Weekly Zero-Day Vulnerability Coverage Bulletin

July 2020

Total Zero Day Vulnerabilities found: 19

Command Injection	Arbitrary File Upload	URL Blocking	Local File Inclusion	Cross Site Scripting	Enumeration Attack
8	2	1	2	5	1

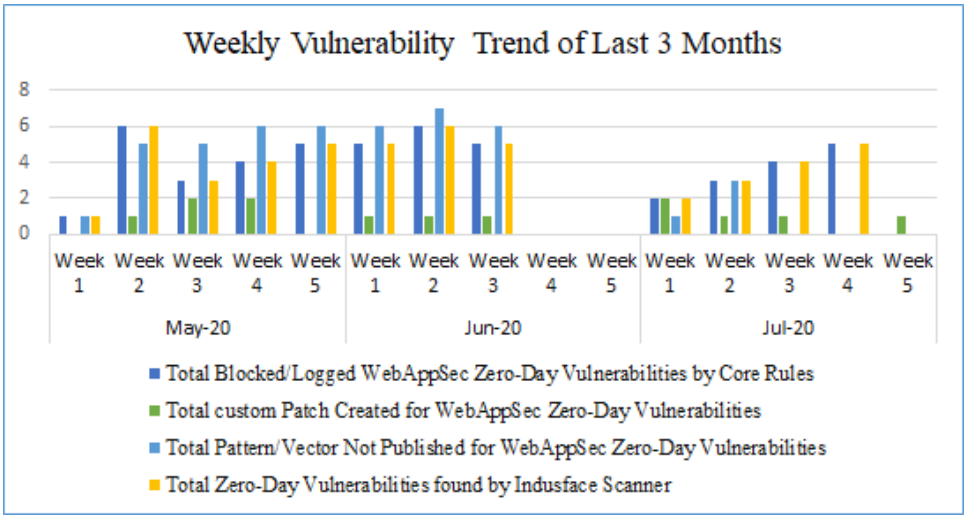
Zero-Day Vulnerabilities Protected through Core Rules	14
Zero-Day Vulnerabilities Protected through Custom Rules	5 *
Zero-Day Vulnerabilities for which protection cannot be determined	0 **
Zero-Day Vulnerabilities found by Indusface WAS	14

* 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:

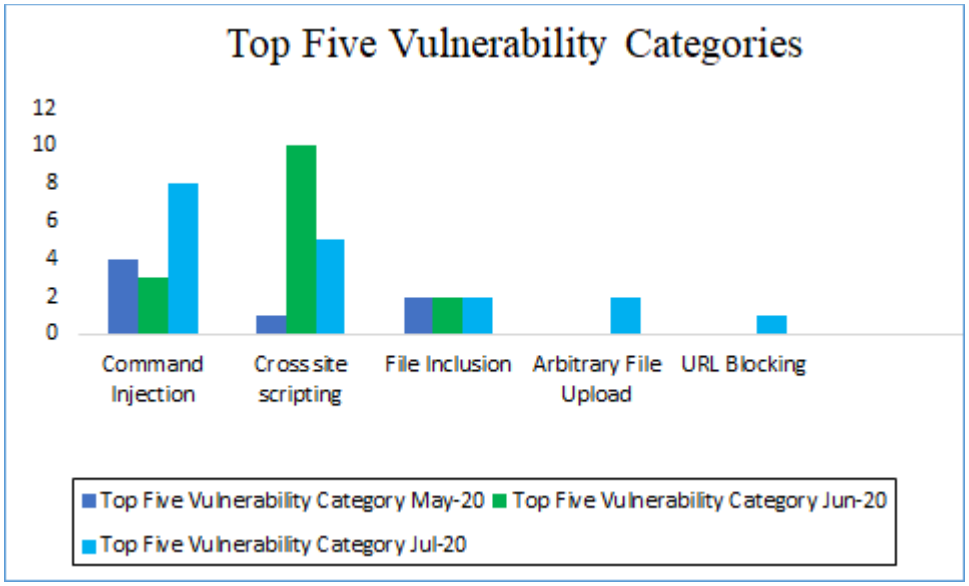
Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.



74% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

26% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

74% 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-2020-1147	PoC Released for Critical CVE-2020-1147 flaw, SharePoint servers exposed to hack	A remote code execution vulnerability exists in .NET Framework, Microsoft SharePoint, and Visual Studio when the software fails to check the source markup of XML file input, aka '.NET Framework, SharePoint Server, and Visual Studio Remote Code Execution Vulnerability'.	Protected by custom rules.	NA
		NA	Adning Advertising	This month, we detected a spike in the number of requests targeting old Joomla components. These types of attacks are	Protected by core rules.	Detected by scanner as Command Injection attack.

			fairly common, but we've seen an increase during this month. Successful attacks can lead to a full website compromise		
	CVE-2020-6110	Zoom client application chat code snippet remote code execution vulnerability	An exploitable partial path traversal vulnerability exists in the way Zoom Client version 4.6.10 processes messages including shared code snippets. A specially crafted chat message can cause arbitrary binary planting which could be abused to achieve arbitrary code execution. An attacker needs to send a specially crafted message to a target user or a group to trigger this vulnerability. For the most severe effect, target user interaction is required.	Protected by core rules.	Detected by scanner as Command Injection attack.
	NA	200K sites with buggy WordPress plugin exposed to wipe attacks (PageLayer is a WordPress plugin)	Two high severity security vulnerabilities found in the PageLayer plugin can let attackers to potentially wipe the contents or take over WordPress sites using vulnerable plugin versions.	Protected by core 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	Protected by core rules.	Detected by scanner as Command Injection attack.

		Citrix SDWAN WAN-OP versions before 11.1.1a, 11.0.3d and 10.2.7 allows the modification of a file download.		
CVE-2020-9576	MAGENTO UP TO 1.9.4.4/1.14.4.4/2.2.11/2.3.4 COMMAND INJECTION	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	Protected by core 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 COMMAND INJECTION	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	Protected by core rules.	Detected by scanner as Command Injection attack.
CVE-2020-9582	MAGENTO UP TO 1.9.4.4/1.14.4.4/2.2.11/2.3.4 COMMAND INJECTION	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	Protected by core rules.	Detected by scanner as Command Injection attack.

2	Arbitrary File Upload	NA	Critical Vulnerability Exposes over 700,000 Sites Using Divi, Extra, and Divi Builder	Elegant Themes is the creator behind one of the most popular premium themes, Divi. One of the features of the Divi theme is that it comes with the Divi Page Builder that makes the site design and editing process easy and customizable. In addition to the Divi theme, Elegant Themes offers an alternative theme, Extra, that includes the Divi Builder. The standalone Divi Builder plugin is also available and can be used with any theme. As part of the Divi Builder functionality, users that have the ability to create posts can import and export Divi page templates using the portability feature. Unfortunately, we discovered that although this feature used a client-side file type verification check, it was missing a server-side verification check. This flaw made it possible for authenticated attackers to easily bypass the JavaScript client-side check and upload malicious PHP files to a targeted website. An attacker could easily use a malicious file	Protected by custom rules.	NA

			uploaded via this method to completely take over a site.		
	NA	Critical WordPress plugin bug lets hackers take over hosting account (wpDiscuz)	The vulnerability was reported to wpDiscuz's developers by Wordfence's Threat Intelligence team on June 19 and was fully patched with the release of version 7.0.5 on July 23, after a failed attempt to fix the issue in version 7.0.4.	Protected by custom rules.	NA

3	URL Blocking	NA	Plugin Payloads in Ongoing Malware Campaign	Our team saw a number of 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
4	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. I discovered a vulnerability in the Zoom web client that allowed checking if a password is correct for a meeting, due to broken CSRF and no rate limiting.	Protected by custom rules.	NA

5	Local File Inclusion	CVE-2020-6287	PoC for CVE-2020-6287, CVE-2020-6286 (SAP RECON vulnerability)	SAP NetWeaver AS JAVA (LM Configuration Wizard), versions - 7.30, 7.31, 7.40, 7.50, does not perform an authentication check which allows an attacker without prior authentication to execute configuration tasks to perform critical actions against the SAP Java system, including the ability to create an administrative user, and therefore compromising Confidentiality, Integrity and Availability of the system, leading to Missing Authentication Check.	Protected by core rules.	Detected by scanner as Local File Inclusion attack.
		CVE-2020-6109	Zoom client application chat Giphy arbitrary file write (TALOS-2020-1055/CVE-2020-6109)	An exploitable path traversal vulnerability exists in the Zoom client, version 4.6.10 processes messages including animated GIFs. A specially crafted chat message can cause an arbitrary file write, which could potentially be abused to achieve arbitrary code execution. An attacker needs to send a specially crafted message to a target user or a group to exploit this vulnerability.	Protected by core rules.	Detected by scanner as Local File Inclusion attack.

6	Cross Site Scripting	NA	Newsletter Plugin Vulnerabilities Affect Over 300,000 Sites	we discussed 2 vulnerabilities in the Newsletter plugin, including a reflected XSS vulnerability and a PHP Object Injection vulnerability. We also explained what PHP Object Injection vulnerabilities are and how they can be exploited.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
		NA	Asset CleanUp: Page Speed Booster	Our team saw a number of 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 core 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 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.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
		NA	YOAST SEO Plugin	We have observed the scam campaign was hosted by exploiting the Yoast SEO plugin with different scam templates. A stored cross-site scripting	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.

			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.		
	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 core rules.	Detected by scanner as Cross Site Scripting attack.