Weekly Zero-Day Vulnerability Coverage Bulletin

(17th February – 23rd February)

Summary:

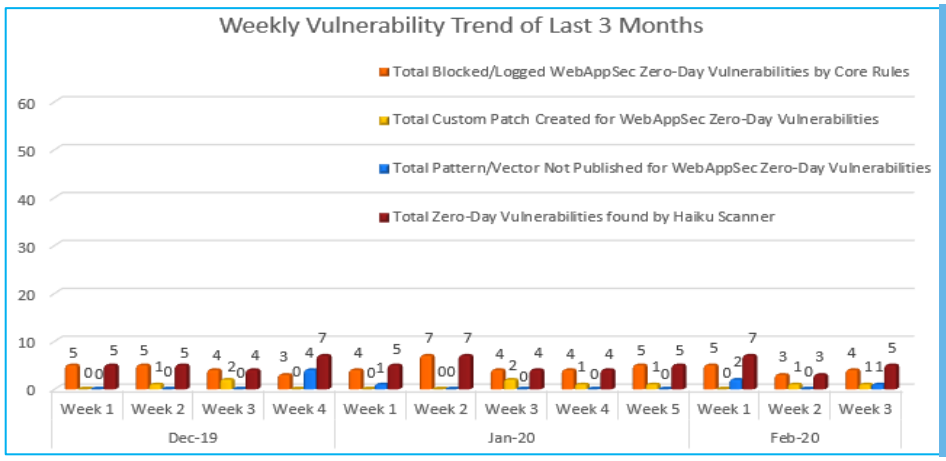
Total **6** Zero-Day Vulnerabilities were discovered in **5** Categories this week

1	2	1	1	1
SQL Injection	Directory Traversal	Redirection	Cross Site Request Forgery	Command Injection

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	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:

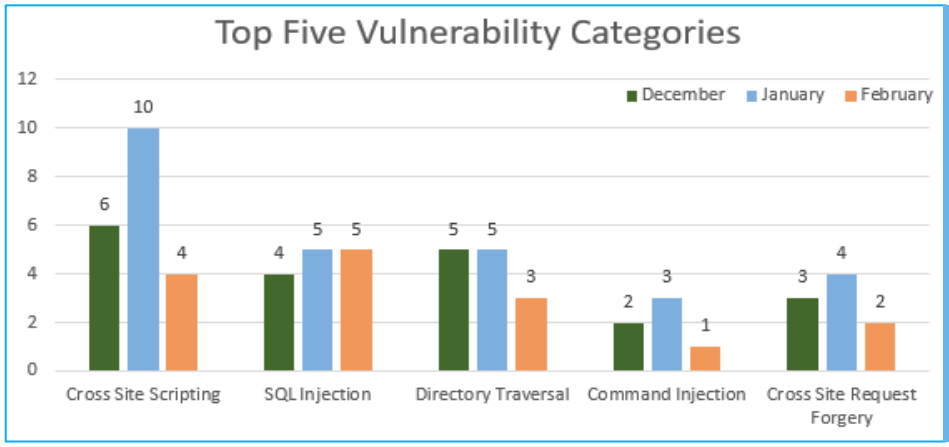


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

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.

Single Command Injection attack is discovered in February 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-2020-9340	fauzantrif eLection 2.0 op_kandidat.ph p id sql injection	A vulnerability was found in fauzantrif eLection 2.0. It has been classified as critical. Affected is some unknown functionality of the file admin/ajax/op_kandidat.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.
2.	Directory Traversal	CVE-2020-8996	AnyShare Cloud 6.0.9 filepath directory traversal	A vulnerability has been found in AnyShare Cloud 6.0.9 (Cloud Software) and classified as problematic. This vulnerability affects some unknown functionality of the file interface/downloadwithpath/downloadfile/. 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.
		CVE-2020-9354	SmartClient 12.0 Remote Procedure Call developerConsoleOperations.jsp directory traversal	A vulnerability has been found in SmartClient 12.0 and classified as critical. Affected by this vulnerability is some unknown functionality of the file /tools/developerConsoleOperations.jsp of the component Remote Procedure Call. 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.
3.	Command Injection	CVE-2020-1790	GaussDB 200 6.5.1 command injection [CVE-2020-1790]	A vulnerability was found in GaussDB 200 6.5.1. It has been declared as critical. Affected by this	Protected by Default Rules.	Detected by scanner as Command

				vulnerability is an unknown part. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.		Injection attack.
4.	Cross Site Request Forgery	CVE-2020-5530	Easy Property Listings up to 3.3 cross site request forgery [CVE-2020-5530]	A vulnerability was found in Easy Property Listings up to 3.3. It has been classified as problematic. This affects an unknown code. Upgrading to version 3.4 eliminates this vulnerability.	Protected by Custom Rules.	NA
5.	Redirection	CVE-2019-20479	mod_auth_openidc up to 2.4.0 Open Redirect [CVE-2019-20479]	A vulnerability was found in mod_auth_openidc up to 2.4.0. It has been classified as problematic. Affected is an unknown code. Upgrading to version 2.4.1 eliminates this vulnerability.	NA	Detected by scanner as Redirection attack.