Weekly Zero-Day Vulnerability Coverage Bulletin

November 2020

Total Zero Day Vulnerabilities found: 17

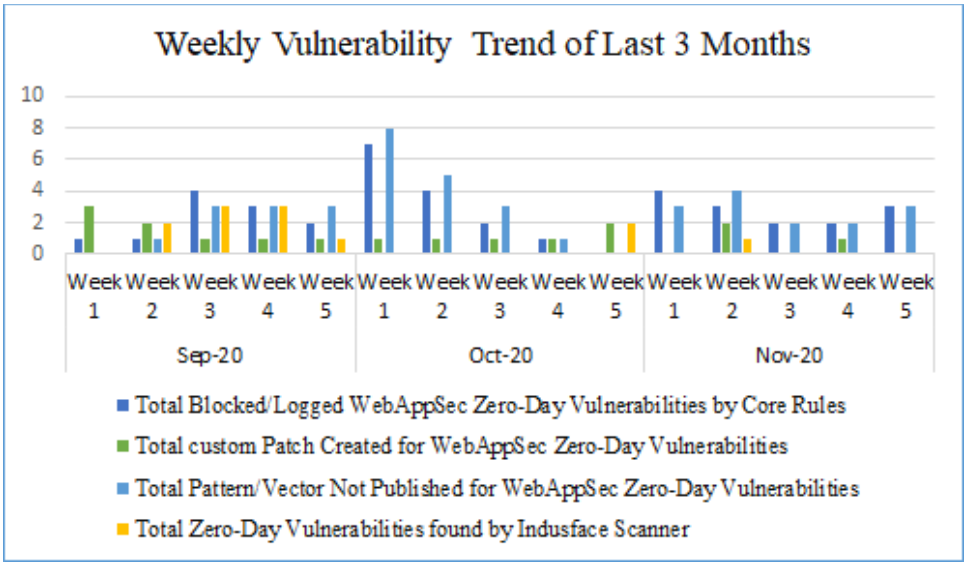
Content-type log exception	Directory Traversal	Injection Attack	WordPress	SQL Injection	Cross Site Scripting
1	1	2	1	8	4

Zero-Day Vulnerabilities Protected through Core Rules	14
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	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:

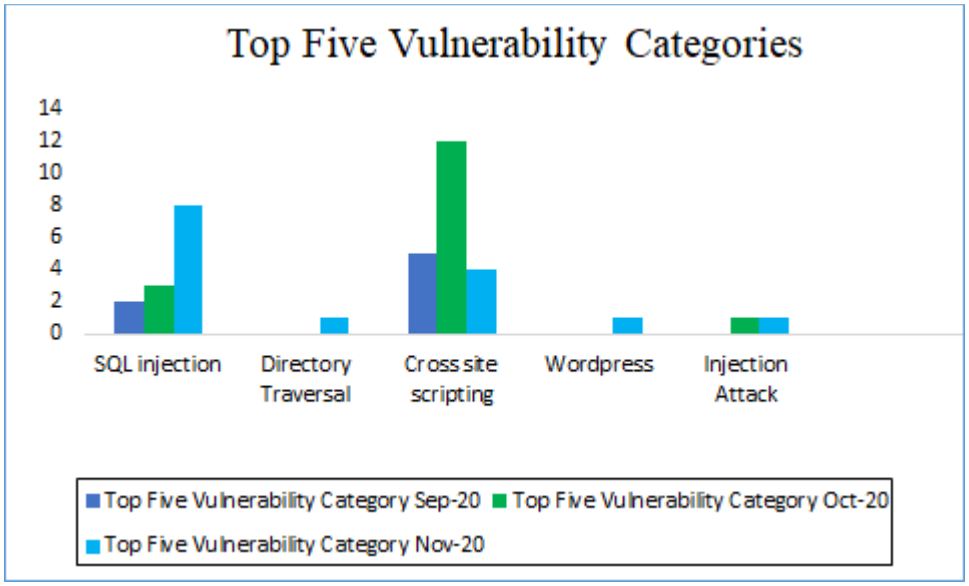
Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.



82% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

18% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

82% 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	Injection Attack	CVE-2020-4006	VMware Workspace ONE Access and related components are vulnerable to command injection	VMware Workspace One Access, Access Connector, Identity Manager, and Identity Manager Connector address have a command injection vulnerability.	Protected by Custom rules.	NA
2	Content-type Log exception	NA	Critical Vulnerabilities Patched in Quiz and Survey Master Plugin	On July 17, 2020, our Threat Intelligence team discovered two vulnerabilities in Quiz and Survey Master (QSM), a WordPress plugin installed on over 30,000 sites. These flaws made it possible for unauthenticated attackers to upload arbitrary files and achieve remote code execution, as well as delete arbitrary files like a site's wp-config.php file which could effectively take a site offline and allow an attacker to take over the vulnerable site.	Protected by core rules.	Detected by scanner as Content-type log exception
3	Directory Traversal/File Inclusion	CVE-2020-17527	Apache Tomcat 10.0.0-M1 to 10.0.0-M9	Apache Tomcat HTTP/2 Request header mix-up	Protected by core rules.	Detected by scanner as Directory Traversal attack.

4	Injection Attack	CVE-2020-7699	NodeJS module downloaded 7M times lets hackers inject code	This affects the package express-fileupload before 1.1.8. If the parseNested option is enabled, sending a corrupt HTTP request can lead to denial of service or arbitrary code execution.	Protected by custom rules.	NA
5	SQL Injection	CVE-2018-19952	QNAP Music Station up to 5.1.12/5.2.8/5.3.10 SQL Injection sql injection	QNAP Music Station up to 5.1.12/5.2.8/5.3.10 SQL Injection sql injection	Protected by core rules.	Detected by scanner as SQL Injection attack.
		CVE-2020-2312	Jenkins SQLPlus Script Runner Plugin up to 2.0.12 Command Line Argument insufficiently protected credentials	Jenkins SQLPlus Script Runner Plugin up to 2.0.12 Command Line Argument insufficiently protected credentials	Protected by core rules.	Detected by scanner as SQL Injection attack.
		CVE-2020-12147	Silver Peak Unity Orchestrator up to 8.9.10/8.10.10/9.0.0 REST API /sqlExecution path traversal	Silver Peak Unity Orchestrator up to 8.9.10/8.10.10/9.0.0 REST API /sqlExecution path traversal	Protected by core rules.	Detected by scanner as SQL Injection attack.
		CVE-2020-24400	Magento up to 2.3.5/2.4.0 sql injection [CVE-2020-24400]	Magento up to 2.3.5/2.4.0 sql injection [CVE-2020-24400]	Protected by core rules.	Detected by scanner as SQL Injection attack.
		CVE-2020-13877	ResourceXpress Meeting Monitor 4.9 sql injection [CVE-2020-13877]	ResourceXpress Meeting Monitor 4.9 sql injection [CVE-2020-13877]	Protected by core rules.	Detected by scanner as SQL Injection attack.
		CVE-2020-5659	XooNIps up to 3.49 sql injection	XooNIps up to 3.49 sql injection [CVE-2020-5659]	Protected by core rules.	Detected by scanner as SQL Injection attack.
		CVE-2020-25694	PostgreSQL up to 13.0 Client	PostgreSQL up to 13.0 Client	Protected by core rules.	Detected by scanner as

			Application downgrade	Application downgrade		SQL Injection attack.
		CVE-2020-25475	SimplePHPscripts News Script PHP Pro 2.3 News Edit id sql injection	SimplePHPscripts News Script PHP Pro 2.3 News Edit id sql injection	Protected by core rules.	Detected by scanner as SQL Injection attack.
6	WordPress	NA	Zero-day in WordPress SMTP plugin abused to reset admin account passwords	Zero-day in WordPress SMTP plugin abused to reset admin account passwords	Protected by custom rules.	NA
7	Cross Site Scripting	NA	Critical Privilege Escalation Vulnerabilities Affect 100K Sites Using Ultimate Member Plugin	Panagiotis Vagenas, a Wordfence Security Researcher, has discovered a reflected cross site scripting vulnerability in the Easy Forms for MailChimp plugin for WordPress. There are over 40,000 active installations according to wordpress.org. We shared the details of the vulnerability with the author on Monday and they released version 6.1.3 on Tuesday, which includes a fix for the vulnerability	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
		NA	Reflected XSS in PageLayer Plugin Affects Over 200,000 WordPress Sites	Reflected XSS in PageLayer Plugin Affects Over 200,000 WordPress Sites	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.
		NA	Large-Scale Attacks Target Epsilon Framework Themes	Large-Scale Attacks Target Epsilon Framework Themes	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.

	NA	Important, Spoofing" - zero-click, wormable, cross-platform remote code execution in Microsoft Teams	MS teams RCE	Protected by core rules.	Detected by scanner as Cross Site Scripting attack.