Weekly Zero-Day Vulnerability Coverage Bulletin

(26th August – 1st September)

Summary:

Total **5 Zero-Day Vulnerabilities** were discovered in **2 Categories** this week

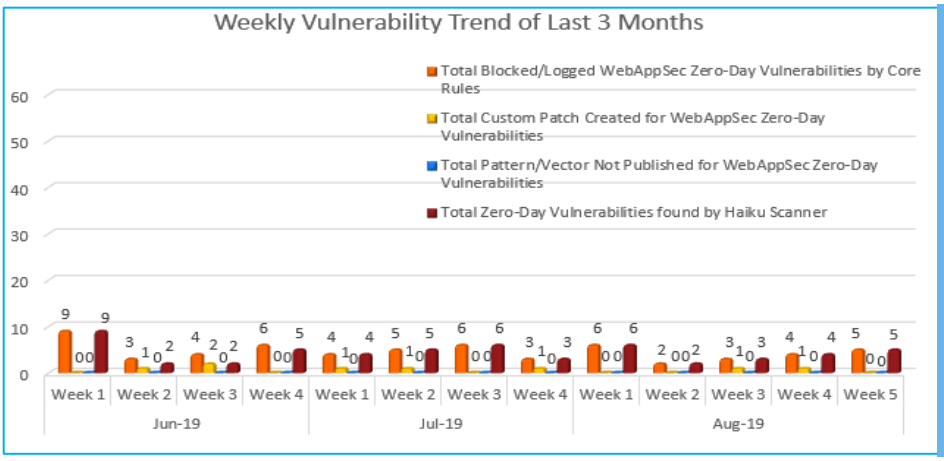
3
Cross Site Scripting

2
SQL Injection

Zero-Day Vulnerabilities Protected through Core Rules	5
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	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:

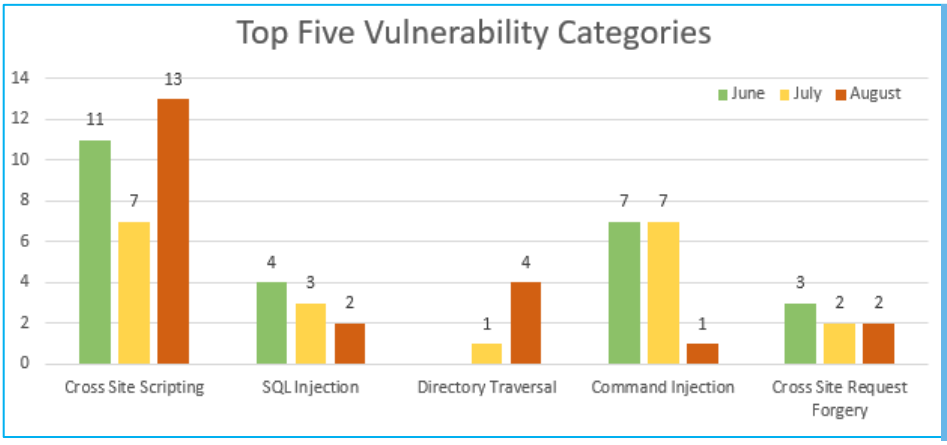


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

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 are discovered in August 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-2019-15643	ultimate-faqs Plugin up to 1.8.21 on WordPress cross site scripting	A vulnerability was found in ultimate-faqs Plugin up to 1.8.21 on WordPress (WordPress Plugin). It has been rated as problematic. This issue affects an unknown code. Upgrading to version 1.8.22 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2019-15644	zoho-salesiq Plugin up to 1.0.8 on WordPress Stored cross site scripting	A vulnerability is classified as problematic has been found in zoho-salesiq Plugin up to 1.0.8 on WordPress (WordPress Plugin). Affected is an unknown code block. Upgrading to version 1.0.9 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2014-10395	cp-polls Plugin up to 1.0.0 on WordPress Votes List cross site scripting	A vulnerability was found in cp-polls Plugin up to 1.0.0 on WordPress (WordPress Plugin) and classified as problematic. This issue affects some unknown functionality of the component Votes List Handler. Upgrading to version 1.0.1 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	SQL Injection	CVE-2019-15646	rsvpmaker Plugin up to 6.1 on WordPress sql injection	A vulnerability, which was classified as critical, has been found in rsvpmaker Plugin up to 6.1 on WordPress (WordPress Plugin). Affected by this issue is an unknown function. Upgrading to version 6.2 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
		CVE-2019-15659	pie-register Plugin up to 3.1.1 on WordPress sql injection	A vulnerability was found in pie-register Plugin up to 3.1.1 on WordPress (WordPress Plugin). It has been declared as critical. Affected by this vulnerability is an unknown code block. Upgrading to version 3.1.2 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.