INDUSFACE™

Weekly Zero-Day Vulnerability Coverage Bulletin

September 2020

Total Zero Day Vulnerabilities found: 19

Command Injection	DOS Attack	Memory Corruption	Privilege Escalation	Remote Code Execution	SQL Injection	XML-RPC	Cross Site Scripting
3	2	1	1	3	2	1	6

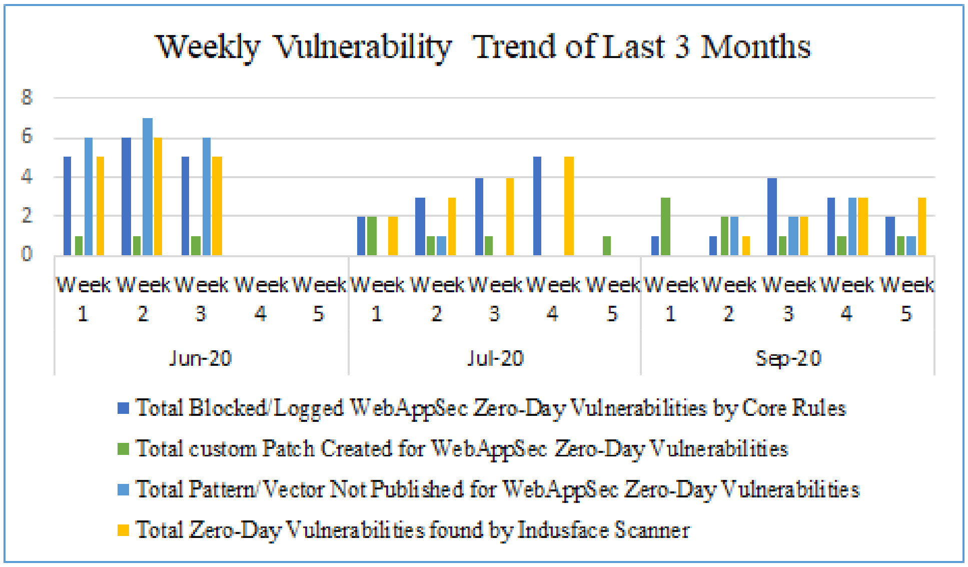
Zero-Day Vulnerabilities Protected through Core Rules	11
Zero-Day Vulnerabilities Protected through Custom Rules	8 *
Zero-Day Vulnerabilities for which protection cannot be determined	0 **
Zero-Day Vulnerabilities found by Indusface WAS	11

* 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:

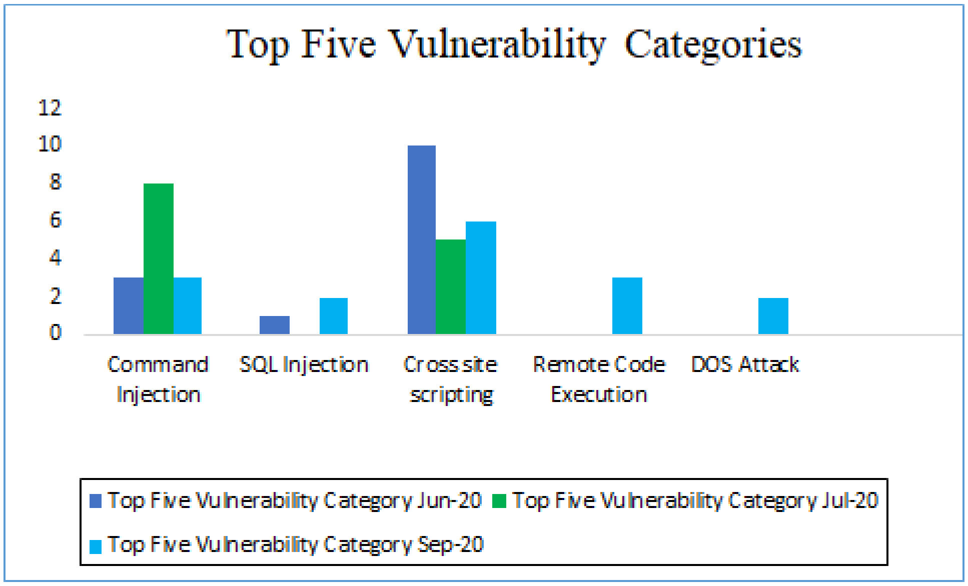
Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.



58% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

42% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

58% 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-2020-17496	Exploits in the Wild for vBulletin Pre-Auth RCE Vulnerability (CVE-2020-17496)	vBulletin 5.5.4 through 5.6.2 allows remote command execution via crafted subWidgets data in an ajax/render/widget_tabbedcontainer_tab_panel request. NOTE: this issue exists because of an incomplete fix for CVE-2019-16759.	Protected by core rules.	Detected by scanner as Command Injection attack.
		NA	Major Security Vulnerability Discovered in CMS System Used by US Army (Concrete5 CMS)	The content management system, Concrete5 CMS, contains a major vulnerability which has now been addressed in an updated version, according to an analysis published today by Edgescan.	Protected by core rules.	Detected by scanner as Command Injection attack.

