Weekly Zero-Day Vulnerability Coverage Bulletin

(2nd September – 8th September)

Summary:

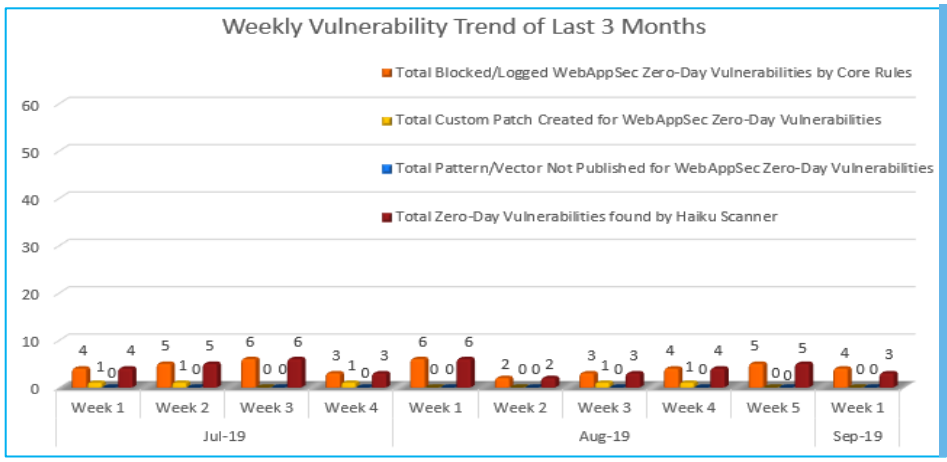
Total **4 Zero-Day Vulnerabilities** were discovered in **4 Categories** this week

1	1	1	1
Cross Site Scripting	SQL Injection	Directory Traversal	Command Injection

Zero-Day Vulnerabilities Protected through Core Rules	4
Zero-Day Vulnerabilities Protected through Custom Rules	0*
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:

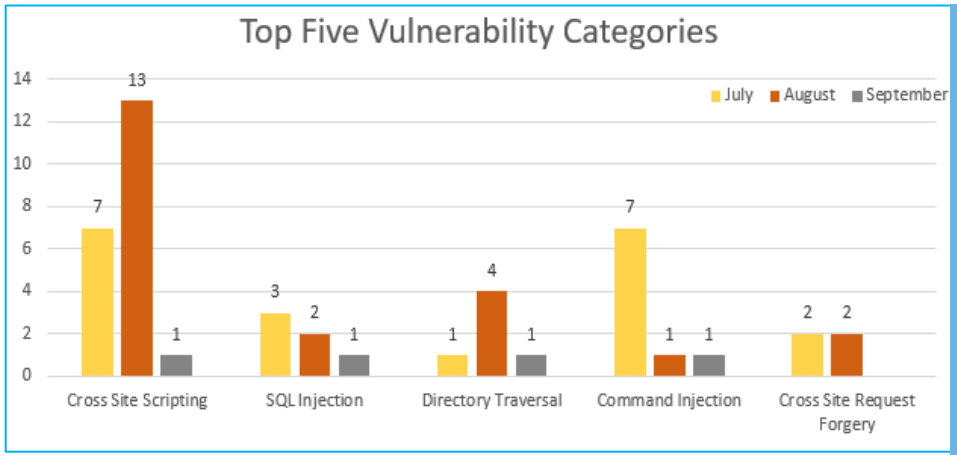


Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.

48% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

6% 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 August compared to other months.

No Cross Site Request Forgery attack is found in September.

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-2018-11198	Mautic 2.13.1 config.json authorUrl cross site scripting	A vulnerability, which was classified as problematic, has been found in Mautic 2.13.1. Affected by this issue is an unknown functionality of the file config.json. 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.	SQL Injection	CVE-2019-13191	IntraMaps MapControl 8 Set sql injection	A vulnerability, which was classified as critical, was found in IntraMaps MapControl 8. This affects an unknown code of the file /ApplicationEngine/Search/Refine/Set. 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.	NA
3.	Directory Traversal	CVE-2019-15952	Total.js CMS 12.0.0 directory traversal	A vulnerability classified as critical was found in Total.js CMS 12.0.0 (JavaScript Library). This affects an 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 Default Rules.	Detected by scanner as Directory Traversal attack.
4.	Command Injection	CVE-2019-14224	Alfresco Community Edition 5.2 201707 Solr Configuration	A vulnerability was found in Alfresco	Protected by Default Rules.	Detected by scanner as Command Injection attack.

	File Code Execution	Community Edition 5.2 201707. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Solr Configuration File Handler. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.