Weekly Zero-Day Vulnerability Coverage Bulletin

(14th October – 20th October)

Summary:

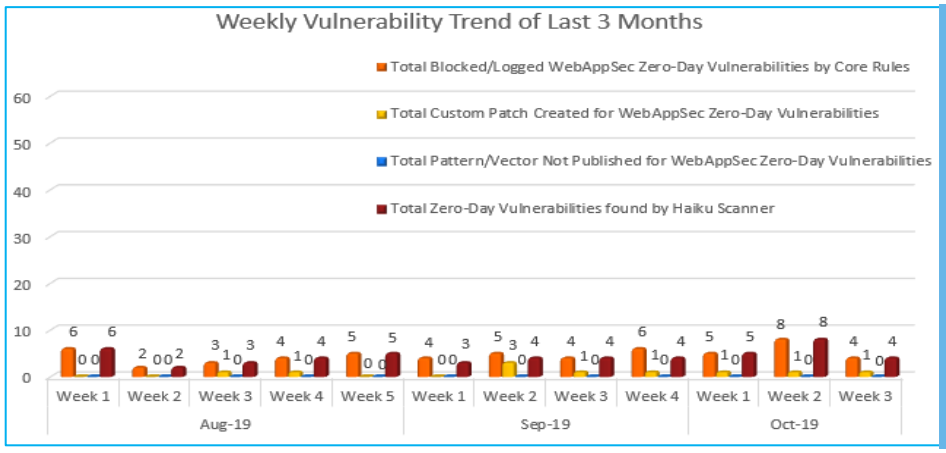
Total **5 Zero-Day Vulnerabilities** were discovered in **4 Categories** in this week

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

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	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:

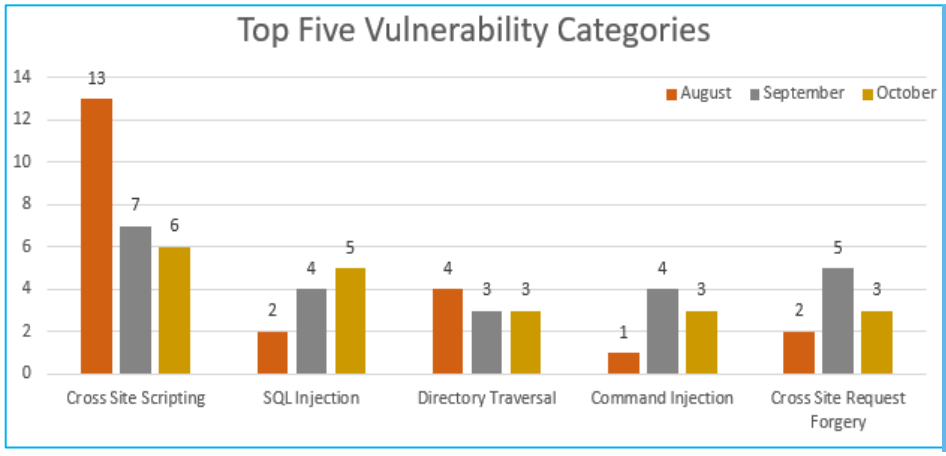


Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a quarter.

47% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

10% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

43% 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 August compared to other months.

Only one Command Injection is found in August compared to other months and categories.

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.	Directory Traversal	NA	Jiangnan Online Judge 0.8.0 viewfile name directory traversal	A vulnerability, which was classified as critical, has been found in Jiangnan Online Judge 0.8.0. This issue affects an unknown code block of the file web/polygon/problem/viewfile?id=1. There is no information about possible countermeasures known. It is suggested to replace the affected object with an alternative product.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		NA	Nostromo nhttpd up to 1.9.6 http_verify HTTP Request directory traversal	A vulnerability classified as critical has been found in Nostromo nhttpd up to 1.9.6 (Web Server). This affects the function <code>http_verify</code>. There is no information about possible countermeasures known. It is suggested to replace the affected object with an alternative product.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	Command Injection	NA	safer-eval up to 1.3.1 Sandbox Remote Code Execution	A vulnerability has been found in safer-eval up to 1.3.1 and classified as critical. This vulnerability affects an unknown part of the component Sandbox. Upgrading to version	Protected by Default Rules.	Detected by scanner as Command Injection attack.

				1.3.2 eliminates this vulnerability.		
3.	Cross Site Request Forgery	NA	JIZHICMS 1.5.1 adminadd.html cross site request forgery	A vulnerability was found in JIZHICMS 1.5.1 (Content Management System). It has been classified as problematic. This affects an unknown part of the file admin.php/Admin/adminadd.html. There is no information about possible countermeasures known. It is suggested to replace the affected object with an alternative product.	Protected by Custom Rules.	NA
4.	SQL Injection	NA	idreamsoft iCMS 7.0.14 spider_project.admincp.php sql injection	A vulnerability was found in idreamsoft iCMS 7.0.14 (Content Management System). It has been rated as critical. This issue affects an unknown functionality of the file spider_project.admincp.php. There is no information about possible countermeasures known. It is suggested to replace the affected object with an alternative product.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.