		NA	Critical Vulnerabilities Patched in XCloner Backup and Restore Plugin ()	XCloner Backup and Restore is a plugin designed to provide WordPress users with easily customizable backups and simple-to-use restore functionality. Most of the plugin’s functionality is powered through the use of various AJAX actions that perform functionality without requiring the page to refresh every time.	Protected by core rules.	Detected by scanner as Command Injection attack.
2	DOS Attack	CVE-2019-0233	Apache Strusts 2 vulnerable to DOS	This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.	Protected by custom rules.	NA
		NA	Prototype Pollution to RCE	The NodeJS component **express-fileupload** – touting 7 million downloads from the npm registry – now has a critical Prototype Pollution vulnerability.	Protected by custom rules.	NA

3	Memory Corruption	CVE-2020-6519	Google Chrome prior 84.0.4147.89 Content Security Policy HTML Page privilege escalation	Policy bypass in CSP in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to bypass content security policy via a crafted HTML page.	Protected by custom rules.	NA
4	Local Privilege Escalation	CVE-2020-1472	Microsoft Windows up to Server 2019 Netlogon privilege escalation	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.	Protected by custom rules.	NA
5	Remote Code Execution	CVE-2019-0752	Script-Based Malware through Internet Explorer Exploits (CVE-2019-0752)	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0739, CVE-2019-0753, CVE-2019-0862.	Protected by custom rules.	NA
		NA	700,000 WordPress Users Affected by Zero-Day Vulnerability in File Manager Plugin	Both Wordfence Premium users and sites still running the free version of Wordfence have been protected against attacks targeting this vulnerability due to the Wordfence firewall's built-in File Upload protection.	Protected by custom rules.	NA

		CVE-2019-0230	PoC exploit code for two Apache Struts 2 flaws available online (CVE-2019-0230 and CVE-2019-0233)	Apache Struts 2.0.0 to 2.5.20 forced double OGNL evaluation, when evaluated on raw user input in tag attributes, may lead to remote code execution.	Protected by custom rules.	NA
6	SQL Injection	CVE-2020-27615	SQL Injection Vulnerability in WordPress Loginizer Plugin Affected Over One Million Sites	The Loginizer plugin before 1.6.4 for WordPress allows SQL injection (with resultant XSS), related to loginizer_login_failed and lz_valid_ip.	Protected by core rules.	Detected by scanner as SQL Injection attack.
		NA	63 billion credential stuffing attacks hit retail, hospitality, travel industries	Akamai published a report detailing criminal activity targeting the retail, travel, and hospitality industries with attacks of all types and sizes between July 2018 and June 2020. The report also includes numerous examples of criminal ads from the darknet illustrating how they cash in on the results from successful attacks and the corresponding data theft.	Protected by core rules.	Detected by scanner as SQL Injection attack.

7	XML – RPC	NA	Malware Leveraging XML-RPC Vulnerability to Exploit WordPress Sites	XML-RPC on WordPress, which is enabled by default, is actually an API that provides third-party applications and services the ability to interact with WordPress sites, rather than through a browser. Attackers use this channel to establish a remote connection to a WordPress site and make modifications without being directly logged in to your WordPress system. However, if a WordPress site didn't disable XML-RPC, there is no limit to the number of login attempts that can be made by a hacker, meaning it is just a matter of time before a cybercriminal can gain access.	Protected by custom rules.	NA
8	Cross Site Scripting	NA	Over 30 Vulnerabilities Discovered Across 20 CMS Products (XSS and server-side template injection (SSTI) attacks)	Researchers have identified more than 30 vulnerabilities across 20 popular content management systems (CMS), including Microsoft SharePoint and Atlassian Confluence.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
		NA	WordPress WooCommerce stores under attack, patch now	Hackers are actively targeting and trying to exploit SQL injection, authorization issues, and unauthenticated stored cross-site scripting (XSS) security vulnerabilities in the	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.

		Discount Rules for WooCommerce WordPress plugin with more than 30,000 installations		
CVE-2020-12648	TinyMCE up to 5.2.1 Classic Editing Mode cross site scripting	A cross-site scripting (XSS) vulnerability in TinyMCE 5.2.1 and earlier allows remote attackers to inject arbitrary web script when configured in classic editing mode.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
SA-CORE-2020-007	Drupal core - Moderately critical - Cross-site scripting - SA-CORE-2020-007	The Drupal AJAX API does not disable JSONP by default, which can lead to cross-site scripting.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
SA-CORE-2020-009	Drupal core - Critical - Cross-site scripting - SA-CORE-2020-009	Drupal 8 and 9 have a reflected cross-site scripting (XSS) vulnerability under certain circumstances. An attacker could leverage the way that HTML is rendered for affected forms in order to exploit the vulnerability.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
SA-CORE-2020-010	Drupal core - Moderately critical - Cross-site scripting - SA-CORE-2020-010	Drupal core's built-in CKEditor image caption functionality is vulnerable to XSS.	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.