnerability -01 May15 (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-0117
Cvss Base: 4.3
Cvss Score: 4.3

Description:

Apache HTTP Server is prone to a denial of service vulnerability. Flaw is due to vulnerability in mod_proxy module in the Apache HTTP Server. Successful exploitation will allow a remote attacker to cause a denial of service via a crafted HTTP Connection header when a reverse proxy is enabled.

Solution:

VendorFix Update to version 2.4.10 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.10 Installation path / port: 80/tcp

References:

- http://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539286 Found on: 2023-10-06 Severity: Medium

OpenSSH Security Bypass Vulnerability (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2015-5352
Cvss Base: 4.3
Cvss Score: 4.3

Description:

OpenSSH is prone to a security bypass vulnerability. The flaw is due to the refusal deadline was not checked within the x11_open_helper function. Successful exploitation will allow remote attackers to bypass intended access restrictions.

Solution:

VendorFix Upgrade to OpenSSH version 6.9 or later.

Result:

Installed version: 6.6.1 Fixed version: 6.9 Installation path / port: 22/tcp

References:

- http://openwall.com/lists/oss-security/2015/07/01/10

Unique Alert ID: 539290 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 'mod_cache' Denial of Service Vulnerability -01 May15 (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-0117
Cvss Base: 4.3
Cvss Score: 4.3

Description:

Apache HTTP Server is prone to a denial of service vulnerability. Flaw is due to vulnerability in mod_proxy module in the Apache HTTP Server. Successful exploitation will allow a remote attacker to cause a denial of service via a crafted HTTP Connection header when a reverse proxy is enabled.

Solution:

VendorFix Update to version 2.4.10 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.10 Installation path / port: 443/tcp

References:

- http://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 539291 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 'mod_lua' Denial of Service Vulnerability May15 (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-8109
Cvss Base: 4.3
Cvss Score: 4.3

Description:

Apache HTTP Server is prone to a denial of service vulnerability. Flaw is due to a vulnerability in LuaAuthzProvider that is triggered if a user-supplied LUA script is supplied more than once with different arguments. Successful exploitation will all ow a remote attacker to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Requir e directives.

Solution:

VendorFix Update to version 2.4.12 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.12 Installation path / port: 80/tcp

References:

- http://httpd.apache.org/security/vulnerabilities_24.html,http://www.rapid7.com/db/vulnerabilities/apache-httpd-cve-2014-8109

Unique Alert ID: 539288 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 'mod_cache' Denial of Service Vulnerability May15 (tcp/80)

Open Status:	Re-OPEN	**First Found:**	2020-11-18
CVE ID:	CVE-2013-4352		
Cvss Base:	4.3		
Cvss Score:	4.3		

Description:

Apache HTTP Server is prone to a denial of service vulnerability. Flaw is due to vulnerability in 'cache_invalidate' function in modules/cache/cache_storage.c script in the mod_cache module in the Apache HTTP Server. Successful exploitation wi ll allow a remote attacker to cause a denial of service via specially crafted request.

Solution:

VendorFix Update to version 2.4.7 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.7 Installation path / port: 80/tcp

References:

- https://bugzilla.redhat.com/show_bug.cgi?id=1120604,http://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 919588 Found on: 2023-10-06 Severity: Medium

SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection (tcp/443)

Open Status:	Re-OPEN	**First Found:**	2022-05-17
CVE ID:	CVE-2011-3389,CVE-2015-0204		
Cvss Base:	4.3		
Cvss Score:	4.3		

Description:

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system. The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like: - CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST) - CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK) An a ttacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service t o get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in t his protocols won't receive security updates anymore.

Solution:

Mitigation It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Result:

In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.802067) VT.

References:

- https://ssl-config.mozilla.org/,https://bettercrypto.org/,https://datatracker.ietf.org/doc/rfc8996/,https://vnhacker.bl ogspot.com/2011/09/beast.html,https://web.archive.org/web/20201108095603/https://censys.io/blog/freak,https:// www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014

Unique Alert ID: 539294 Found on: 2023-10-06 Severity: Medium

PHP 'LibGD' Denial of Service Vulnerability (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2014-2497
Cvss Base: 4.3
Cvss Score: 4.3

Description:

PHP is prone to a denial of service (DoS) vulnerability. The flaw is due to a NULL pointer dereference error in 'gdImageCreateFromXpm' function within LibGD. Successful exploitation will allow remote attackers to conduct denial of service attacks.

Solution:

VendorFix Update to PHP version 5.4.32 or 5.5.16 or 5.6.0 or later.

Result:

Installed version: 5.4.16 Fixed version: 5.4.32/5.5.16/5.6.0

References:

- https://bugs.php.net/bug.php?id=66901

Unique Alert ID: 539303 Found on: 2023-10-06 Severity: Medium

Weak Encryption Algorithm(s) Supported (SSH) (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 4.3
Cvss Score: 4.3

Description:

The remote SSH server is configured to allow / support weak encryption algorithm(s). - The 'arcfour' cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore. - The 'none' algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it. - A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Solution:

Mitigation Disable the reported weak encryption algorithm(s).

Result:

The remote SSH server supports the following weak client-to-server encryption algorithm(s): 3des-cbc aes128-cbc aes192-cbc aes256-cbc arcfour arcfour128 arcfour256 blowfish-cbc cast128-cbc rijndael-cbc@lysator.liu.se The remote SSH server supports the following weak server-to-client encryption algorithm(s): 3des-cbc aes128-cbc aes192-cbc aes256-cbc arcfour arcfour128 arcfour256 blowfish-cbc cast128-cbc rijndael-cbc@lysator.liu.se

References:

- https://www.rfc-editor.org/rfc/rfc4253#section-6.3

Unique Alert ID: 539289 Found on: 2023-10-06 Severity: Medium

Apache HTTP Server 'mod_cache' Denial of Service Vulnerability May15 (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2013-4352
Cvss Base: 4.3
Cvss Score: 4.3

Description:

Apache HTTP Server is prone to a denial of service vulnerability. Flaw is due to vulnerability in 'cache_invalidate' function in modules/cache/cache_storage.c script in the mod_cache module in the Apache HTTP Server. Successful exploitation wi ll allow a remote attacker to cause a denial of service via specially crafted request.

Solution:

VendorFix Update to version 2.4.7 or later.

Result:

Installed version: 2.4.6 Fixed version: 2.4.7 Installation path / port: 443/tcp

References:

- https://bugzilla.redhat.com/show_bug.cgi?id=1120604,http://httpd.apache.org/security/vulnerabilities_24.html

Unique Alert ID: 1533232 Found on: 2023-10-06 Severity: Medium

OpenBSD OpenSSH < 9.1 Multiple Vulnerabilities (tcp/22)

Open Status: Re-OPEN **First Found:** 2023-10-06
Cvss Base: 4.0
Cvss Score: 4.0

Description:

OpenBSD OpenSSH is prone to multiple vulnerabilities. The following vulnerabilities exist: - A one-byte overflow in SSH-banner processing in ssh-keyscan. - A double free() in error path of file hashing step in signing/verify code in ssh-keygen . - A double-free in error path in ssh-keysign.

Solution:

VendorFix Update to version 9.1 or later.

Result:

Installed version: 6.6.1 Fixed version: 9.1 Installation path / port: 22/tcp

Unique Alert ID: 539295 Found on: 2023-10-06 Severity: Low

OpenSSL 1.0.2, 1.1.0, 1.1.1 Multiple Vulnerabilities - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2019-1547,CVE-2019-1563
Cvss Base: 3.7
Cvss Score: 3.7
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

Description:

OpenSSL is prone to multiple vulnerabilities. OpenSSL is prone to multiple vulnerabilities: - ECDSA remote timing attack (CVE-2019-1547) - Padding Oracle in PKCS7_dataDecode and CMS_decrypt_set1_pkey (CVE-2019-1563)

Solution:

VendorFix Update to version 1.0.2t, 1.1.0l, 1.1.1d or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2t Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20190910.txt

Unique Alert ID: 919590 Found on: 2023-10-06 Severity: Low

OpenSSL: Raccoon Attack (CVE-2020-1968) (Linux) (tcp/80)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2020-1968	
Cvss Base:	3.7	
Cvss Score:	3.7	
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N	

Description:

OpenSSL is prone to Racoon attacks. The Raccoon attack exploits a flaw in the TLS specification which can lead to an atta cker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuit e. In such a case this would result in the attacker being able to eavesdrop on all encrypted communications sent over tha t TLS connection. The attack can only be exploited if an implementation re-uses a DH secret across multiple TLS connecti ons. Note that this issue only impacts DH ciphersuites and not ECDH ciphersuites. An attacker may eavesdrop on encrypt ed communications sent over a TLS connection.

