Weekly Zero-Day Vulnerability Coverage Bulletin

(5th August – 11th August)

Summary:

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

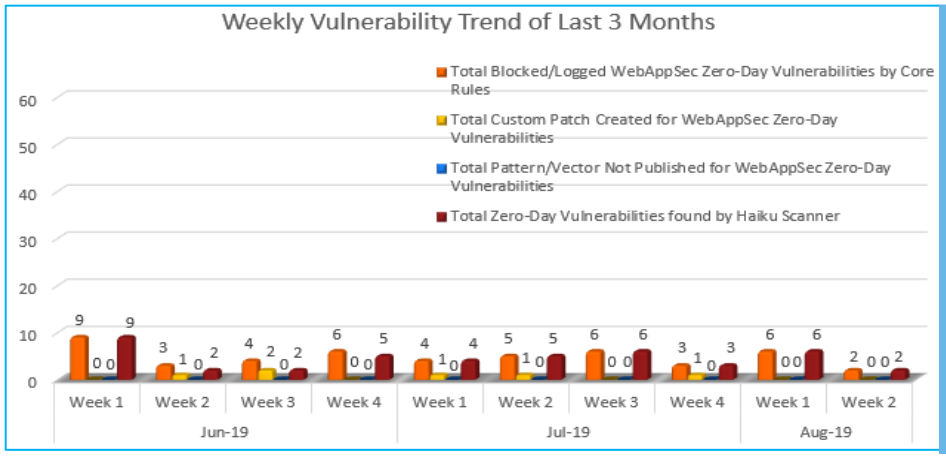
1
Cross Site Scripting

1
Directory Traversal

Zero-Day Vulnerabilities Protected through Core Rules	2
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	2

* 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:

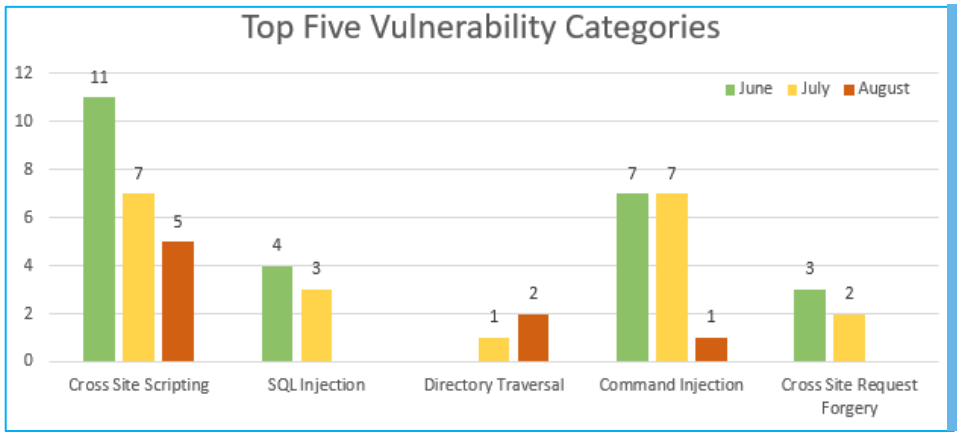


Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a quarter.

49% 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

45% Of Zero-Day Vulnerabilities were reported by Haiku Scanner in last quarter



From the graph, we infer that maximum Cross Site Scripting and SQL Injection vulnerabilities are 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	NA	WordPress Plugin Facebook Widget affected by authenticated XSS	It was found that plugin contains an authenticated persistent cross-site scripting (XSS) vulnerability due to not properly handling the security of shortcode attributes	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	Directory Traversal	NA	Cisco Enterprise NFV Infrastructure Software directory traversal	A vulnerability classified as problematic has been found in Cisco Enterprise NFV Infrastructure Software (the affected version unknown). This affects an unknown code. Upgrading eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.