Weekly Zero-Day Vulnerability Coverage Bulletin

(24th February – 1st March)

Summary:

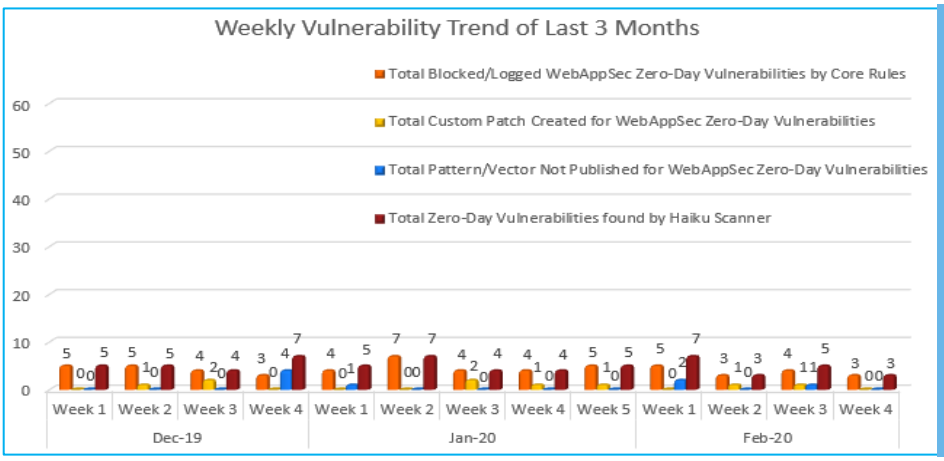
Total **3** Zero-Day Vulnerabilities were discovered in **2** Categories this week

1	2
Directory Traversal	Command Injection

Zero-Day Vulnerabilities Protected through Core Rules	3
Zero-Day Vulnerabilities Protected through Custom Rules	0*
Zero-Day Vulnerabilities for which protection cannot be determined	0**
Zero-Day Vulnerabilities found by Haiku Scanner	3

* 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:

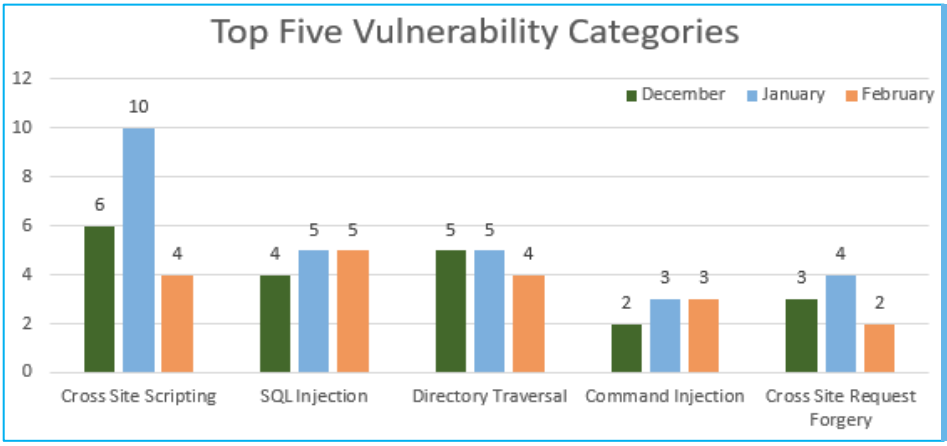


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

43% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

7% 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 vulnerabilities are discovered in January compared to other months.

Five Vulnerabilities are found for SQL Injection & Directory Traversal in both December & January months.

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.	Directory Traversal	CVE-2020-5187	DNN up to 9.4.4 directory traversal [CVE-2020-5187]	A vulnerability classified as critical was found in DNN up to 9.4.4. This vulnerability affects an unknown function. 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.
2.	Command Injection	CVE-2019-18182	Pacman up to 5.1 conf.c download_with_xfercommand() command injection	A vulnerability, which was classified as critical, has been found in Pacman up to 5.1. This issue affects the function <code>download_with_xfercommand()</code> of the file conf.c. Upgrading to version 5.2 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Command Injection attack.
		CVE-2020-9381	Total.js CMS 13 POST Request controllers/admin.js Remote Code Execution	A vulnerability was found in Total.js CMS 13 (JavaScript Library). It has been classified as critical. Affected is an unknown function of the file controllers/admin.js of the component POST Request 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 Command Injection attack.