Solution:

VendorFix Update to version 1.0.2w, 1.1.1 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2w Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20200909.txt

Unique Alert ID: 919589 Found on: 2023-10-06 Severity: Low

OpenSSL: Raccoon Attack (CVE-2020-1968) (Linux) (tcp/443)

Open Status:	Re-OPEN	**First Found:** 2022-05-17
CVE ID:	CVE-2020-1968	
Cvss Base:	3.7	
Cvss Score:	3.7	
Cvss Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N	

Description:

OpenSSL is prone to Racoon attacks. The Raccoon attack exploits a flaw in the TLS specification which can lead to an atta cker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuit e. In such a case this would result in the attacker being able to eavesdrop on all encrypted communications sent over tha t TLS connection. The attack can only be exploited if an implementation re-uses a DH secret across multiple TLS connecti ons. Note that this issue only impacts DH ciphersuites and not ECDH ciphersuites. An attacker may eavesdrop on encrypt ed communications sent over a TLS connection.

Solution:

VendorFix Update to version 1.0.2w, 1.1.1 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2w Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20200909.txt

Unique Alert ID: 607310 Found on: 2023-10-06 Severity: Low

OpenSSL 1.0.2, 1.1.0, 1.1.1 Multiple Vulnerabilities - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-12-18
CVE ID: CVE-2019-1547,CVE-2019-1563
Cvss Base: 3.7
Cvss Score: 3.7
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

Description:

OpenSSL is prone to multiple vulnerabilities. OpenSSL is prone to multiple vulnerabilities: - ECDSA remote timing attack (CVE-2019-1547) - Padding Oracle in PKCS7_dataDecode and CMS_decrypt_set1_pkey (CVE-2019-1563)

Solution:

VendorFix Update to version 1.0.2t, 1.1.0l, 1.1.1d or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2t Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20190910.txt

Unique Alert ID: 919592 Found on: 2023-10-06 Severity: Low

PHP <= 5.6.0 'PEAR' Symlink Attack Vulnerability (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2014-5459
Cvss Base: 3.6
Cvss Score: 3.6

Description:

PHP is prone to a symlink attack vulnerability in the included PEAR installer. The PEAR_REST class in REST.php in PEAR al lows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/ cache/, related to the retrieveCacheFirst and useLocalCache functions.

Solution:

VendorFix Update to a later PHP version including an PEAR installer in version 1.9.2 or later.

Result:

Installed version: 5.4.16 Fixed version: See references Installation path / port: 443/tcp

References:

- https://pear.php.net/bugs/bug.php?id=18056,https://pear.php.net/bugs/bug.php?id=18055,http://www.openwall.com/lists/oss-security/2014/08/27/3

Unique Alert ID: 539307 Found on: 2023-10-06 Severity: Low

PHP < 7.2.33, 7.3 < 7.3.21, 7.4 < 7.4.9 DoS Vulnerability - August20 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2020-7068
Cvss Base: 3.6
Cvss Score: 3.6
Cvss Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:L

Description:

PHP is prone to a denial of service vulnerability in the phar_parse_zipfile function. The phar_parse_zipfile function had us e-after-free vulnerability because of mishandling of the actual_alias variable.

Solution:

VendorFix Update to version 7.2.33, 7.3.21, 7.4.9 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.33 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.33,https://www.php.net/ChangeLog-7.php#7.3.21,https://www.php.net/ChangeLog-7.php#7.4.9

Unique Alert ID: 919591 Found on: 2023-10-06 Severity: Low

PHP <= 5.6.0 'PEAR' Symlink Attack Vulnerability (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2014-5459
Cvss Base: 3.6
Cvss Score: 3.6

Description:

PHP is prone to a symlink attack vulnerability in the included PEAR installer. The PEAR_REST class in REST.php in PEAR al lows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/ cache/, related to the retrieveCacheFirst and useLocalCache functions.

Solution:

VendorFix Update to a later PHP version including an PEAR installer in version 1.9.2 or later.

Result:

Installed version: 5.4.16 Fixed version: See references Installation path / port: 80/tcp

References:

- https://pear.php.net/bugs/bug.php?id=18056,https://pear.php.net/bugs/bug.php?id=18055,http://www.openwall.com/lists/oss-security/2014/08/27/3

Unique Alert ID: 539306 Found on: 2023-10-06 Severity: Low

PHP < 7.2.33, 7.3 < 7.3.21, 7.4 < 7.4.9 DoS Vulnerability - August20 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2020-7068
Cvss Base: 3.6
Cvss Score: 3.6
Cvss Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:L

Description:

PHP is prone to a denial of service vulnerability in the phar_parse_zipfile function. The phar_parse_zipfile function had us e-after-free vulnerability because of mishandling of the actual_alias variable.

Solution:

VendorFix Update to version 7.2.33, 7.3.21, 7.4.9 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.33 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.33,https://www.php.net/ChangeLog-7.php#7.3.21,https://www.php.net/ChangeLog-7.php#7.4.9

Unique Alert ID: 539313 Found on: 2023-10-06 Severity: Low

TCP Timestamps Information Disclosure (tcp)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 2.6
Cvss Score: 2.6

Description:

The remote host implements TCP timestamps and therefore allows to compute the uptime. The remote host implements TCP timestamps, as defined by RFC1323/RFC7323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution:

Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Result:

It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 46234789 Packet 2: 46236098

References:

- https://datatracker.ietf.org/doc/html/rfc1323,https://datatracker.ietf.org/doc/html/rfc7323,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

Unique Alert ID: 539312 Found on: 2023-10-06 Severity: Low

Weak MAC Algorithm(s) Supported (SSH) (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 2.6
Cvss Score: 2.6

Description:

The remote SSH server is configured to allow / support weak MAC algorithm(s).

Solution:

Mitigation Disable the reported weak MAC algorithm(s).

Result:

The remote SSH server supports the following weak client-to-server MAC algorithm(s): hmac-md5 hmac-md5-96 hmac-md5-96-etm@openssh.com hmac-md5-etm@openssh.com hmac-sha1-96 hmac-sha1-96-etm@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm(s): hmac-md5 hmac-md5-96 hmac-md5-96-etm@openssh.com hmac-md5-etm@openssh.com hmac-sha1-96 hmac-sha1-96-etm@openssh.com

Unique Alert ID: 539295 Found on: 2023-10-06 Severity: Low

OpenSSL 1.0.2, 1.1.0, 1.1.1 Multiple Vulnerabilities - Linux (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2019-1547,CVE-2019-1563
Cvss Base: 3.7
Cvss Score: 3.7
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

Description:

OpenSSL is prone to multiple vulnerabilities. OpenSSL is prone to multiple vulnerabilities: - ECDSA remote timing attack (CVE-2019-1547) - Padding Oracle in PKCS7_dataDecode and CMS_decrypt_set1_pkey (CVE-2019-1563)

Solution:

VendorFix Update to version 1.0.2t, 1.1.0l, 1.1.1d or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2t Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20190910.txt

Unique Alert ID: 919590 Found on: 2023-10-06 Severity: Low

OpenSSL: Raccoon Attack (CVE-2020-1968) (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2020-1968
Cvss Base: 3.7
Cvss Score: 3.7
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

Description:

OpenSSL is prone to Racoon attacks. The Raccoon attack exploits a flaw in the TLS specification which can lead to an atta cker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuit e. In such a case this would result in the attacker being able to eavesdrop on all encrypted communications sent over tha t TLS connection. The attack can only be exploited if an implementation re-uses a DH secret across multiple TLS connecti ons. Note that this issue only impacts DH ciphersuites and not ECDH ciphersuites. An attacker may eavesdrop on encrypt ed communications sent over a TLS connection.

