Weekly Zero-Day Vulnerability Coverage Bulletin

July 20

Summary:

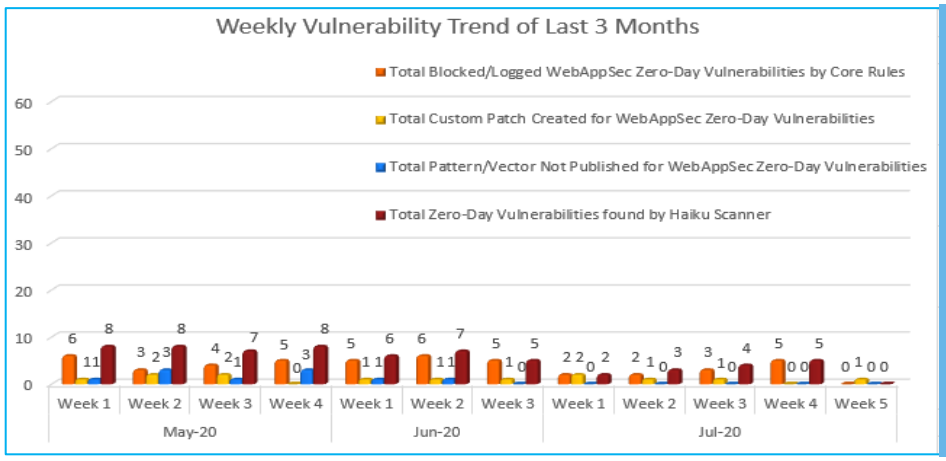
Total **17 Zero-Day Vulnerabilities** were discovered in **6 Categories** this month

5	1	1	7	2	1
Cross Site Scripting	URL Blocking	Enumeration Attack	Command Injection	Arbitrary File Upload	Local File Injection

Zero-Day Vulnerabilities Protected through Core Rules	12
Zero-Day Vulnerabilities Protected through Custom Rules	5*
Zero-Day Vulnerabilities for which protection cannot be determined	0**
Zero-Day Vulnerabilities found by Indusface WAS	13

* 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:

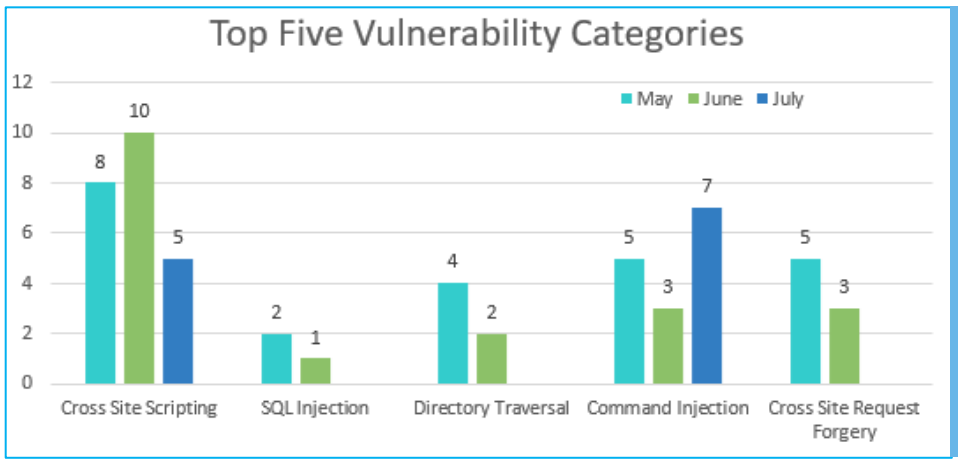


Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.

70% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

20% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

85% Of Zero-Day Vulnerabilities were reported by Haiku Scanner in last quarter



From the graph, we infer that maximum Cross Site Scripting vulnerabilities are discovered in June compared to other months.

Zero Cross Site Request Forgery and SQL Injection is found in July.

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.

