Weekly Zero-Day Vulnerability Coverage Bulletin

(7th October – 13th October)

Summary:

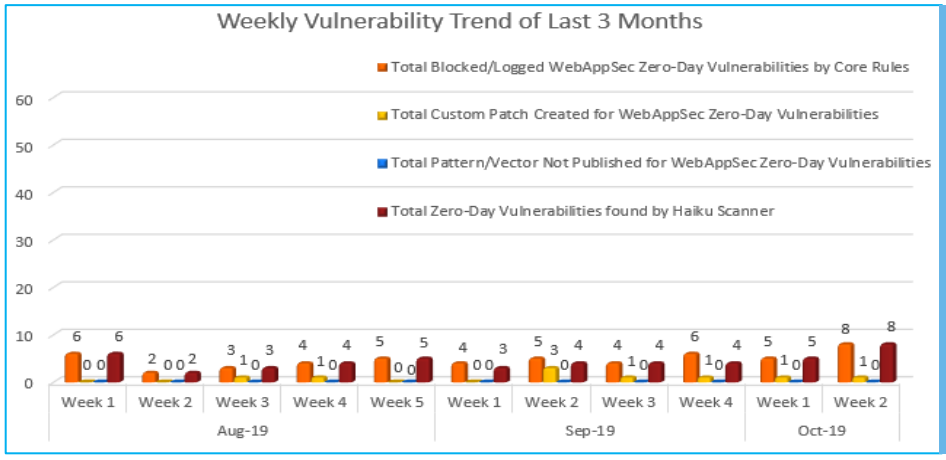
Total **9 Zero-Day Vulnerabilities** were discovered in **4 Categories** this week

4	3	1	1
Cross Site Scripting	SQL Injection	Command Injection	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	8
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	8

* 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:

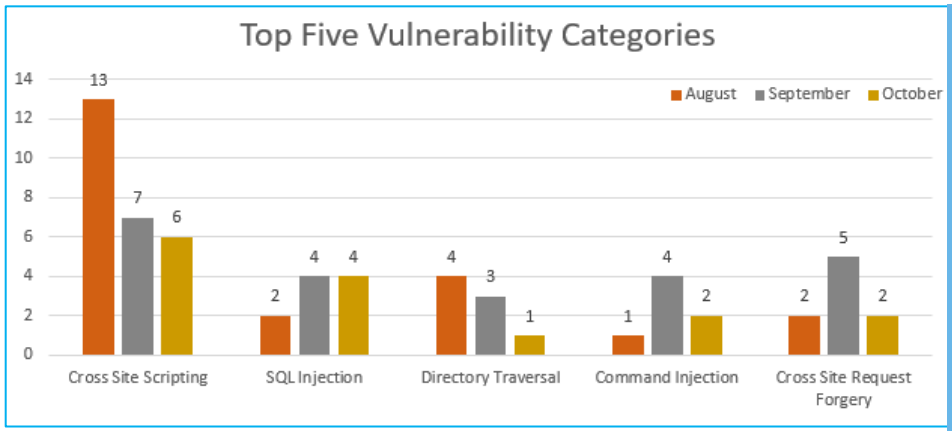


Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a quarter.

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

9% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

43% 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.

Similar count of SQL Injection attacks found in September and October.

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	Subrion CMS 4.2.1 panel/members/ Username/Full Name/Email cross site scripting	A vulnerability classified as problematic has been found in Subrion CMS 4.2.1 (Content Management System). This affects an unknown functionality of the file panel/members/. 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.
		NA	CMS Made Simple 2.2.11 Module Manager Term cross site scripting	A vulnerability classified as problematic was found in CMS Made Simple 2.2.11 (Content Management System). This vulnerability affects some unknown functionality of the component Module Manager. 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.
		NA	cPanel up to 82.0.14 SSL Key Delete Interface cross site scripting	A vulnerability classified as problematic was found in cPanel up to 82.0.14 (Hosting Control Software). Affected by this vulnerability is an unknown functionality	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.

				of the component SSL Key Delete Interface. Upgrading to version 82.0.15 eliminates this vulnerability.		
		NA	cPanel up to 82.0.14 LiveAPI Example Scripts cross site scripting	A vulnerability classified as problematic has been found in cPanel up to 82.0.14 (Hosting Control Software). Affected is an unknown function of the component LiveAPI Example Scripts. Upgrading to version 82.0.15 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	SQL Injection	NA	knex.js up to 0.19.4 MSSQL sql injection	A vulnerability classified as critical was found in knex.js up to 0.19.4 (JavaScript Library). This vulnerability affects an unknown part of the component MSSQL Handler. Upgrading to version 0.19.5 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
		NA	SugarCRM up to 8.0.3/9.0.1 Emails sql injection	A vulnerability, which was classified as critical, has been found in SugarCRM up to 8.0.3/9.0.1. Affected by this issue is an unknown part of the component Emails. Upgrading to version 8.0.4 or 9.0.2 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
		NA	Adhouma CMS up to 2019-10-09 post.php p_id sql injection	A vulnerability classified as critical was found in Adhouma CMS up to	Protected by Default Rules.	Detected by scanner as SQL Injection attack.

				2019-10-09 (Content Management System). Affected by this vulnerability is an unknown part of the file post.php. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.		
3.	Cross Site Request Forgery	CVE-2019-17369	OTCMS 3.85 Admin Panel admin/member_deal.php cross site request forgery	A vulnerability classified as problematic was found in OTCMS 3.85. Affected by this vulnerability is some unknown processing of the file admin/member_deal.php of the component Admin Panel. There is no information about possible countermeasures known. It is suggested to replace the affected object with an alternative product.	Protected by Custom Rules.	NA
4.	Command Injection	NA	Zingbox Inspector up to 1.293 Update Image command injection	A vulnerability, which was classified as critical, has been found in Zingbox Inspector up to 1.293. This issue affects an unknown part of the component Update Image Handler. There is no information about possible countermeasures known. It is suggested to replace the affected object with an alternative product.	Protected by default Rules.	Detected by scanner as Command Injection attack.