Solution:

VendorFix Update to version 1.0.2w, 1.1.1 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2w Installation path / port: 80/tcp

References:

- https://www.openssl.org/news/secadv/20200909.txt

Unique Alert ID: 919589 Found on: 2023-10-06 Severity: Low

OpenSSL: Raccoon Attack (CVE-2020-1968) (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2020-1968
Cvss Base: 3.7
Cvss Score: 3.7
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

Description:

OpenSSL is prone to Racoon attacks. The Raccoon attack exploits a flaw in the TLS specification which can lead to an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based ciphersuite. In such a case this would result in the attacker being able to eavesdrop on all encrypted communications sent over that TLS connection. The attack can only be exploited if an implementation re-uses a DH secret across multiple TLS connections. Note that this issue only impacts DH ciphersuites and not ECDH ciphersuites. An attacker may eavesdrop on encrypted communications sent over a TLS connection.

Solution:

VendorFix Update to version 1.0.2w, 1.1.1 or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2w Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20200909.txt

Unique Alert ID: 607310 Found on: 2023-10-06 Severity: Low

OpenSSL 1.0.2, 1.1.0, 1.1.1 Multiple Vulnerabilities - Linux (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-12-18
CVE ID: CVE-2019-1547,CVE-2019-1563
Cvss Base: 3.7
Cvss Score: 3.7
Cvss Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

Description:

OpenSSL is prone to multiple vulnerabilities. OpenSSL is prone to multiple vulnerabilities: - ECDSA remote timing attack (CVE-2019-1547) - Padding Oracle in PKCS7_dataDecode and CMS_decrypt_set1_pkey (CVE-2019-1563)

Solution:

VendorFix Update to version 1.0.2t, 1.1.0l, 1.1.1d or later.

Result:

Installed version: 1.0.2k Fixed version: 1.0.2t Installation path / port: 443/tcp

References:

- https://www.openssl.org/news/secadv/20190910.txt

Unique Alert ID: 919592 Found on: 2023-10-06 Severity: Low

PHP <= 5.6.0 'PEAR' Symlink Attack Vulnerability (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2014-5459
Cvss Base: 3.6
Cvss Score: 3.6

Description:

PHP is prone to a symlink attack vulnerability in the included PEAR installer. The PEAR_REST class in REST.php in PEAR al lows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/ cache/, related to the retrieveCacheFirst and useLocalCache functions.

Solution:

VendorFix Update to a later PHP version including an PEAR installer in version 1.9.2 or later.

Result:

Installed version: 5.4.16 Fixed version: See references Installation path / port: 443/tcp

References:

- https://pear.php.net/bugs/bug.php?id=18056,https://pear.php.net/bugs/bug.php?id=18055,http://www.openwall.com/lists/oss-security/2014/08/27/3

Unique Alert ID: 539307 Found on: 2023-10-06 Severity: Low

PHP < 7.2.33, 7.3 < 7.3.21, 7.4 < 7.4.9 DoS Vulnerability - August20 (Linux) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2020-7068
Cvss Base: 3.6
Cvss Score: 3.6
Cvss Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:L

Description:

PHP is prone to a denial of service vulnerability in the phar_parse_zipfile function. The phar_parse_zipfile function had us e-after-free vulnerability because of mishandling of the actual_alias variable.

Solution:

VendorFix Update to version 7.2.33, 7.3.21, 7.4.9 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.33 Installation path / port: 80/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.33,https://www.php.net/ChangeLog-7.php#7.3.21,https://www.php.net/ChangeLog-7.php#7.4.9

Unique Alert ID: 919591 Found on: 2023-10-06 Severity: Low

PHP <= 5.6.0 'PEAR' Symlink Attack Vulnerability (tcp/80)

Open Status: Re-OPEN **First Found:** 2022-05-17
CVE ID: CVE-2014-5459
Cvss Base: 3.6
Cvss Score: 3.6

Description:

PHP is prone to a symlink attack vulnerability in the included PEAR installer. The PEAR_REST class in REST.php in PEAR al lows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/ cache/, related to the retrieveCacheFirst and useLocalCache functions.

Solution:

VendorFix Update to a later PHP version including an PEAR installer in version 1.9.2 or later.

Result:

Installed version: 5.4.16 Fixed version: See references Installation path / port: 80/tcp

References:

- https://pear.php.net/bugs/bug.php?id=18056,https://pear.php.net/bugs/bug.php?id=18055,http://www.openwall.co

m/lists/oss-security/2014/08/27/3

Unique Alert ID: 539306 Found on: 2023-10-06 Severity: Low

PHP < 7.2.33, 7.3 < 7.3.21, 7.4 < 7.4.9 DoS Vulnerability - August20 (Linux) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
CVE ID: CVE-2020-7068
Cvss Base: 3.6
Cvss Score: 3.6
Cvss Vector: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:L

Description:

PHP is prone to a denial of service vulnerability in the phar_parse_zipfile function. The phar_parse_zipfile function had use-after-free vulnerability because of mishandling of the actual_alias variable.

Solution:

VendorFix Update to version 7.2.33, 7.3.21, 7.4.9 or later.

Result:

Installed version: 5.4.16 Fixed version: 7.2.33 Installation path / port: 443/tcp

References:

- https://www.php.net/ChangeLog-7.php#7.2.33,https://www.php.net/ChangeLog-7.php#7.3.21,https://www.php.net/ChangeLog-7.php#7.4.9

Unique Alert ID: 539313 Found on: 2023-10-06 Severity: Low

TCP Timestamps Information Disclosure (tcp)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 2.6
Cvss Score: 2.6

Description:

The remote host implements TCP timestamps and therefore allows to compute the uptime. The remote host implements TCP timestamps, as defined by RFC1323/RFC7323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution:

Mitigation To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See the references for more information.

Result:

It was detected that the host implements RFC1323/RFC7323. The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 46234789 Packet 2: 46236098

References:

- https://datatracker.ietf.org/doc/html/rfc1323,https://datatracker.ietf.org/doc/html/rfc7323,https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152

Unique Alert ID: 539312 Found on: 2023-10-06 Severity: Low

Weak MAC Algorithm(s) Supported (SSH) (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 2.6
Cvss Score: 2.6

Description:

The remote SSH server is configured to allow / support weak MAC algorithm(s).

Solution:

Mitigation Disable the reported weak MAC algorithm(s).

Result:

The remote SSH server supports the following weak client-to-server MAC algorithm(s): hmac-md5 hmac-md5-96 hmac-md5-96-etm@openssh.com hmac-md5-etm@openssh.com hmac-sha1-96 hmac-sha1-96-etm@openssh.com The remote SSH server supports the following weak server-to-client MAC algorithm(s): hmac-md5 hmac-md5-96 hmac-md5-96-etm@openssh.com hmac-md5-etm@openssh.com hmac-sha1-96 hmac-sha1-96-etm@openssh.com

Unique Alert ID: 919596 Found on: 2023-10-06 Severity: Info

OpenSSL Detection Consolidation (tcp)

Open Status: Re-OPEN **First Found:** 2022-05-17
Cvss Base: 0.0
Cvss Score: 0.0

Description:

Consolidation of OpenSSL detections.

Solution:

Result:

Detected OpenSSL Version: 1.0.2k Location: 443/tcp CPE: cpe:/a:openssl:openssl:1.0.2k Concluded from version/product identification result: Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16 OpenSSL/1.0.2k-fips Detected OpenSSL Version: 1.0.2k Location: 80/tcp CPE: cpe:/a:openssl:openssl:1.0.2k Concluded from version/product identification result: Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16 OpenSSL/1.0.2k-fips

Unique Alert ID: 539330 Found on: 2023-10-06 Severity: Info

SSL/TLS: Collect and Report Certificate Details (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This script collects and reports the details of all SSL/TLS certificates. This data will be used by other tests to verify server certificates.