Details:

S. No.	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
1.	Cross Site Scripting	NA	Newsletter Plugin Vulnerabilities Affect Over 300,000 Sites	While investigating recently patched vulnerability in Newsletter, a WordPress plugin with over 300,000 installations, discovered two additional, more serious vulnerabilities, including a reflected Cross-Site Scripting(XSS) vulnerability and a PHP Object Injection vulnerability. The Newsletter plugin includes a full-featured visual editor that can be used to create visually appealing newsletters and email campaigns. It uses an AJAX function, tnpc_render_callback, to display edited blocks based on a set of options sent in the AJAX request. Unfortunately, the vulnerable versions did not filter these options, but passed them onto a second function, restore_options_from_request which used multiple methods to decode options that were passed in before displaying them using the render_block function.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		NA	Asset CleanUp: Page Speed Booster	Multiple vulnerabilities in Asset CleanUp: Page Speed Booster caused by an improper handling of user input. This plugin has 80000 active installations. A successful attack can lead to malicious script execution.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		NA	XSS Flaw Impacting 100,000 Sites Patched in KingComposer	KingComposer is a WordPress plugin that allows Drag and Drop page building, and it registers a number of	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.

		AJAX actions to accomplish this. One of these AJAX actions was no longer actively used by the plugin but could still be used by sending a POST request to wp-admin/admin-ajax.php with the action parameter set to kc_install_online_preset. As such, if an attacker used base64-encoding on a malicious payload, and tricked a victim into sending a request containing this payload in the kc-online-preset-data parameter, the malicious payload would be decoded and executed in the victim's browser.		
NA	YOAST SEO Plugin	A stored cross-site scripting vulnerability was discovered in the past year by researchers in Yoast SEO plugin. The vulnerability allows attackers to inject a redirector script in the affected WordPress site. A patched version of this vulnerability was released under version 11.6 and the current updated version is 14.4.1.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
NA	WordPress All in One SEO Pack plugin	A stored cross-site scripting vulnerability was discovered last week in the popular WordPress All in One SEO Pack plugin. The vulnerability allows authenticated users to inject malicious scripts by accessing the wp-admin panel's "all posts" page. All versions of this plugin before version 3.6.1 are vulnerable. The patched version of this vulnerability was released on July 15, 2020, and the current updated version is 3.6.2.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.

2.	URL Blocking	NA	Plugin Payloads in Ongoing Malware Campaign	Several new IPs and domains added to an ongoing campaign. This malware is typically found to redirect visitors to various kinds of scam landing pages including tech support scams, fake lottery wins, and malicious browser notifications.	Protected by Custom Rules.	NA
3.	Enumeration Attack	NA	Zoom Security Exploit – Cracking private meeting passwords	Zoom meetings were default protected by a 6 digit numeric password, meaning 1 million maximum passwords. The discovered a vulnerability in the Zoom web client allowed checking if a password is correct for a meeting, due to broken CSRF and no rate limiting.	Protected by Custom Rules.	NA
4.	Command Injection	CVE-2020-1147	PoC Released for Critical CVE-2020-1147 flaw, SharePoint servers exposed to hack	CVE-2020-1147 is found in two .NET components (DataSet and DataTable) used to manage data sets, and affects Microsoft SharePoint, .NET Framework, and Visual Studio. The vulnerability is triggered when the software fails to check the source markup of XML file input. “An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the process responsible for deserialization of the XML content. To exploit this vulnerability, an attacker could upload a specially crafted document to a server utilizing an affected product to process content”.	Protected by Custom Rules.	Detected by scanner as Command Injection attack.
		NA	Adning Advertising	The paid plugin Adning Advertising, boasting over 8,800 license sales, fixed a remote code execution caused by poor file validation.	Protected by Default Rules.	Detected by scanner as Command Injection attack.

