Weekly Zero-Day Vulnerability Coverage Bulletin

(9th December – 15th December)

Summary:

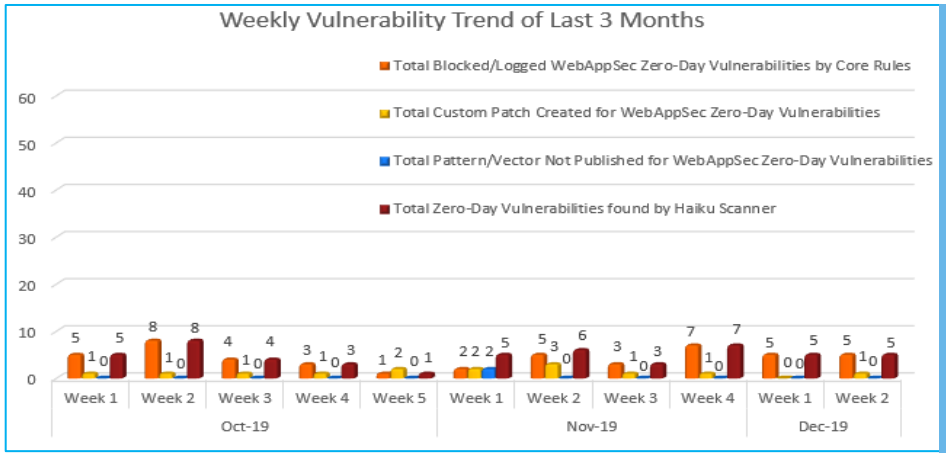
Total **6 Zero-Day Vulnerabilities** were discovered in **3 Categories** this week

3	2	1
Cross Site Scripting	Directory Traversal	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	5
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	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:

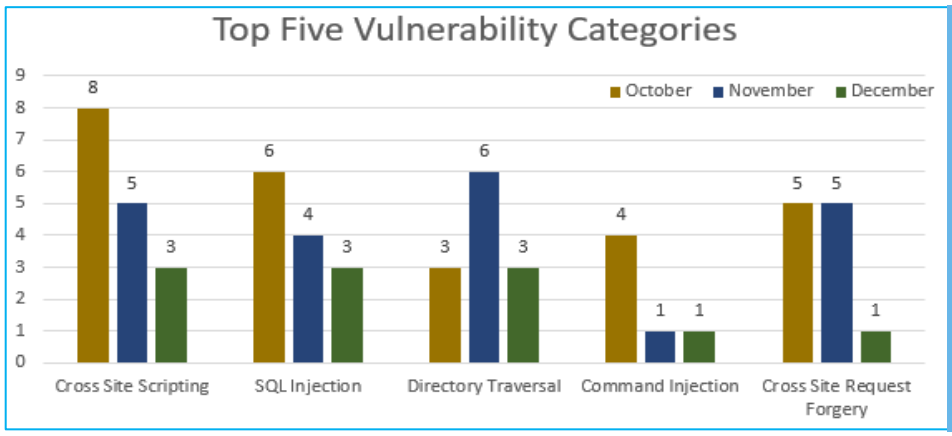


Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a quarter.

42% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

12% 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 October compared to other months and categories so far.

Single Command Injection and Cross Site Request Forgery is found in December 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-2013-7370	node-connect to 2.8.0 Middleware cross site scripting	A vulnerability classified as problematic was found in node-connect up to 2.8.0. This vulnerability affects an unknown function of the component Middleware. Upgrading to version 2.8.1 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2013-5978	Cart66 Lite Plugin up to 1.5.1.14 on WordPress products.php Request cross site scripting	A vulnerability has been found in Cart66 Lite Plugin up to 1.5.1.14 on WordPress (WordPress Plugin) and classified as problematic. This vulnerability affects some unknown functionality of the file products.php. Upgrading to version 1.5.1.15 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2019-19198	Scoutnet Kalender Plugin 1.1.0 on WordPress cross site scripting	A vulnerability has been found in Scoutnet Kalender Plugin 1.1.0 on WordPress (WordPress Plugin) and classified as problematic. Affected by this 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.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	Directory Traversal	CVE-2019-15931	Intesync Solismed 3.3sp directory traversal	A vulnerability, which was classified as critical, was found in Intesync Solismed 3.3sp.	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.

			[CVE-2019-15931]	This 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.		
		CVE-2019-19790	Telerik UI for ASP.NET AJAX RadChart Request directory traversal	A vulnerability was found in Telerik UI for ASP.NET AJAX (affected version unknown). It has been declared as critical. Affected by this vulnerability is an unknown code of the component RadChart. 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.	Cross Site Request Forgery	CVE-2019-15934	Intesync Solismed 3.3sp cross site request forgery [CVE-2019-15934]	A vulnerability was found in Intesync Solismed 3.3sp. It has been classified as problematic. Affected 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.	Protected by Custom Rules.	NA