Solution:

Result:

The following certificate details of the remote service were collected. Certificate details: fingerprint (SHA-1) | 81C5AB98A9E8BECAEEB849E97EF47D7A14DCF936 fingerprint (SHA-256) | 635269291BDF6067EEDB2D40DB10B25C354D9FEA326F43779AE51D6C3FEB0FAB issued by | CN=Let's Encrypt Authority X3,O=Let's Encrypt,C=US public key algorithm | RSA public key size (bits) | 2048 serial |

0342FA98D61F9F34FD44E05EE95726E89BB3 signature algorithm | sha256WithRSAEncryption subject | CN=*.testapptrana.com subject alternative names (SAN) | *.testapptrana.com valid from | 2018-12-13 13:40:08 UTC valid until | 2019-03-13 13:40:08 UTC

Unique Alert ID: 539342 Found on: 2023-10-06 Severity: Info

Services (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This plugin performs service detection. This plugin attempts to guess which service is running on the remote port(s). For i nstance, it searches for a web server which could listen on another port than 80 or 443 and makes this information availa ble for other check routines.

Solution:

Result:

An ssh server is running on this port

Unique Alert ID: 539349 Found on: 2023-10-06 Severity: Info

CGI Scanning Consolidation (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

The script consolidates various information for CGI scanning. This information is based on the following scripts / settings: - HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034) - No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386) - Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662) - Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032) - The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use - The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to direc tories for CGI scanning' within the 'Global variable settings' of the scan config in use If you think any of this information i s wrong please report it to the referenced community forum.

Solution:

Result:

The Hostname/IP "ec2-34-233-47-30.compute-1.amazonaws.com" was used to access the remote host. Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use. Requests to this service are done via HTTP/1.1. This service seems to be able to host PHP scripts. This service seems to be NOT able to host ASP scripts. The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.4.0)" was used to access the remote host. Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use. The following directories were used for CGI scanning: http://ec2-34-233-47-30.compute-1.amazonaws.com/ http://ec2-34-233-47-30.compute-1.amazonaws.com/config http://ec2-34-233-47-30.compute-1.amazonaws.com/docs http://ec2-34-233-47-30.compute-1.amazonaws.com/dvwa http://ec2-34-233-47-30.compute-1.amazonaws.com/external While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards The following directories were excluded from CGI scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the VT "Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|picture|bilder|thumb nail|media/|skins?/)" http://ec2-34-233-47-30.compute-1.amazonaws.com/icons

Unique Alert ID: 539341 Found on: 2023-10-06 Severity: Info

Services (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This plugin performs service detection. This plugin attempts to guess which service is running on the remote port(s). For i nstance, it searches for a web server which could listen on another port than 80 or 443 and makes this information availa ble for other check routines.

Solution:

Result:

A web server is running on this port

Unique Alert ID: 539338 Found on: 2023-10-06 Severity: Info

Services (tcp/3306)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This plugin performs service detection. This plugin attempts to guess which service is running on the remote port(s). For i nstance, it searches for a web server which could listen on another port than 80 or 443 and makes this information availa ble for other check routines.

Solution:

Result:

A MySQL server is running on this port

Unique Alert ID: 539325 Found on: 2023-10-06 Severity: Info

HTTP Server type and version (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Solution:

Result:

The remote HTTP Server banner is: Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16 OpenSSL/1.0.2k-fips

Unique Alert ID: 539351 Found on: 2023-10-06 Severity: Info

SSL/TLS: Report Supported Cipher Suites (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This routine reports all SSL/TLS cipher suites accepted by a service. Notes: - As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead. - SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Solution:

Result:

'Strong' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA 'Medium' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA No 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol. No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol. No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol. 'Strong' cipher suites accepted by this service via the TLSv1.1 protocol: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA No 'Weak' cipher suites accepted by this service via the TLSv1.1 protocol. No 'Null' cipher suites accepted by this service via the TLSv1.1 protocol. No 'Anonymous' cipher suites accepted by this service via the TLSv1.1 protocol. 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol. No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol. No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.

Unique Alert ID: 539322 Found on: 2023-10-06 Severity: Info

SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Solution:

Result:

The certificate of the remote service contains a common name (CN) that does not match the hostname "ec2-34-233-47-30.compute-1.amazonaws.com". Certificate details: fingerprint (SHA-1) | 81C5AB98A9E8BECAEEB849E97EF47D7A14DCF936 fingerprint (SHA-256) | 635269291BDF6067EEDB2D40DB10B25C354D9FEA326F43779AE51D6C3FEB0FAB issued by | CN=Let's Encrypt Authority X3,O=Let's Encrypt,C=US public key algorithm | RSA public key size (bits) | 2048 serial | 0342FA98D61F9F34FD44E05EE95726E89BB3 signature algorithm | sha256WithRSAEncryption subject | CN=*.testapptrana.com subject alternative names (SAN) | *.testapptrana.com valid from | 2018-12-13 13:40:08 UTC valid until | 2019-03-13 13:40:08 UTC

Unique Alert ID: 539317 Found on: 2023-10-06 Severity: Info

SSL/TLS: Report Non Weak Cipher Suites (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Solution:

Result:

'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA 'Non Weak' cipher suites accepted by this service via the TLSv1.1 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA 'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

Unique Alert ID: 539335 Found on: 2023-10-06 Severity: Info

SSH Server type and version (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This detects the SSH Server's type and version by connecting to the server and processing the buffer received. This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Solution:

Result:

Remote SSH server banner: SSH-2.0-OpenSSH_6.6.1 Remote SSH supported authentication: publickey
Remote SSH text/login banner: (not available) This is probably: - OpenSSH Concluded from remote connection attempt with credentials: Login: OpenVASVT Password: OpenVASVT

Unique Alert ID: 539333 Found on: 2023-10-06 Severity: Info

OpenSSH Detection Consolidation (tcp)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

Consolidation of OpenSSH detections.

Solution:

Result:

Detected OpenSSH Server Version: 6.6.1 Location: 22/tcp CPE: cpe:/a:openbsd:openssh:6.6.1 Concluded from version/product identification result: SSH-2.0-OpenSSH_6.6.1

Unique Alert ID: 539326 Found on: 2023-10-06 Severity: Info

Traceroute (tcp)

Open Status: OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

Collect information about the network route and network distance between the scanner host and the target host. For internal networks, the distances are usually small, often less than 4 hosts between scanner and target. For public targets the distance is greater and might be 10 hosts or more.

Solution:

Result:

Network route from scanner (10.0.1.193) to target (34.233.47.30): 10.0.1.193 34.233.47.30 Network

distance between scanner and target: 2

Unique Alert ID: 539352 Found on: 2023-10-06 Severity: Info

PHP Detection (HTTP) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

HTTP based detection of PHP.

Solution:

Result:

Detected PHP Version: 5.4.16 Location: 443/tcp CPE: cpe:/a:php:php:5.4.16 Concluded from version/product identification result: Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16 OpenSSL/1.0.2k-fips

Unique Alert ID: 539344 Found on: 2023-10-06 Severity: Info

PHP Detection (HTTP) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

HTTP based detection of PHP.

Solution:

Result:

Detected PHP Version: 5.4.16 Location: 80/tcp CPE: cpe:/a:php:php:5.4.16 Concluded from version/product identification result: Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16 OpenSSL/1.0.2k-fips

Unique Alert ID: 539318 Found on: 2023-10-06 Severity: Info

SSL/TLS: Report Medium Cipher Suites (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This routine reports all Medium SSL/TLS cipher suites accepted by a service. Any cipher suite considered to be secure for only the next 10 years is considered as medium.

