Weekly Zero-Day Vulnerability Coverage Bulletin

February 2021

Total Zero Day Vulnerabilities found: 16

Command Injection	Cross site request forgery	File Inclusion	Local Privilege	SQL Injection	Cross Site Scripting
4	4	3	1	2	2

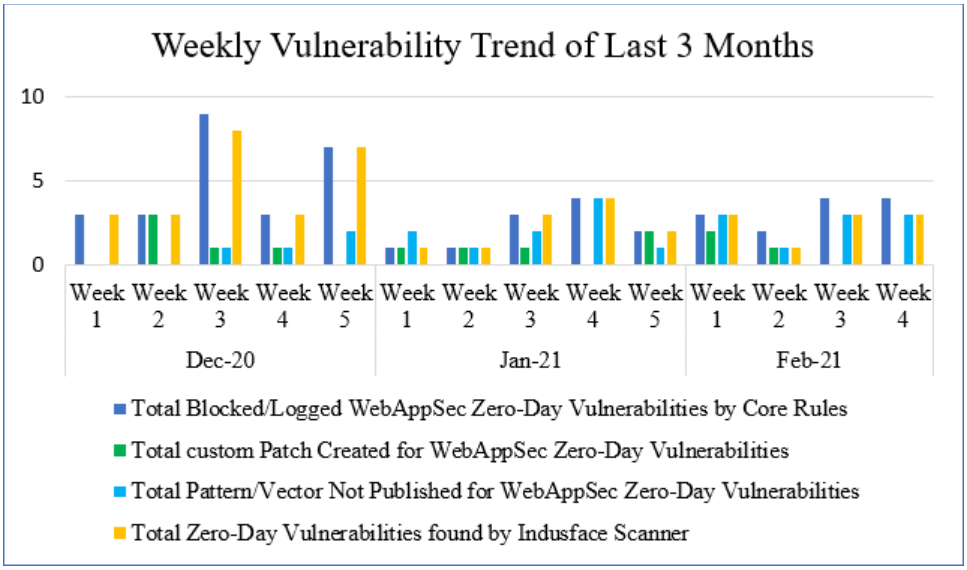
Zero-Day Vulnerabilities Protected through Core Rules	13
Zero-Day Vulnerabilities Protected through Custom Rules	3 *
Zero-Day Vulnerabilities for which protection cannot be determined	0 **
Zero-Day Vulnerabilities found by Indusface WAS	11

* To enable custom rules please contact support@indusface.com

** Since attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected.

Vulnerability Trend:

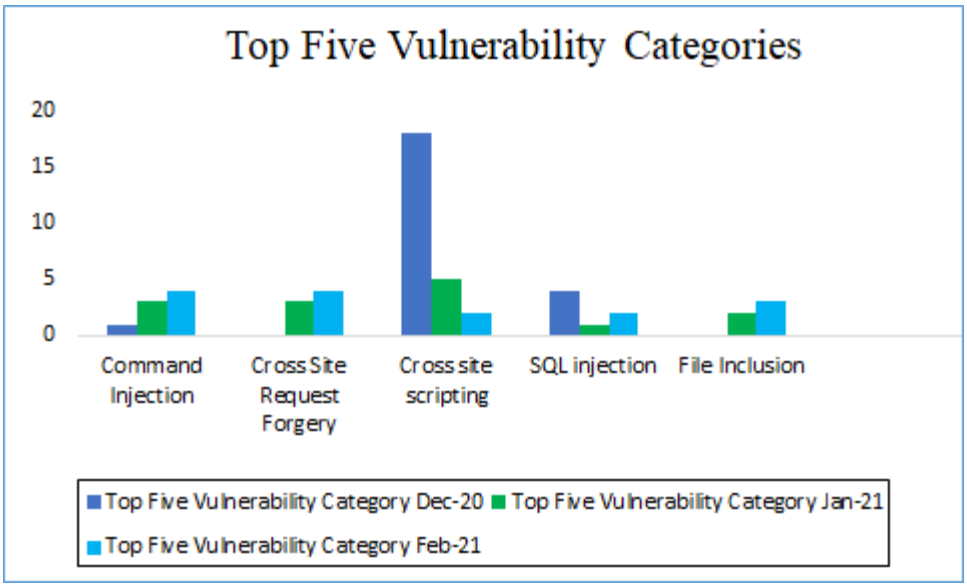
Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.



81% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

19% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

69% Of Zero-Day Vulnerabilities were reported by Indusface Scanner in last quarter



Note: Our Sig-Dev team constantly monitors the security landscape and leading security websites to identify any new vulnerabilities identified/published and monitors/updates rules to ensure around the clock protection for customer sites.

Vulnerability Details:

S. No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
1	Command Injection	CVE-2021-21015	Magento up to 2.3.6/2.4.0-p1/2.4.1 Customer Attribute os command injection	Magento versions 2.4.1 (and earlier), 2.4.0-p1 (and earlier) and 2.3.6 (and earlier) are vulnerable to an OS command injection via the customer attribute save controller. Successful exploitation could lead to arbitrary code execution by an authenticated attacker. Access to the admin console is required for successful exploitation.	Protected by core rules.	Detected by scanner as Command Injection attack.
		CVE-2021-23337	lodash Template command injection [CVE-2021-23337]	Lodash versions prior to 4.17.21 are vulnerable to Command Injection via the template function.	Protected by core rules.	Detected by scanner as Command Injection attack.