	NA	200K sites with buggy WordPress plugin exposed to wipe attacks (PageLayer is a WordPress plugin)	the two security flaws can be exploited by attackers to wipe WordPress sites running older unpatched versions of the plugin, as well as launch takeover attacks. "One flaw allowed any authenticated user with subscriber-level and above permissions the ability to update and modify posts with malicious content, amongst many other things," Wordfence explains. "A second flaw allowed attackers to forge a request on behalf of a site's administrator to modify the settings of the plugin which could allow for malicious JavaScript injection.	Protected by Default Rules.	Detected by scanner as Command Injection attack.
	CVE-2020-8194	Adventures in Citrix security research	Reflected code injection in Citrix ADC and Citrix Gateway versions before 13.0-58.30, 12.1-57.18, 12.0-63.21, 11.1-64.14 and 10.5-70.18 and Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows the modification of a file download.	Protected by Default Rules.	Detected by scanner as Command Injection attack.
	CVE-2020-9576	MAGENTO UP TO 1.9.4.4/1.14.4.4 /2.2.11/2.3.4 COMMAND INJECTION	A vulnerability, which was classified as critical, was found in Magento up to 1.9.4.4/1.14.4.4/2.2.11/2. 3.4. This affects some unknown processing. The manipulation with an unknown input leads to a privilege escalation vulnerability (Command Injection). CWE is classifying the issue as CWE-78. This is going to have an impact on confidentiality, integrity, and availability.	Protected by Default Rules.	Detected by scanner as Command Injection attack.
	CVE-2020-9578	MAGENTO UP TO 1.9.4.4/1.14.4.4 /2.2.11/2.3.4	A vulnerability was found in Magento up to 1.9.4.4/1.14.4.4/2.2.11/2. 3.4 and classified as critical. This issue affects	Protected by Default Rules.	Detected by scanner as Command Injection attack.

			COMMAND INJECTION	an unknown functionality. The manipulation with an unknown input leads to a privilege escalation vulnerability (Command Injection). Using CWE to declare the problem leads to CWE-78. Impacted is confidentiality, integrity, and availability. The weakness was released on 06/26/2020 as APSB20-22 as confirmed security bulletin (Website). The advisory is shared at helpx.adobe.com. The identification of this vulnerability is CVE-2020-9578 since 03/02/2020. The attack may be initiated remotely. No form of authentication is needed for a successful exploitation.		
		CVE-2020-9582	access-policy up to 3.1.0 eval Code Execution	A vulnerability classified as critical has been found in Magento up to 1.9.4.4/1.14.4.4/2.2.11/2.3.4. This affects an unknown code block. The manipulation with an unknown input leads to a privilege escalation vulnerability (Command Injection). CWE is classifying the issue as CWE-78. This is going to have an impact on confidentiality, integrity, and availability. The weakness was published 06/26/2020 as APSB20-22 as confirmed security bulletin (Website). The advisory is shared at helpx.adobe.com. This vulnerability is uniquely identified as CVE-2020-9582 since 03/02/2020. It is possible to initiate the attack remotely. No form of authentication is needed for exploitation.	Protected by Default Rules.	Detected by scanner as Command Injection attack.
5.	Arbitrary File Upload	NA	Critical Vulnerability	Recently discovered a vulnerability present in	Protected by Custom Rules.	NA

			Exposes over 700,000 Sites Using Divi, Extra, and Divi Builder	two themes by Elegant Themes, Divi and Extra, as well as Divi Builder, a WordPress plugin. Combined, these products are installed on an estimated 700,000 sites. This flaw gave authenticated attackers, with contributor-level or above capabilities, the ability to upload arbitrary files, including PHP files, and achieve remote code execution on a vulnerable site's server.		
		NA	Critical Wordpress plugin bug lets hackers take over hosting account (wpDiscuz)	Hackers can exploit a maximum severity vulnerability in the wpDiscuz plugin installed on over 70,000 WordPress sites to execute code remotely after uploading arbitrary files on servers hosting vulnerable sites. While wpDiscuz was designed to only allow using image attachments, the file mime type detection functions included in unpatched versions of the plugin and used to verify file types fail to block users from uploading arbitrary files like PHP files.	Protected by Custom Rules.	NA
6.	Local File Injection	CVE-2020-6287	PoC for CVE-2020-6287, CVE-2020-6286 (SAP RECON vulnerability)	This vulnerability resides inside SAP NetWeaver Java versions 7.30 to 7.50 (the latest version as of [our analysis publication]. All Support Packages tested to date were vulnerable. SAP NetWeaver is the base layer for several SAP products and solutions."An attacker leveraging this vulnerability will have unrestricted access to critical business information and processes in a variety of different scenarios. The bug affects	Protected by Default Rules.	Detected by scanner as Local File Injection attack.

		a default component present in every SAP application running the SAP NetWeaver Java technology stack. This technical component is used in many SAP business solutions, such as SAP S/4HANA, SAP SCM, SAP CRM, SAP CRM, SAP Enterprise Portal, SAP Solution Manager (SolMan) and many others.