Solution:

Result:

'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA 'Medium' cipher suites accepted by this service via the TLSv1.1 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA 'Medium' cipher suites
accepted by this service via the TLSv1.2 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

Unique Alert ID: 539343 Found on: 2023-10-06 Severity: Info

OS Detection Consolidation and Reporting (tcp)

Open Status: OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This script consolidates the OS information detected by several VTs and tries to find the best matching OS. Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional informatio n which might help to improve the OS detection. If any of this information is wrong or could be improved please consider to report these to the referenced community forum.

Solution:

Result:

Best matching OS: OS: Red Hat Enterprise Linux CPE: cpe:/o:redhat:enterprise_linux Found by VT: 1.3.6.1.4.1.25623.1.0.111067 (Operating System (OS) Detection (HTTP)) Concluded from HTTP Server banner on port 80/tcp: Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16 OpenSSL/1.0.2k-fips Setting key "Host/runs_unixoide" based on this information Other OS detections (in order of reliability): OS: Red Hat Enterprise Linux CPE: cpe:/o:redhat:enterprise_linux Found by VT: 1.3.6.1.4.1.25623.1.0.111067 (Operating System (OS) Detection (HTTP)) Concluded from HTTP Server banner on port 443/tcp: Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16 OpenSSL/1.0.2k-fips

Unique Alert ID: 539332 Found on: 2023-10-06 Severity: Info

SSH Protocol Algorithms Supported (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This script detects which algorithms are supported by the remote SSH Service.

Solution:

Result:

The following options are supported by the remote ssh service: kex_algorithms: curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1 server_host_key_algorithms: ssh-rsa,ecdsa-sha2-nistp256,ssh-ed25519

encryption_algorithms_client_to_server: aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se
encryption_algorithms_server_to_client: aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se
mac_algorithms_client_to_server: hmac-md5-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-ripemd160-etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-md5-96-etm@openssh.com,hmac-md5,hmac-sha1,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
mac_algorithms_server_to_client: hmac-md5-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-ripemd160-etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-md5-96-etm@openssh.com,hmac-md5,hmac-sha1,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
compression_algorithms_client_to_server: none,zlib@openssh.com
compression_algorithms_server_to_client: none,zlib@openssh.com

Unique Alert ID: 539331 Found on: 2023-10-06 Severity: Info

SSH Protocol Versions Supported (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints fr om the service. The following versions are tried: 1.33, 1.5, 1.99 and 2.0

Solution:

Result:

The remote SSH Server supports the following SSH Protocol Versions: 1.99 2.0 SSHv2 Fingerprint(s): ecdsa-sha2-nistp256: ca:f7:d0:03:26:7a:29:ec:7a:7e:46:c5:c0:ec:e1:6e ssh-ed25519: fa:e2:ef:60:00:85:ba:50:9f:dd:92:ef:35:10:19:4f ssh-rsa: 43:f7:2a:af:a7:fb:50:9c:ac:78:f1:20:1b:ef:ee:42

Unique Alert ID: 919593 Found on: 2023-10-06 Severity: Info

SSL/TLS: Version Detection (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
Cvss Base: 0.0
Cvss Score: 0.0

Description:

Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.

Solution:

Result:

The remote SSL/TLS service supports the following SSL/TLS protocol version(s): TLSv1.0 TLSv1.1 TLSv1.2

Unique Alert ID: 539319 Found on: 2023-10-06 Severity: Info

SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Solution:

Result:

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.0 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.1 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Unique Alert ID: 539323 Found on: 2023-10-06 Severity: Info

Services (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This plugin performs service detection. This plugin attempts to guess which service is running on the remote port(s). For i nstance, it searches for a web server which could listen on another port than 80 or 443 and makes this information availa ble for other check routines.

Solution:

Result:

A web server is running on this port

Unique Alert ID: 539345 Found on: 2023-10-06 Severity: Info

HTTP Security Headers Detection (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

All known security headers are being checked on the remote web server. On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Solution:

Result:

Missing Headers | More Information ----------

------- Content-Security-Policy | https://owasp.org/www-project-secure-headers/#content-security-policy Cross-Origin-Embedder-Policy | https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header Cross-Origin-Opener-Policy | https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header Cross-Origin-Resource-Policy | https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header Document-Policy | https://w3c.github.io/webappsec-feature-policy/document-policy#document-policy-http-header Feature-Policy | https://owasp.org/www-project-secure-headers/#feature-policy, Note: The Feature Policy header has been renamed to Permissions Policy Permissions-Policy | https://w3c.github.io/webappsec-feature-policy/#permissions-policy-http-header-field Referrer-Policy | https://owasp.org/www-project-secure-headers/#referrer-policy Sec-Fetch-Dest | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90 Sec-Fetch-Mode | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90 Sec-Fetch-Site | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90 Sec-Fetch-User | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90 X-Content-Type-Options | https://owasp.org/www-project-secure-headers/#x-content-type-options X-Frame-Options | https://owasp.org/www-project-secure-headers/#x-frame-options X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers/#x-permitted-cross-domain-policies X-XSS-Protection | https://owasp.org/www-project-secure-headers/#x-xss-protection, Note: Most major browsers have dropped / deprecated support for this header in 2020.

References:

- https://owasp.org/www-project-secure-headers/,https://owasp.org/www-project-secure-headers/#div-headers,https://securityheaders.com/

Unique Alert ID: 539346 Found on: 2023-10-06 Severity: Info

HTTP Security Headers Detection (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

All known security headers are being checked on the remote web server. On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Solution:

Result:

Missing Headers | More Information ----------

------- Content-Security-Policy | https://owasp.org/www-project-secure-headers/#content-security-policy Cross-Origin-Embedder-Policy | https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header Cross-Origin-Opener-Policy | https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header Cross-Origin-Resource-Policy | https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header Document-Policy | https://w3c.github.io/webappsec-feature-policy/document-policy#document-policy-http-header Feature-Policy | https://owasp.org/www-project-secure-headers/#feature-policy, Note: The Feature Policy header has been renamed to Permissions Policy Permissions-Policy | https://w3c.github.io/webappsec-feature-policy/#permissions-policy-http-header-field Referrer-Policy | https://owasp.org/www-project-secure-headers/#referrer-policy Sec-Fetch-Dest | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90 Sec-Fetch-Mode | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90 Sec-Fetch-Site | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90 Sec-Fetch-User | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90 X-Content-Type-Options | https://owasp.org/www-project-secure-headers/#x-content-type-options X-Frame-Options | https://owasp.org/www-project-secure-headers/#x-frame-options X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers/#x-permitted-cross-domain-policies X-XSS-Protection | https://owasp.org/www-project-secure-headers/#x-xss-protection, Note: Most major browsers have dropped / deprecated support for this header in 2020.

References:

- https://owasp.org/www-project-secure-headers/,https://owasp.org/www-project-secure-headers/#div-headers,https://securityheaders.com/

Unique Alert ID: 539350 Found on: 2023-10-06 Severity: Info

CGI Scanning Consolidation (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

The script consolidates various information for CGI scanning. This information is based on the following scripts / settings: - HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034) - No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386) - Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662) - Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032) - The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use - The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use If you think any of this information is wrong please report it to the referenced community forum.

Solution:

Result:

The Hostname/IP "ec2-34-233-47-30.compute-1.amazonaws.com" was used to access the remote host. Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use. Requests to this service are done via HTTP/1.1. This service seems to be able to host PHP scripts. This service seems to be NOT able to host ASP scripts. The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.4.0)" was used to access the remote host. Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use. The following directories were used for CGI scanning: http://ec2-34-233-47-30.compute-1.amazonaws.com/ While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

Unique Alert ID: 1010828 Found on: 2023-10-06 Severity: Info

SSL/TLS: Safe/Secure Renegotiation Support Status (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-08-27
Cvss Base: 0.0
Cvss Score: 0.0

Description:

Checks and reports if a remote SSL/TLS service supports safe/secure renegotiation.

Solution:

Result:

Protocol Version | Safe/Secure Renegotiation Support Status ---------- SSLv3 | Unknown, Reason: Failed to open a socket to the remote service. TLSv1.0 | Unknown, Reason: Failed to open a socket to the remote service. TLSv1.1 | Unknown, Reason: Failed to open a socket to the remote service. TLSv1.2 | Unknown, Reason: Failed to open a socket to the remote service. TLSv1.3 | Unknown, Reason: Failed to open a socket to the remote service.

