Weekly Zero-Day Vulnerability Coverage Bulletin

(30th September – 6th October)

Summary:

Total **6 Zero-Day Vulnerabilities** were discovered in **5 Categories** this week

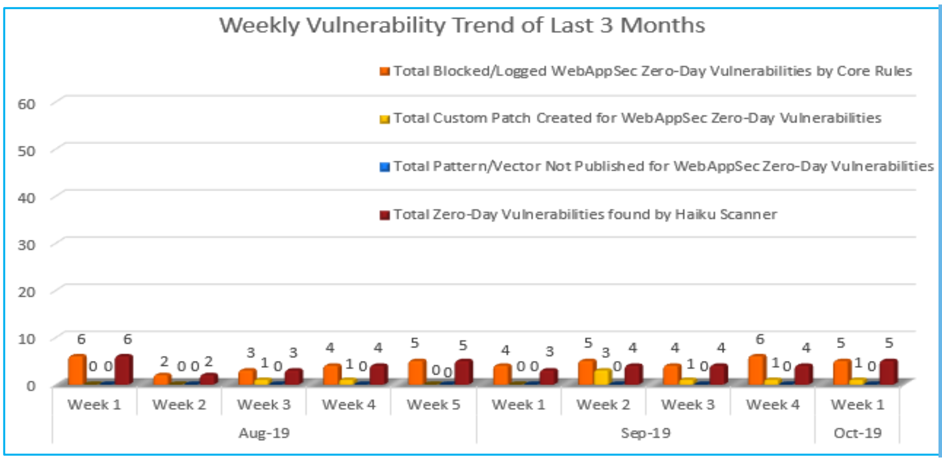
2	**1**	**1**	**1**	**1**
Cross Site Scripting	SQL Injection	Cross Site Request Forgery	Directory Traversal	Command Injection

Zero-Day Vulnerabilities Protected through Core Rules	5
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	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:

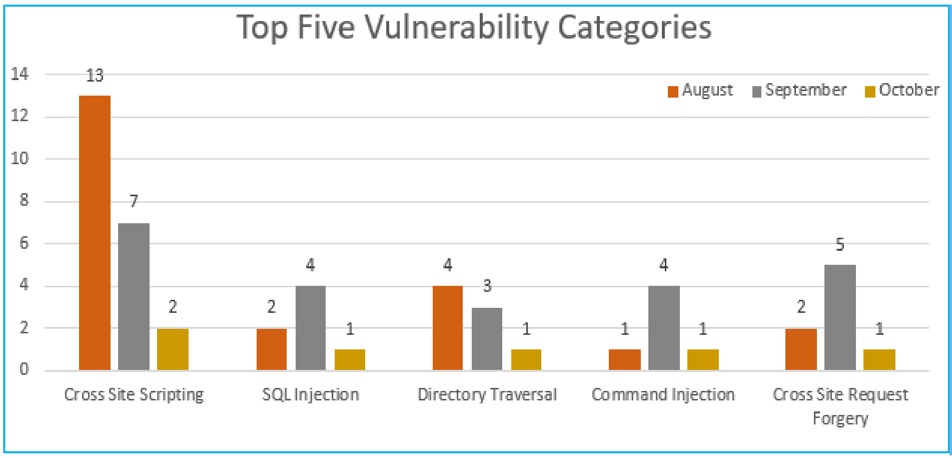


Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.

47% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

10% 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.

Only one vulnerability is found for various categories in October so far.

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	JetBrains YouTrack prior 2019.1.52584 Issue Title cross site scripting	A vulnerability was found in <a href="https://vuldb.com/?product.jetbrains:youtrack">JetBrains YouTrack</a>. It has been classified as problematic. This affects an unknown functionality of the component <em>Issue Title Handler</em>. Upgrading to version 2019.1.52584 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		NA	Online Store 1.0 user_view.php adidas_member_user cross site scripting	A vulnerability was found in <a href="https://vuldb.com/?product.online_store">Online Store 1.0</a> and classified as problematic. Affected by this issue is an unknown functionality of the file <em>user_view.php</em>. 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.	SQL Injection	NA	eBrigade up to 4.x evenements.php cid sql injection	A vulnerability has been found in <a href="https://vuldb.com/?product.ebrigade">eBrigade up to 4.x</a> and classified as critical. This vulnerability affects some unknown processing of the file <em>evenements.php</em>. Upgrading to version 5.0 eliminates this vulnerability.	Protected by Default Rules.	NA
3.	Directory Traversal	NA	CDG up to 2017-01-01 downloadDocument.jsp pathAndName directory traversal	A vulnerability was found in <a href="https://vuldb.com/?product.cdg">CDG up to 2017-01-01</a>. It has been rated as critical. This issue affects an unknown functionality of the file <em>downloadDocument.jsp?command=download</em>. 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 Directory Traversal attack.

4.	Cross Site Request Forgery	NA	phpBB up to 3.1.7 BBcode Page acp_bbcodes.php cross site request forgery	A vulnerability was found in <a href="https://vuldb.com/?product.phpbb">phpBB up to 3.1.7</a> (Forum Software). It has been declared as problematic. Affected by this vulnerability is some unknown functionality of the file <em>includes/acp/acp_bbcodes.php</em> of the component <em>BBcode Page</em>. Upgrading to version 3.1.7-PL1 eliminates this vulnerability.	Protected by Custom Rules.	NA
5.	Command Injection	NA	JetBrains Ktor Framework up to 1.1.x LDAP Username command injection	A vulnerability was found in <a href="https://vuldb.com/?product.jetbrains:ktor_framework">JetBrains Ktor Framework up to 1.1.x</a>. It has been classified as critical. Affected is some unknown functionality of the component <em>LDAP Handler</em>. Upgrading to version 1.2.0-rc eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Command Injection attack.