Weekly Zero-Day Vulnerability Coverage Bulletin

(16th December – 22nd December)

Summary:

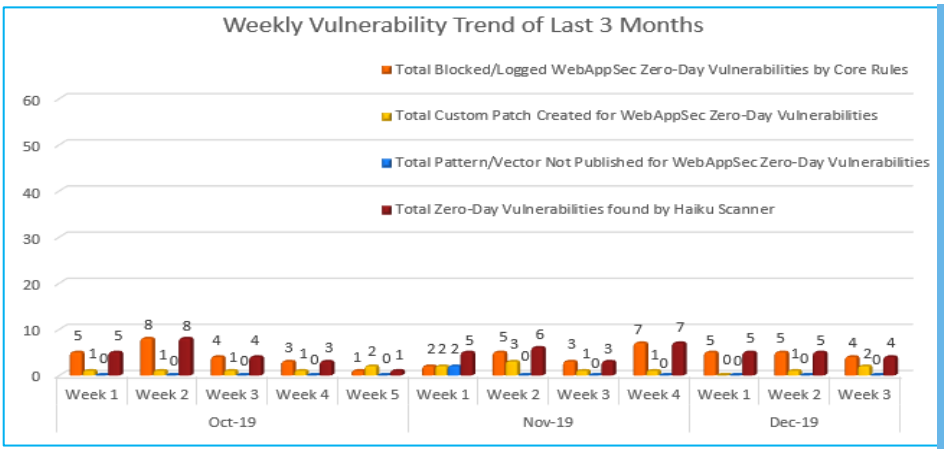
Total **6 Zero-Day Vulnerabilities** were discovered in **3 Categories** in this week

2	2	2
Cross Site Scripting	Directory Traversal	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:

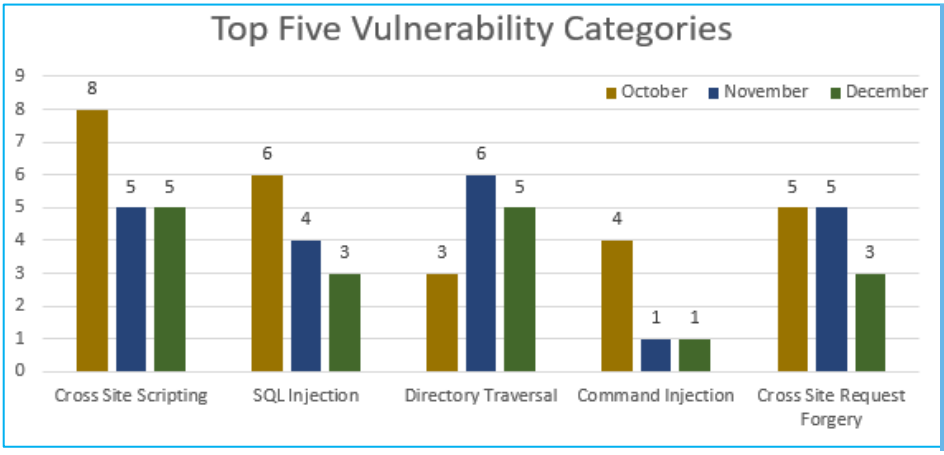


Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a quarter.

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

13% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

45% 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.

Only one Command Injection is discovered in November and 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-2019-19368	Rumpus FTP Web File Manager 8.2.9.1 Login Page Reflected cross site scripting	A vulnerability has been found in Rumpus FTP Web File Manager 8.2.9.1 and classified as problematic. This vulnerability affects an unknown part of the component Login Page. 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-2019-19497	Alt-N MDaemon Attachment filename cross site scripting	A vulnerability, which was classified as problematic, has been found in Alt-N MDaemon (Mail Server Software) (unknown version). This issue affects an unknown code block of the component Attachment 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 Cross Site Scripting attack.
2.	Directory Traversal	CVE-2019-15600	http_server directory traversal [CVE-2019-15600]	A vulnerability classified as problematic was found in http_server (the affected version is unknown). This vulnerability affects an unknown functionality. There is no information about possible countermeasures known. It may be suggested to	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.

				replace the affected object with an alternative product.		
		CVE-2019-15596	statics-server Symlink directory traversal [CVE-2019-15596]	A vulnerability was found in statics-server (version unknown). It has been classified as critical. Affected is an unknown code. 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-2019-16569	Mantis Plugin up to 0.26 on Jenkins cross site request forgery	A vulnerability was found in Mantis Plugin up to 0.26 on Jenkins (Bug Tracking Software) and classified as problematic. This issue affects an unknown code block. 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
		CVE-2019-16570	RapidDeploy Plugin up to 4.1 on Jenkins cross site request forgery	A vulnerability was found in RapidDeploy Plugin up to 4.1 on Jenkins (Jenkins Plugin). It has been classified as problematic. Affected is some unknown processing. 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