Weekly Zero-Day Vulnerability Coverage Bulletin

(13th January – 19th January)

Summary:

Total **6 Zero-Day Vulnerabilities** were discovered in **4 Categories** in this week

2
Cross Site Scripting

1
Directory Traversal

1
Remote Code Execution

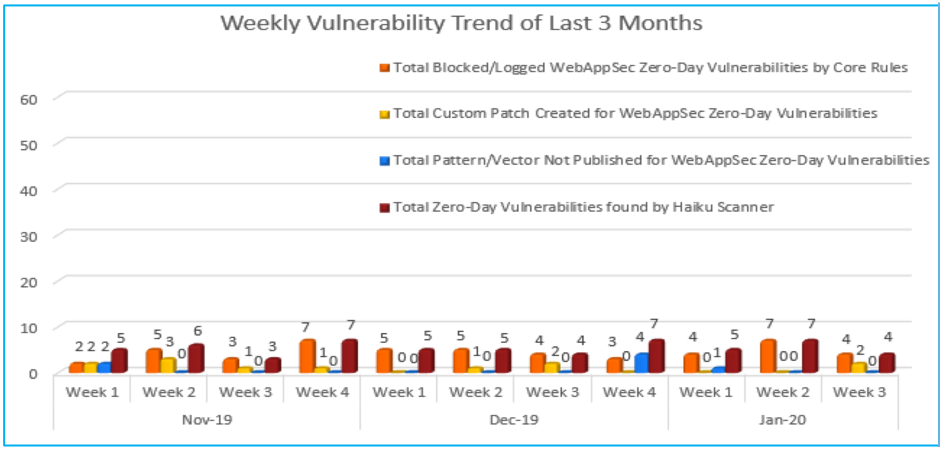
2
Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	4
Zero-Day Vulnerabilities Protected through Custom Rules	2*
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:

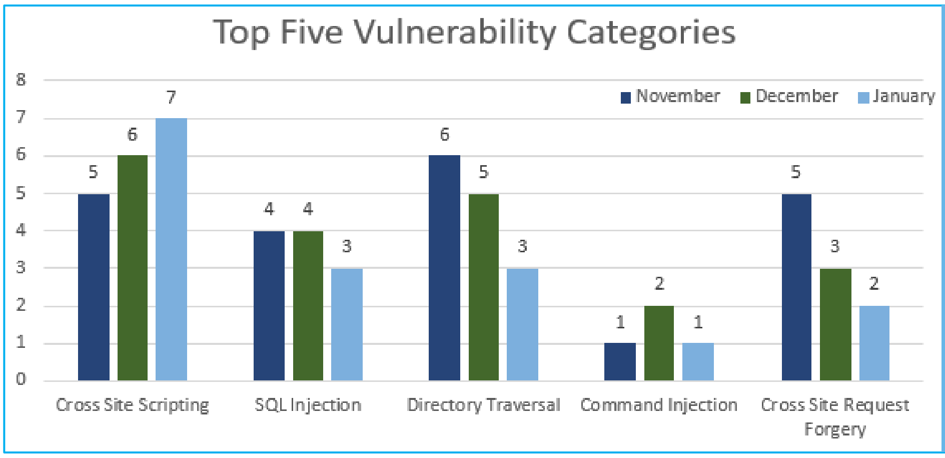


Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a quarter.

39% 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

46% 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 so far compared to other categories.

Only one Command Injection is discovered in November and 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.	Cross Site Scripting	CVE-2020-6955	Cayin SMP-PRO4 image_preview.html filename cross site scripting	A vulnerability classified as problematic was found in Cayin SMP-PRO4 (the affected version is unknown). This vulnerability affects an unknown code of the file <em>image_preview.html</em>. 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.
		CVE-2020-7106	Cacti 1.2.8 data_sources.php header cross site scripting	A vulnerability was found in Cacti 1.2.8 (Log Management Software). It has been rated as problematic. Affected by this issue is an unknown functionality of the file <em>data_sources.php</em>. 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.	Directory Traversal	CVE-2019-15855	Maarch RM up to 2.4 POST Request directory traversal	A vulnerability was found in March RM up to 2.4. It has been declared as critical. This vulnerability affects an unknown part. Upgrading to version 2.5 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.
3.	Denial of Service	CVE-2020-7058	Cacti 1.2.8 data_input.php Remote Code Execution [Disputed]	A vulnerability was found in Cacti 1.2.8 (Log Management Software). It has been classified as critical. Affected is some unknown processing of the file <em>data_input.php</em>. There is no information about possible countermeasures known. It may be suggested to	Protected by Default Rules.	Detected by scanner as Denial of Service attack.

				replace the affected object with an alternative product.		
4.	Cross Site Request Forgery	NA	Cisco IOS/IOS XE up to 16.1.0 Web UI cross site request forgery	A vulnerability was found in Cisco IOS and IOS XE up to 16.1.0 (Router Operating System). It has been rated as problematic. This issue affects an unknown part of the component <em>Web UI</em>. Upgrading to version 16.1.1 eliminates this vulnerability. It is possible to mitigate the problem by applying the configuration setting <code>no ip http server/no ip http secure-server</code>. The best possible mitigation is suggested to be upgrading to the latest version. A possible mitigation has been published immediately after the disclosure of the vulnerability.	Protected by Custom Rules.	NA
		CVE-2020-5501	phpBB 3.2.8 Group Avatar cross site request forgery	A vulnerability was found in phpBB 3.2.8 (Forum Software). It has been classified as problematic. Affected is some unknown functionality of the component <em>Group Avatar Handler</em>. 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