References:

- https://www.gnutls.org/manual/html_node/Safe-renegotiation.html,https://wiki.openssl.org/index.php/TLS1.3#Renegotiation,https://datatracker.ietf.org/doc/html/rfc5746

Unique Alert ID: 539324 Found on: 2023-10-06 Severity: Info

HTTP Server type and version (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Solution:

Result:

The remote HTTP Server banner is: Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16 OpenSSL/1.0.2k-fips

Unique Alert ID: 539337 Found on: 2023-10-06 Severity: Info

MariaDB / Oracle MySQL Detection (MySQL Protocol) (tcp/3306)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

MySQL protocol-based detection of MariaDB / Oracle MySQL.

Solution:

Result:

Detected MariaDB Version: unknown Location: 3306/tcp CPE: cpe:/a:mariadb:mariadb Extra information: Scanner received a ER_HOST_NOT_PRIVILEGED error from the remote MariaDB server. Some tests may fail. Allow the scanner to access the remote MariaDB server for better results.

Unique Alert ID: 919595 Found on: 2023-10-06 Severity: Info

Apache HTTP Server Detection Consolidation (tcp)

Open Status: Re-OPEN **First Found:** 2022-05-17
Cvss Base: 0.0
Cvss Score: 0.0

Description:

Consolidation of Apache HTTP Server detections.

Solution:

Result:

Detected Apache HTTP Server Version: 2.4.6 Location: 443/tcp CPE: cpe:/a:apache:http_server:2.4.6 Concluded from version/product identification result: Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16 OpenSSL/1.0.2k-fips Detected Apache HTTP Server Version: 2.4.6 Location: 80/tcp CPE: cpe:/a:apache:http_server:2.4.6 Concluded from version/product identification result: Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16 OpenSSL/1.0.2k-fips

Unique Alert ID: 919596 Found on: 2023-10-06 Severity: Info

OpenSSL Detection Consolidation (tcp)

Open Status: Re-OPEN **First Found:** 2022-05-17
Cvss Base: 0.0
Cvss Score: 0.0

Description:

Consolidation of OpenSSL detections.

Solution:

Result:

Detected OpenSSL Version: 1.0.2k Location: 443/tcp CPE: cpe:/a:openssl:openssl:1.0.2k Concluded from version/product identification result: Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16 OpenSSL/1.0.2k-fips Detected OpenSSL Version: 1.0.2k Location: 80/tcp CPE: cpe:/a:openssl:openssl:1.0.2k Concluded from version/product identification result: Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16 OpenSSL/1.0.2k-fips

Unique Alert ID: 539330 Found on: 2023-10-06 Severity: Info

SSL/TLS: Collect and Report Certificate Details (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This script collects and reports the details of all SSL/TLS certificates. This data will be used by other tests to verify server certificates.

Solution:

Result:

The following certificate details of the remote service were collected. Certificate details: fingerprint (SHA-1) | 81C5AB98A9E8BECAEEB849E97EF47D7A14DCF936 fingerprint (SHA-256) | 635269291BDF6067EEDB2D40DB10B25C354D9FEA326F43779AE51D6C3FEB0FAB issued by | CN=Let's Encrypt Authority X3,O=Let's Encrypt,C=US public key algorithm | RSA public key size (bits) | 2048 serial |

0342FA98D61F9F34FD44E05EE95726E89BB3 signature algorithm | sha256WithRSAEncryption subject | CN=*.testapptrana.com subject alternative names (SAN) | *.testapptrana.com valid from | 2018-12-13 13:40:08 UTC valid until | 2019-03-13 13:40:08 UTC

Unique Alert ID: 539342 Found on: 2023-10-06 Severity: Info

Services (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This plugin performs service detection. This plugin attempts to guess which service is running on the remote port(s). For i nstance, it searches for a web server which could listen on another port than 80 or 443 and makes this information availa ble for other check routines.

Solution:

Result:

An ssh server is running on this port

Unique Alert ID: 539349 Found on: 2023-10-06 Severity: Info

CGI Scanning Consolidation (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

The script consolidates various information for CGI scanning. This information is based on the following scripts / settings: - HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034) - No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386) - Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662) - Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032) - The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use - The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to direc tories for CGI scanning' within the 'Global variable settings' of the scan config in use If you think any of this information i s wrong please report it to the referenced community forum.

Solution:

Result:

The Hostname/IP "ec2-34-233-47-30.compute-1.amazonaws.com" was used to access the remote host. Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use. Requests to this service are done via HTTP/1.1. This service seems to be able to host PHP scripts. This service seems to be NOT able to host ASP scripts. The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.4.0)" was used to access the remote host. Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use. The following directories were used for CGI scanning: http://ec2-34-233-47-30.compute-1.amazonaws.com/ http://ec2-34-233-47-30.compute-1.amazonaws.com/config http://ec2-34-233-47-30.compute-1.amazonaws.com/docs http://ec2-34-233-47-30.compute-1.amazonaws.com/dvwa http://ec2-34-233-47-30.compute-1.amazonaws.com/external While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards The following directories were excluded from CGI scanning because the "Regex pattern to exclude directories from CGI scanning" setting of the VT "Global variable settings" (OID: 1.3.6.1.4.1.25623.1.0.12288) for this scan was: "/(index\.php|image|img|css|js$|js/|javascript|style|theme|icon|jquery|graphic|grafik|picture|bilder|thumb nail|media/|skins?/)" http://ec2-34-233-47-30.compute-1.amazonaws.com/icons

Unique Alert ID: 539341 Found on: 2023-10-06 Severity: Info

Services (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This plugin performs service detection. This plugin attempts to guess which service is running on the remote port(s). For i nstance, it searches for a web server which could listen on another port than 80 or 443 and makes this information availa ble for other check routines.

Solution:

Result:

A web server is running on this port

Unique Alert ID: 539338 Found on: 2023-10-06 Severity: Info

Services (tcp/3306)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This plugin performs service detection. This plugin attempts to guess which service is running on the remote port(s). For i nstance, it searches for a web server which could listen on another port than 80 or 443 and makes this information availa ble for other check routines.

Solution:

Result:

A MySQL server is running on this port

Unique Alert ID: 539325 Found on: 2023-10-06 Severity: Info

HTTP Server type and version (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Solution:

Result:

The remote HTTP Server banner is: Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16 OpenSSL/1.0.2k-fips

Unique Alert ID: 539351 Found on: 2023-10-06 Severity: Info

SSL/TLS: Report Supported Cipher Suites (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This routine reports all SSL/TLS cipher suites accepted by a service. Notes: - As the VT 'SSL/TLS: Check Supported Cipher Suites' (OID: 1.3.6.1.4.1.25623.1.0.900234) might run into a timeout the actual reporting of all accepted cipher suites takes place in this VT instead. - SSLv2 ciphers are not getting reported as the protocol itself is deprecated, needs to be considered as weak and is reported separately as deprecated.

Solution:

Result:

'Strong' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_AES_256_CBC_SHA 'Medium' cipher suites accepted by this service via the TLSv1.0 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA No 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol. No 'Null' cipher suites accepted by this service via the TLSv1.0 protocol. No 'Anonymous' cipher suites accepted by this service via the TLSv1.0 protocol. 'Strong' cipher suites accepted by this service via the TLSv1.1 protocol: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA No 'Weak' cipher suites accepted by this service via the TLSv1.1 protocol. No 'Null' cipher suites accepted by this service via the TLSv1.1 protocol. No 'Anonymous' cipher suites accepted by this service via the TLSv1.1 protocol. 'Strong' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
'Medium' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA No 'Weak' cipher suites accepted by this service via the TLSv1.2 protocol. No 'Null' cipher suites accepted by this service via the TLSv1.2 protocol. No 'Anonymous' cipher suites accepted by this service via the TLSv1.2 protocol.

