Weekly Zero-Day Vulnerability Coverage Bulletin

(12th August – 18th August)

Summary:

Total **4 Zero-Day Vulnerabilities** were discovered in **3 Categories** in this week

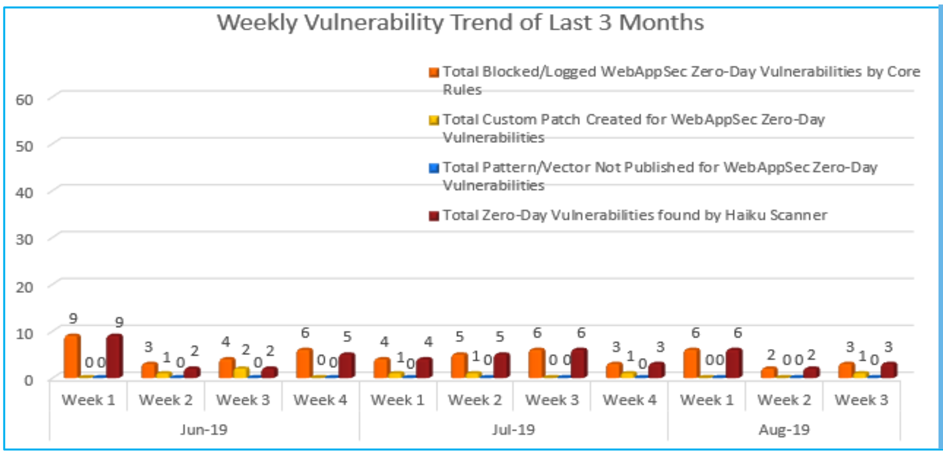
2	1	1
Cross Site Scripting	Cross Site Request Forgery	Directory Traversal

Zero-Day Vulnerabilities Protected through Core Rules	3
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	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:

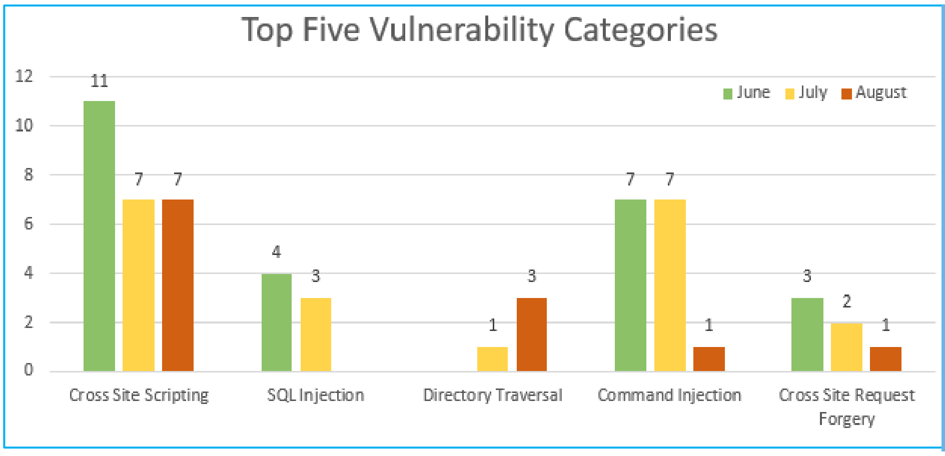


Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a quarter.

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 Cross Site Scripting vulnerabilities were discovered in June compared to other months and categories so far.

Zero Directory Traversal vulnerabilities were 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-2017-18496	htaccess Plugin up to 1.7.5 on WordPress cross site scripting	A vulnerability classified as problematic was found in <a href="https://vuldb.com/?product.htaccess_plugin">htaccess Plugin up to 1.7.5</a> on WordPress (WordPress Plugin). Affected by this vulnerability is an unknown functionality. Upgrading to version 1.7.6 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2017-18507	wp-live-chat-support Plugin up to 7.1.4 on WordPress cross site scripting	A vulnerability has been found in <a href="https://vuldb.com/?product.wp-live-chat-support_plugin">wp-live-chat-support Plugin up to 7.1.4</a> on WordPress (Chat Software) and classified as problematic. This vulnerability affects an unknown code. Upgrading to version 7.1.05 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	Directory Traversal	CVE-2019-14530	OpenEMR up to 5.0.1 custom/ajax_download.php fileName directory traversal	A vulnerability, which was classified as problematic, has been found in <a href="https://vuldb.com/?product.openemr">OpenEMR up to 5.0.1</a> (Business Process Management Software). This issue affects an unknown code of the file <em>custom/ajax_download.php</em>. Upgrading to version 5.0.2 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.
3.	Cross Site Request Forgery	CVE-2018-20964	contact-form-to-email Plugin up to 1.2.65 on WordPress cross site request forgery	A vulnerability was found in <a href="https://vuldb.com/?product.contact-form-to-email_plugin">contact-form-to-email Plugin up to 1.2.65</a> on WordPress (WordPress Plugin). It has been declared as problematic. Affected by this vulnerability is an unknown function. Upgrading to version 1.2.66 eliminates this vulnerability.	Protected by Custom Rules.	NA