		CVE-2020-28431	wc-cmd index.js command injection	All versions of package wc-cmd are vulnerable to Command Injection via the index.js file. PoC: var a =require("wc-cmd"); a ("touch JHU")	Protected by core rules.	Detected by scanner as Command Injection attack.
		CVE-2020-28429	geojson2kml index.js command injection	All versions of package geojson2kml are vulnerable to Command Injection via the index.js file. PoC: var a =require("geojson2kml"); a("./","& touch JHU",function(){})	Protected by core rules.	Detected by scanner as Command Injection attack.
2	Cross Site Request Forgery	CVE-2020-24271	EasyCMS up to 1.6 cross-site request forgery [CVE-2020-24271]	A CSRF vulnerability was discovered in EasyCMS v1.6 that can add an admin account through index.php?s=/admin/rbacuser/insert/navTabId/rbacuser/callbackType/closeCurrent, then post username=***&password=***.	Protected by custom rules.	NA
		CVE-2021-24175	Critical 0-day in The Plus Addons for Elementor Allows Site Takeover	The Plus Addons for Elementor Page Builder WordPress plugin before 4.1.7 was being actively exploited to by malicious actors to bypass authentication, allowing unauthenticated users to log in as any user (including admin) by just providing the related username, as well as create accounts with arbitrary roles, such as admin. These issues can be exploited even if registration is disabled, and the	Protected by core rules.	NA

				Login widget is not active.		
		CVE-2021-21972, CVE-2021-21973	Critical RCE Flaws Affect VMware ESXi and vSphere Client	Critical RCE Flaws Affect VMware ESXi and vSphere Client — Patch Now	Protected by core rules.	NA
		CVE-2021-22986	Threat actors are attempting to exploit CVE-2021-22986 in F5 BIG-IP devices in the wild	On BIG-IP versions 16.0.x before 16.0.1.1, 15.1.x before 15.1.2.1, 14.1.x before 14.1.4, 13.1.x before 13.1.3.6, and 12.1.x before 12.1.5.3 amd BIG-IQ 7.1.0.x before 7.1.0.3 and 7.0.0.x before 7.0.0.2, the iControl REST interface has an unauthenticated remote command execution vulnerability. Note: Software versions which have reached End of Software Development (EoSD) are not evaluated.	Protected by core rules.	
3	File Inclusion	NA	Magento 2 PHP Credit Card Skimmer Saves to JPG	The following PHP code was found injected to the file ./vendor/magento/module-customer/Model/Session.php.	Protected by custom rules.	Detected by scanner as File Inclusion attack.
		CVE-2020-9050	Johnson Controls Metasys Reporting Engine up to 2.1 Web Services path traversal	Path Traversal vulnerability exists in Metasys Reporting Engine (MRE) Web Services which could allow a remote unauthenticated attacker to access and download arbitrary files from the system.	Protected by core rules.	Detected by scanner as File Inclusion attack.
		CVE-2021-26725	Nozomi Guardian/CMC up to 20.0.7.3 Web GUI path traversal	Path Traversal vulnerability when changing timezone using web GUI of Nozomi Networks Guardian, CMC allows an	Protected by core rules.	Detected by scanner as File Inclusion attack.

				authenticated administrator to read-protected system files. This issue affects: Nozomi Networks Guardian 20.0.7.3 version 20.0.7.3 and prior versions. Nozomi Networks CMC 20.0.7.3 version 20.0.7.3 and prior versions.		
4	Local Privilege Escalation	CVE-2020-28243	Why so salty? Local privilege escalation on SaltStack minions	An issue was discovered in SaltStack Salt before 3002.5. The minion's restartcheck is vulnerable to command injection via a crafted process name. This allows for a local privilege escalation by any user able to create a files on the minion in a non-blacklisted directory.	Protected by custom rules.	Detected by scanner as Local Privilege Escalation attack.
5	SQL Injection	CVE-2020-21179	koa2-blog 1.0.0 Signin Page name sql injection	Sql injection vulnerability in koa2-blog 1.0.0 allows remote attackers to Injecting a malicious SQL statement via the name parameter to the signin page.	Protected by core rules.	Detected by scanner as SQL Injection attack.
		CVE-2020-22425	Centreon 19.10-3.el7 sql injection [CVE-2020-22425]	Centreon 19.10-3.el7 is affected by a SQL injection vulnerability, where an authorized user is able to inject additional SQL queries to perform remote command execution.	Protected by core rules.	Detected by scanner as SQL Injection attack.

6	Cross Site Scripting	NA	Cross-Site Scripting Vulnerabilities in Elementor Impact Over 7 Million Sites	In the plugin, the accordion widget (includes/widgets/accordion.php) accepts a 'title_html_tag' parameter. Although the element control lists a fixed set of possible html tags, it is possible for a user with Contributor or above permissions to send a modified 'save_builder' request containing JavaScript in the 'title_html_tag' parameter, which is not filtered and is output without escaping. This JavaScript will then be executed when the saved page is viewed or previewed.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2020-13563	phpGACL 3.3.7 HTTP Request group_id cross site scripting	A cross-site scripting vulnerability exists in the template functionality of phpGACL 3.3.7. A specially crafted HTTP request can lead to arbitrary JavaScript execution. An attacker can provide a crafted URL to trigger this vulnerability in the phpGACL template group_id parameter.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.