Unique Alert ID: 539322 Found on: 2023-10-06 Severity: Info

SSL/TLS: Certificate - Subject Common Name Does Not Match Server FQDN (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

The SSL/TLS certificate contains a common name (CN) that does not match the hostname.

Solution:

Result:

The certificate of the remote service contains a common name (CN) that does not match the hostname "ec2-34-233-47-30.compute-1.amazonaws.com". Certificate details: fingerprint (SHA-1) | 81C5AB98A9E8BECAEEB849E97EF47D7A14DCF936 fingerprint (SHA-256) | 635269291BDF6067EEDB2D40DB10B25C354D9FEA326F43779AE51D6C3FEB0FAB issued by | CN=Let's Encrypt Authority X3,O=Let's Encrypt,C=US public key algorithm | RSA public key size (bits) | 2048 serial | 0342FA98D61F9F34FD44E05EE95726E89BB3 signature algorithm | sha256WithRSAEncryption subject | CN=*.testapptrana.com subject alternative names (SAN) | *.testapptrana.com valid from | 2018-12-13 13:40:08 UTC valid until | 2019-03-13 13:40:08 UTC

Unique Alert ID: 539317 Found on: 2023-10-06 Severity: Info

SSL/TLS: Report Non Weak Cipher Suites (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This routine reports all Non Weak SSL/TLS cipher suites accepted by a service.

Solution:

Result:

'Non Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA 'Non Weak' cipher suites accepted by this service via the TLSv1.1 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA 'Non Weak' cipher suites accepted by this service via the TLSv1.2 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

Unique Alert ID: 539335 Found on: 2023-10-06 Severity: Info

SSH Server type and version (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This detects the SSH Server's type and version by connecting to the server and processing the buffer received. This information gives potential attackers additional information about the system they are attacking. Versions and Types should be omitted where possible.

Solution:

Result:

Remote SSH server banner: SSH-2.0-OpenSSH_6.6.1 Remote SSH supported authentication: publickey
Remote SSH text/login banner: (not available) This is probably: - OpenSSH Concluded from remote connection attempt with credentials: Login: OpenVASVT Password: OpenVASVT

Unique Alert ID: 539333 Found on: 2023-10-06 Severity: Info

OpenSSH Detection Consolidation (tcp)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

Consolidation of OpenSSH detections.

Solution:

Result:

Detected OpenSSH Server Version: 6.6.1 Location: 22/tcp CPE: cpe:/a:openbsd:openssh:6.6.1 Concluded from version/product identification result: SSH-2.0-OpenSSH_6.6.1

Unique Alert ID: 539326 Found on: 2023-10-06 Severity: Info

Traceroute (tcp)

Open Status: OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

Collect information about the network route and network distance between the scanner host and the target host. For internal networks, the distances are usually small, often less than 4 hosts between scanner and target. For public targets the distance is greater and might be 10 hosts or more.

Solution:

Result:

Network route from scanner (10.0.1.193) to target (34.233.47.30): 10.0.1.193 34.233.47.30 Network

distance between scanner and target: 2

Unique Alert ID: 539352 Found on: 2023-10-06 Severity: Info

PHP Detection (HTTP) (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

HTTP based detection of PHP.

Solution:

Result:

Detected PHP Version: 5.4.16 Location: 443/tcp CPE: cpe:/a:php:php:5.4.16 Concluded from version/product identification result: Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16 OpenSSL/1.0.2k-fips

Unique Alert ID: 539344 Found on: 2023-10-06 Severity: Info

PHP Detection (HTTP) (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

HTTP based detection of PHP.

Solution:

Result:

Detected PHP Version: 5.4.16 Location: 80/tcp CPE: cpe:/a:php:php:5.4.16 Concluded from version/product identification result: Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16 OpenSSL/1.0.2k-fips

Unique Alert ID: 539318 Found on: 2023-10-06 Severity: Info

SSL/TLS: Report Medium Cipher Suites (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This routine reports all Medium SSL/TLS cipher suites accepted by a service. Any cipher suite considered to be secure for only the next 10 years is considered as medium.

Solution:

Result:

'Medium' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA 'Medium' cipher suites accepted by this service via the TLSv1.1 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_RSA_WITH_CAMELLIA_256_CBC_SHA 'Medium' cipher suites
accepted by this service via the TLSv1.2 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

Unique Alert ID: 539343 Found on: 2023-10-06 Severity: Info

OS Detection Consolidation and Reporting (tcp)

Open Status: OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This script consolidates the OS information detected by several VTs and tries to find the best matching OS. Furthermore it reports all previously collected information leading to this best matching OS. It also reports possible additional informatio n which might help to improve the OS detection. If any of this information is wrong or could be improved please consider to report these to the referenced community forum.

Solution:

Result:

Best matching OS: OS: Red Hat Enterprise Linux CPE: cpe:/o:redhat:enterprise_linux Found by VT: 1.3.6.1.4.1.25623.1.0.111067 (Operating System (OS) Detection (HTTP)) Concluded from HTTP Server banner on port 80/tcp: Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16 OpenSSL/1.0.2k-fips Setting key "Host/runs_unixoide" based on this information Other OS detections (in order of reliability): OS: Red Hat Enterprise Linux CPE: cpe:/o:redhat:enterprise_linux Found by VT: 1.3.6.1.4.1.25623.1.0.111067 (Operating System (OS) Detection (HTTP)) Concluded from HTTP Server banner on port 443/tcp: Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16 OpenSSL/1.0.2k-fips

Unique Alert ID: 539332 Found on: 2023-10-06 Severity: Info

SSH Protocol Algorithms Supported (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This script detects which algorithms are supported by the remote SSH Service.

Solution:

Result:

The following options are supported by the remote ssh service: kex_algorithms: curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1 server_host_key_algorithms: ssh-rsa,ecdsa-sha2-nistp256,ssh-ed25519

encryption_algorithms_client_to_server: aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se
encryption_algorithms_server_to_client: aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se
mac_algorithms_client_to_server: hmac-md5-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-ripemd160-etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-md5-96-etm@openssh.com,hmac-md5,hmac-sha1,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
mac_algorithms_server_to_client: hmac-md5-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-ripemd160-etm@openssh.com,hmac-sha1-96-etm@openssh.com,hmac-md5-96-etm@openssh.com,hmac-md5,hmac-sha1,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
compression_algorithms_client_to_server: none,zlib@openssh.com
compression_algorithms_server_to_client: none,zlib@openssh.com

Unique Alert ID: 539331 Found on: 2023-10-06 Severity: Info

SSH Protocol Versions Supported (tcp/22)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

Identification of SSH protocol versions supported by the remote SSH Server. Also reads the corresponding fingerprints fr om the service. The following versions are tried: 1.33, 1.5, 1.99 and 2.0

Solution:

Result:

The remote SSH Server supports the following SSH Protocol Versions: 1.99 2.0 SSHv2 Fingerprint(s): ecdsa-sha2-nistp256: ca:f7:d0:03:26:7a:29:ec:7a:7e:46:c5:c0:ec:e1:6e ssh-ed25519: fa:e2:ef:60:00:85:ba:50:9f:dd:92:ef:35:10:19:4f ssh-rsa: 43:f7:2a:af:a7:fb:50:9c:ac:78:f1:20:1b:ef:ee:42

Unique Alert ID: 919593 Found on: 2023-10-06 Severity: Info

SSL/TLS: Version Detection (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-05-17
Cvss Base: 0.0
Cvss Score: 0.0

Description:

Enumeration and reporting of SSL/TLS protocol versions supported by a remote service.

Solution:

Result:

The remote SSL/TLS service supports the following SSL/TLS protocol version(s): TLSv1.0 TLSv1.1 TLSv1.2

Unique Alert ID: 539319 Found on: 2023-10-06 Severity: Info

SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Solution:

Result:

Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.0 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.1 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Unique Alert ID: 539323 Found on: 2023-10-06 Severity: Info

Services (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This plugin performs service detection. This plugin attempts to guess which service is running on the remote port(s). For i nstance, it searches for a web server which could listen on another port than 80 or 443 and makes this information availa ble for other check routines.

