Weekly Zero-Day Vulnerability Coverage Bulletin

(10th February – 16th February)

Summary:

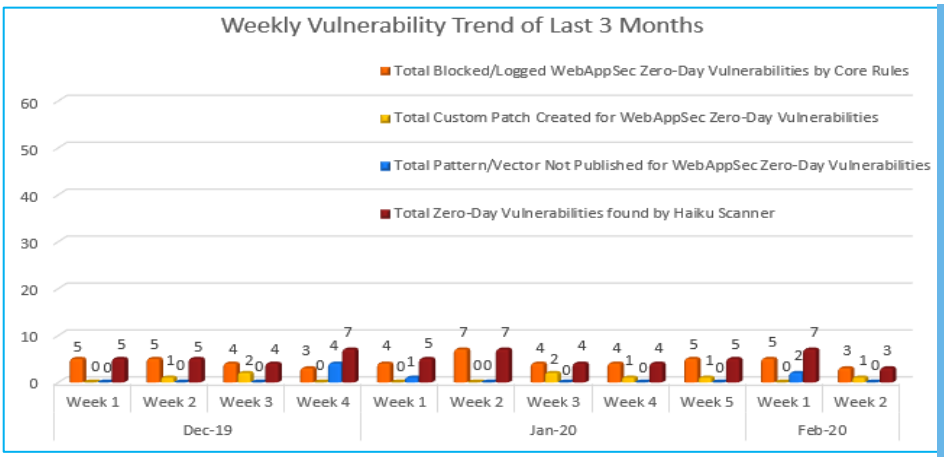
Total **4** Zero-Day Vulnerabilities were discovered in **3** Categories this week

2	**1**	**1**
Cross Site Scripting	SQL Injection	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	3
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	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:

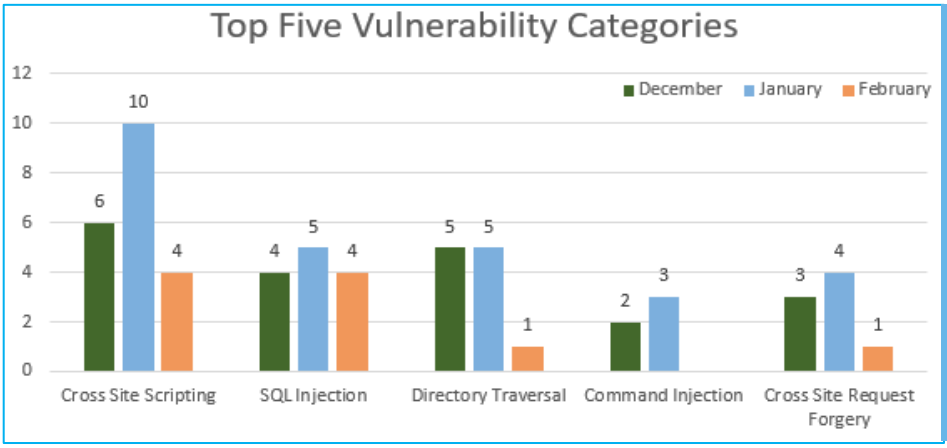


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

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

50% 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.

Zero 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.	Cross Site Scripting	CVE-2020-5241	matestack-ui-core up to 0.7.3 cross site scripting [CVE-2020-5241]	A vulnerability was found in matestack-ui-core up to 0.7.3 and classified as problematic. Affected by this issue is an unknown code. Upgrading to version 0.7.4 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2019-13965	Combodo iTop up to 2.6.0 webservices/export.php param_file cross site scripting	A vulnerability was found in Combodo iTop up to 2.6.0 and classified as problematic. Affected by this issue is an unknown function of the file webservices/export.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 Cross Site Scripting attack.
2.	Cross Site Request Forgery	CVE-2020-1977	Expedition Migration Tool up to 1.1.51 cross site request forgery	A vulnerability, which was classified as problematic, was found in Expedition Migration Tool up to 1.1.51. Affected is some unknown functionality. 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
3.	SQL Injection	CVE-2020-8804	SuiteCRM up to 7.11.10 SOAP API sql injection	A vulnerability was found in SuiteCRM up to 7.11.10. It has been classified as critical. This affects an unknown code of the component SOAP API. 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.