Weekly Zero-Day Vulnerability Coverage Bulletin

(20th January – 26th January)

Summary:

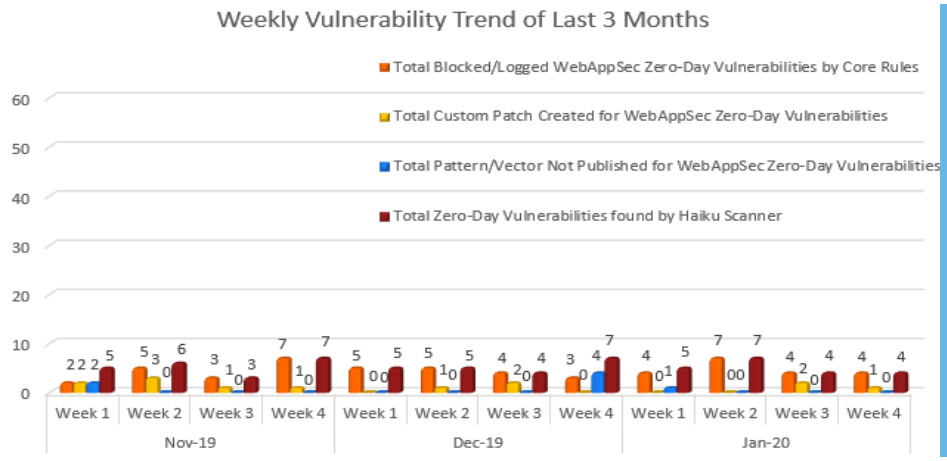
Total **5** Zero-Day Vulnerabilities were discovered in **4** categories this week

1	2	1	1
Cross Site Scripting	SQL Injection	Directory Traversal	Cross Site Request Forgery

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

* 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:

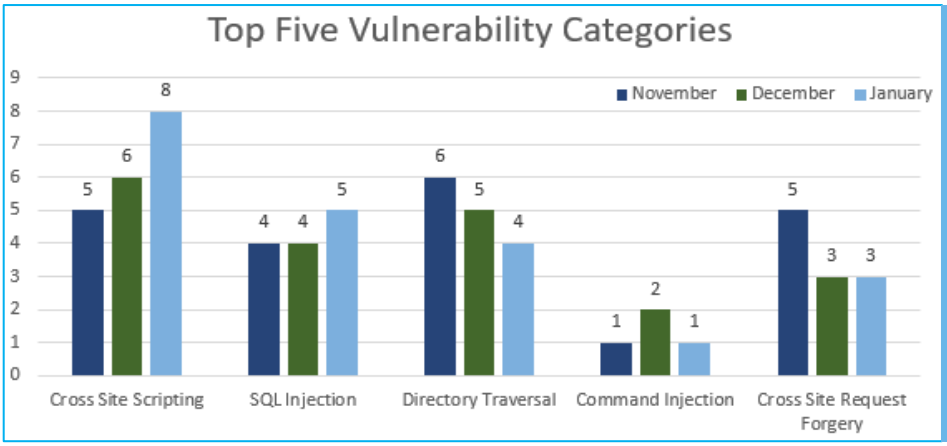


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

38% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

9% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

47% 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 January compared to other months.

Only 1 Command Injection attack is discovered in November and January compared to other months and categories.

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.	Cross Site Scripting	CVE-2019-6146	Forcepoint Web Security 8.x Header Host cross site scripting	A vulnerability, which was classified as problematic, has been found in Forcepoint Web Security 8.x (Anti-Malware Software). Affected by this issue is an unknown code of the component Header Handler. 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 Cross Site Scripting attack.
2.	SQL Injection	CVE-2019-17357	Cacti up to 1.2.7 graphs.php template_id sql injection	A vulnerability was found in Cacti up to 1.2.7 (Log Management Software). It has been declared as critical. This vulnerability affects an unknown code block of the file graphs.php. 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-2020-7939	Plone up to 5.2.1 DTML sql injection	A vulnerability was found in Plone up to 5.2.1 (Content Management System). It has been classified as critical. This affects an unknown code of the component DTML. 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.

3.	Directory Traversal	CVE-2020-7211	libslirp 4.1.0 on Windows tftp.c directory traversal	A vulnerability was found in libslirp 4.1.0 on Windows and classified as critical. Affected by this issue is an unknown code of the file tftp.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 Directory Traversal attack.
4.	Cross Site Request Forgery	CVE-2019-16513	ConnectWise Control 19.3.25270.7185 API Request cross site request forgery	A vulnerability was found in ConnectWise Control 19.3.25270.7185 (Network Management Software). It has been declared as problematic. This vulnerability affects an unknown code. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Custom Rules.	NA