Solution:

Result:

A web server is running on this port

Unique Alert ID: 539345 Found on: 2023-10-06 Severity: Info

HTTP Security Headers Detection (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

All known security headers are being checked on the remote web server. On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Solution:

Result:

Missing Headers | More Information ----------

------- Content-Security-Policy | https://owasp.org/www-project-secure-headers/#content-security-policy Cross-Origin-Embedder-Policy | https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header Cross-Origin-Opener-Policy | https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header Cross-Origin-Resource-Policy | https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header Document-Policy | https://w3c.github.io/webappsec-feature-policy/document-policy#document-policy-http-header Feature-Policy | https://owasp.org/www-project-secure-headers/#feature-policy, Note: The Feature Policy header has been renamed to Permissions Policy Permissions-Policy | https://w3c.github.io/webappsec-feature-policy/#permissions-policy-http-header-field Referrer-Policy | https://owasp.org/www-project-secure-headers/#referrer-policy Sec-Fetch-Dest | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90 Sec-Fetch-Mode | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90 Sec-Fetch-Site | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90 Sec-Fetch-User | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90 X-Content-Type-Options | https://owasp.org/www-project-secure-headers/#x-content-type-options X-Frame-Options | https://owasp.org/www-project-secure-headers/#x-frame-options X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers/#x-permitted-cross-domain-policies X-XSS-Protection | https://owasp.org/www-project-secure-headers/#x-xss-protection, Note: Most major browsers have dropped / deprecated support for this header in 2020.

References:

- https://owasp.org/www-project-secure-headers/,https://owasp.org/www-project-secure-headers/#div-headers,https://securityheaders.com/

Unique Alert ID: 539346 Found on: 2023-10-06 Severity: Info

HTTP Security Headers Detection (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

All known security headers are being checked on the remote web server. On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.

Solution:

Result:

Missing Headers | More Information ----------

------- Content-Security-Policy | https://owasp.org/www-project-secure-headers/#content-security-policy Cross-Origin-Embedder-Policy | https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header Cross-Origin-Opener-Policy | https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header Cross-Origin-Resource-Policy | https://scotthelme.co.uk/coop-and-coep/, Note: This is an upcoming header Document-Policy | https://w3c.github.io/webappsec-feature-policy/document-policy#document-policy-http-header Feature-Policy | https://owasp.org/www-project-secure-headers/#feature-policy, Note: The Feature Policy header has been renamed to Permissions Policy Permissions-Policy | https://w3c.github.io/webappsec-feature-policy/#permissions-policy-http-header-field Referrer-Policy | https://owasp.org/www-project-secure-headers/#referrer-policy Sec-Fetch-Dest | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90 Sec-Fetch-Mode | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90 Sec-Fetch-Site | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90 Sec-Fetch-User | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90 X-Content-Type-Options | https://owasp.org/www-project-secure-headers/#x-content-type-options X-Frame-Options | https://owasp.org/www-project-secure-headers/#x-frame-options X-Permitted-Cross-Domain-Policies | https://owasp.org/www-project-secure-headers/#x-permitted-cross-domain-policies X-XSS-Protection | https://owasp.org/www-project-secure-headers/#x-xss-protection, Note: Most major browsers have dropped / deprecated support for this header in 2020.

References:

- https://owasp.org/www-project-secure-headers/,https://owasp.org/www-project-secure-headers/#div-headers,https://securityheaders.com/

Unique Alert ID: 539350 Found on: 2023-10-06 Severity: Info

CGI Scanning Consolidation (tcp/443)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

The script consolidates various information for CGI scanning. This information is based on the following scripts / settings: - HTTP-Version Detection (OID: 1.3.6.1.4.1.25623.1.0.100034) - No 404 check (OID: 1.3.6.1.4.1.25623.1.0.10386) - Web mirroring / webmirror.nasl (OID: 1.3.6.1.4.1.25623.1.0.10662) - Directory Scanner / DDI_Directory_Scanner.nasl (OID: 1.3.6.1.4.1.25623.1.0.11032) - The configured 'cgi_path' within the 'Scanner Preferences' of the scan config in use - The configured 'Enable CGI scanning', 'Enable generic web application scanning' and 'Add historic /scripts and /cgi-bin to directories for CGI scanning' within the 'Global variable settings' of the scan config in use If you think any of this information is wrong please report it to the referenced community forum.

Solution:

Result:

The Hostname/IP "ec2-34-233-47-30.compute-1.amazonaws.com" was used to access the remote host. Generic web application scanning is disabled for this host via the "Enable generic web application scanning" option within the "Global variable settings" of the scan config in use. Requests to this service are done via HTTP/1.1. This service seems to be able to host PHP scripts. This service seems to be NOT able to host ASP scripts. The User-Agent "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.4.0)" was used to access the remote host. Historic /scripts and /cgi-bin are not added to the directories used for CGI scanning. You can enable this again with the "Add historic /scripts and /cgi-bin to directories for CGI scanning" option within the "Global variable settings" of the scan config in use. The following directories were used for CGI scanning: http://ec2-34-233-47-30.compute-1.amazonaws.com/ While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

Unique Alert ID: 1010828 Found on: 2023-10-06 Severity: Info

SSL/TLS: Safe/Secure Renegotiation Support Status (tcp/443)

Open Status: Re-OPEN **First Found:** 2022-08-27
Cvss Base: 0.0
Cvss Score: 0.0

Description:

Checks and reports if a remote SSL/TLS service supports safe/secure renegotiation.

Solution:

Result:

Protocol Version | Safe/Secure Renegotiation Support Status ---------- SSLv3 | Unknown, Reason: Failed to open a socket to the remote service. TLSv1.0 | Unknown, Reason: Failed to open a socket to the remote service. TLSv1.1 | Unknown, Reason: Failed to open a socket to the remote service. TLSv1.2 | Unknown, Reason: Failed to open a socket to the remote service. TLSv1.3 | Unknown, Reason: Failed to open a socket to the remote service.

References:

- https://www.gnutls.org/manual/html_node/Safe-renegotiation.html,https://wiki.openssl.org/index.php/TLS1.3#Renegotiation,https://datatracker.ietf.org/doc/html/rfc5746

Unique Alert ID: 539324 Found on: 2023-10-06 Severity: Info

HTTP Server type and version (tcp/80)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

This script detects and reports the HTTP Server's banner which might provide the type and version of it.

Solution:

Result:

The remote HTTP Server banner is: Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16 OpenSSL/1.0.2k-fips

Unique Alert ID: 539337 Found on: 2023-10-06 Severity: Info

MariaDB / Oracle MySQL Detection (MySQL Protocol) (tcp/3306)

Open Status: Re-OPEN **First Found:** 2020-11-18
Cvss Base: 0.0
Cvss Score: 0.0

Description:

MySQL protocol-based detection of MariaDB / Oracle MySQL.

Solution:

Result:

Detected MariaDB Version: unknown Location: 3306/tcp CPE: cpe:/a:mariadb:mariadb Extra information: Scanner received a ER_HOST_NOT_PRIVILEGED error from the remote MariaDB server. Some tests may fail. Allow the scanner to access the remote MariaDB server for better results.

Unique Alert ID: 919595 Found on: 2023-10-06 Severity: Info

Apache HTTP Server Detection Consolidation (tcp)

Open Status: Re-OPEN **First Found:** 2022-05-17
Cvss Base: 0.0
Cvss Score: 0.0

Description:

Consolidation of Apache HTTP Server detections.

Solution:

Result:

Detected Apache HTTP Server Version: 2.4.6 Location: 443/tcp CPE: cpe:/a:apache:http_server:2.4.6 Concluded from version/product identification result: Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16 OpenSSL/1.0.2k-fips Detected Apache HTTP Server Version: 2.4.6 Location: 80/tcp CPE: cpe:/a:apache:http_server:2.4.6 Concluded from version/product identification result: Server: Apache/2.4.6 (Red Hat Enterprise Linux) PHP/5.4.16 OpenSSL/1.0.2k-fips