Weekly Zero-Day Vulnerability Coverage Bulletin

(30th December – 5th January)

Summary:

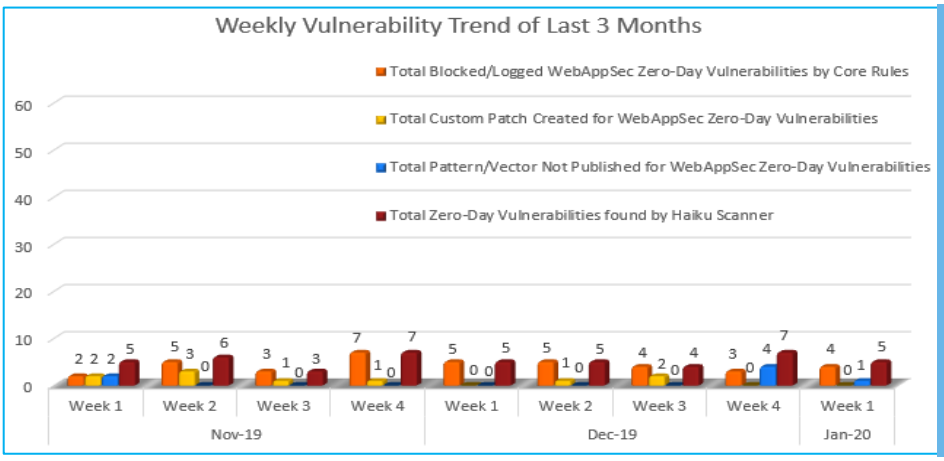
Total **5 Zero-Day Vulnerabilities** were discovered in **4 Categories** this week

2	1	1	1
SQL Injection	Redirection	Command Injection	Cross Site Scripting

Zero-Day Vulnerabilities Protected through Core Rules	4
Zero-Day Vulnerabilities Protected through Custom Rules	0*
Zero-Day Vulnerabilities for which protection cannot be determined	1**
Zero-Day Vulnerabilities found by Haiku Scanner	5

* 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:

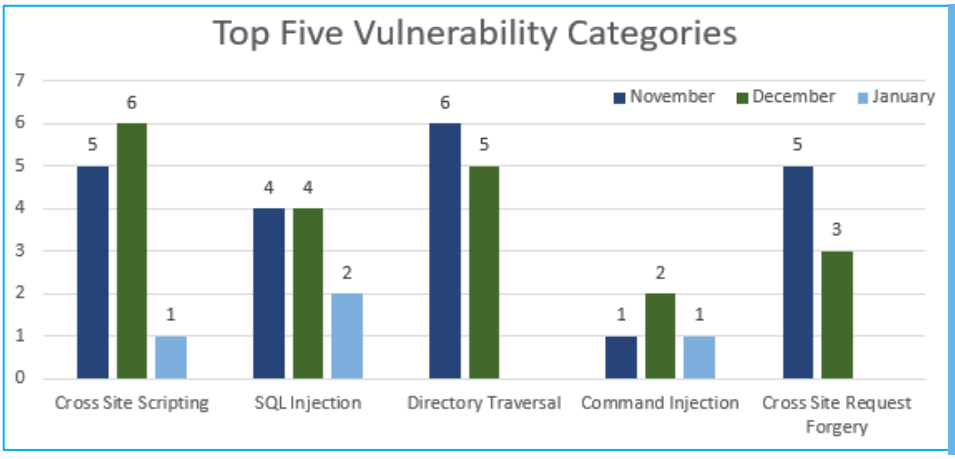


Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.

40% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

11% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

49% Of Zero-Day Vulnerabilities were reported by Haiku Scanner in last quarter



From the graph, we infer that maximum Cross Site Scripting and Directory Traversal vulnerabilities are discovered in December and November respectively.

Zero Cross Site Request Forgery is found in January so far.

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	Haiku Scanner Coverage
1.	SQL Injection	CVE-2019-7478	GMS up to 9.1 Webservice Module sql injection	A vulnerability classified as critical was found in GMS up to 9.1. This vulnerability affects an unknown part of the component Webservice Module. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
		CVE-2019-20218	SQLite 3.30.1 select.c selectExpander sql injection	A vulnerability was found in SQLite 3.30.1. It has been classified as critical. This affects the function <code>selectExpander</code> of the file select.c. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
2.	Redirection	NA	Thousands of WordPress Sites Hacked to Fuel Scam Campaign - "CP Contact Form with PayPal" and the "Simple Fields" plugins	When exploited, the vulnerabilities allow the attackers to inject JavaScript that loads scripts from admarketlocation[.]com and gotosecond2[.]com directly into the site's theme.	NA	Detected by scanner as Redirection attack.
3.	Command Injection	CVE-2019-10774	php-shellcommand up to 1.6.0 command injection [CVE-2019-10774]	A vulnerability, which was classified as critical, was found in php-shellcommand up to 1.6.0 (Programming Language Software). Affected is an unknown code. Upgrading to version 1.6.1 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Command Injection attack.
4.	Cross Site Scripting	CVE-2019-20058	Bolt 3.7.0 Symfony Web Profiler search cross site scripting	A vulnerability, which was classified as problematic, was found in Bolt 3.7.0. This affects an unknown functionality of the	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.

		component Symfony Web Profiler. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.