Weekly Zero-Day Vulnerability Coverage Bulletin

(19th August – 21st August)

Summary:

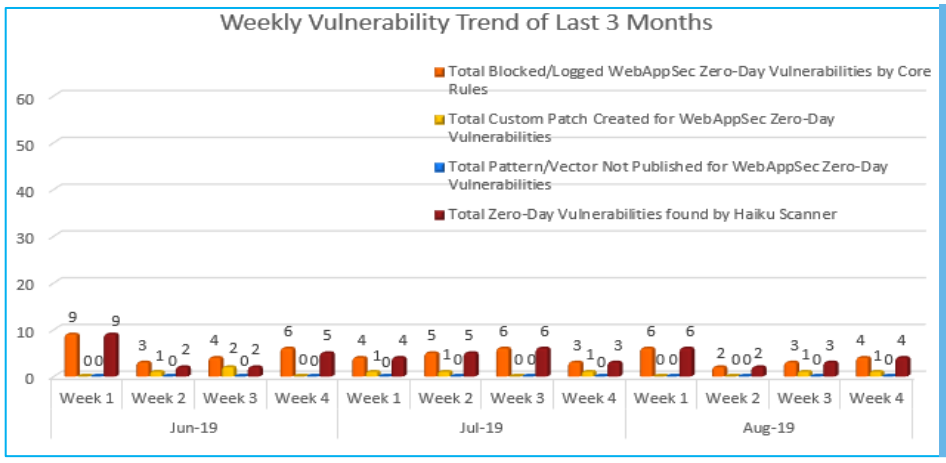
Total **5 Zero-Day Vulnerabilities** were discovered in **3 Categories** this week

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

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:

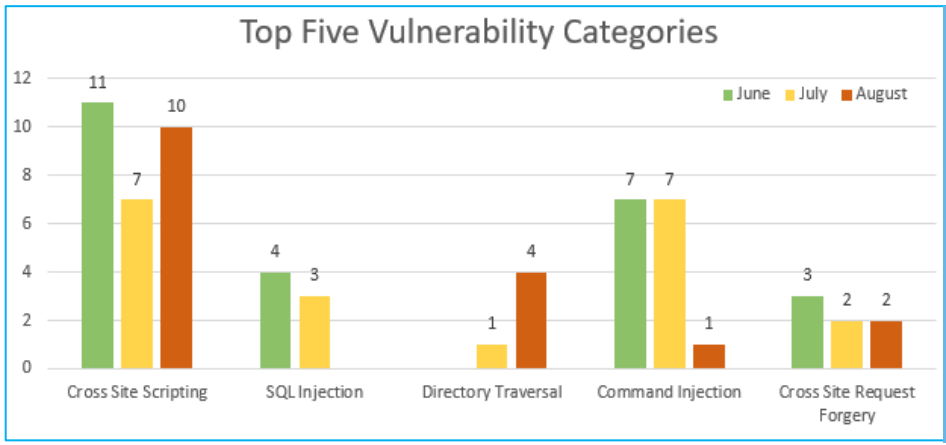


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

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

7% 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 no. of Cross Site Scripting vulnerabilities discovered in June compared to other months.

No Directory Traversal vulnerabilities are found in June.

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-2019-6159	IBM System x IMM V1 Stored cross site scripting	A vulnerability was found in IBM System x IMM V1. It has been classified as problematic. Affected is an unknown functionality. Upgrading to version V2 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2018-20978	wp-all-import Plugin up to 3.4.6 on WordPress cross site scripting	A vulnerability, which was classified as problematic, was found in wp-all-import Plugin up to 3.4.6 on WordPress (WordPress Plugin). This affects an unknown function. Upgrading to version 3.4.7 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2019-11522	OX App Suite 7.10.0 cross site scripting	A vulnerability classified as problematic has been found in OX App Suite 7.10.0. This affects 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 Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	Cross Site Request Forgery	CVE-2019-15238	cforms2 Plugin up to 15.0.1 on WordPress cross site request forgery	A vulnerability, which was classified as problematic, has been found in cforms2 Plugin up to 15.0.1 on WordPress (WordPress Plugin). Affected by this issue is an unknown part. Upgrading to version 15.0.2 eliminates this vulnerability.	Protected by Custom Rules.	NA
3.	Command Injection	CVE-2019-4460	IBM API Connect up to 5.0.8.6 Developer Portal Request directory traversal	A vulnerability classified as critical was found in IBM API Connect up to 5.0.8.6 (Automation Software). This vulnerability affects an unknown code block of the component Developer Portal. 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 Command Injection attack.