Weekly Zero-Day Vulnerability Coverage Bulletin

(17th September – 23rd September)

Summary:

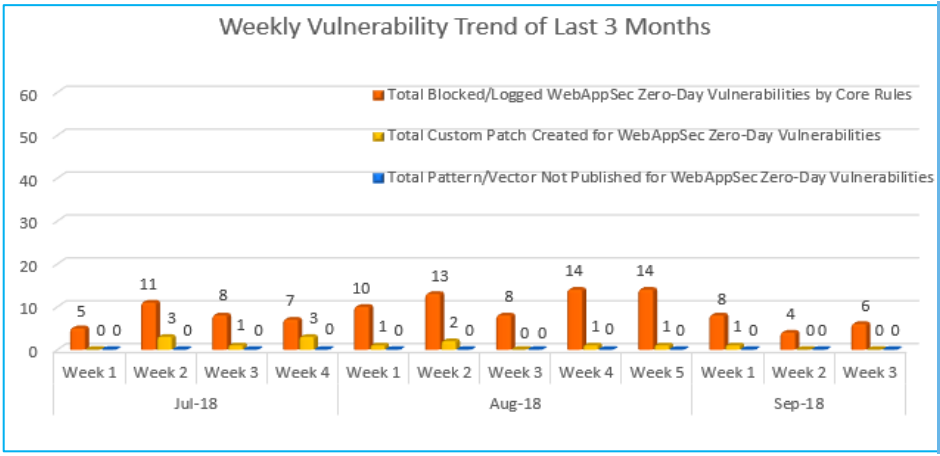
Total **6 Zero-Day Vulnerabilities** were discovered in **3 Categories** previous week

3	2	1
Cross Site Scripting	SQL Injection	Command Injection

Zero-Day Vulnerabilities Protected through Core Rules	6
Zero-Day Vulnerabilities Protected through Custom Rules	0*
Zero-Day Vulnerabilities for which protection cannot be determined	0**

* To enable custom rules please contact support@indusface.com
** Since attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected

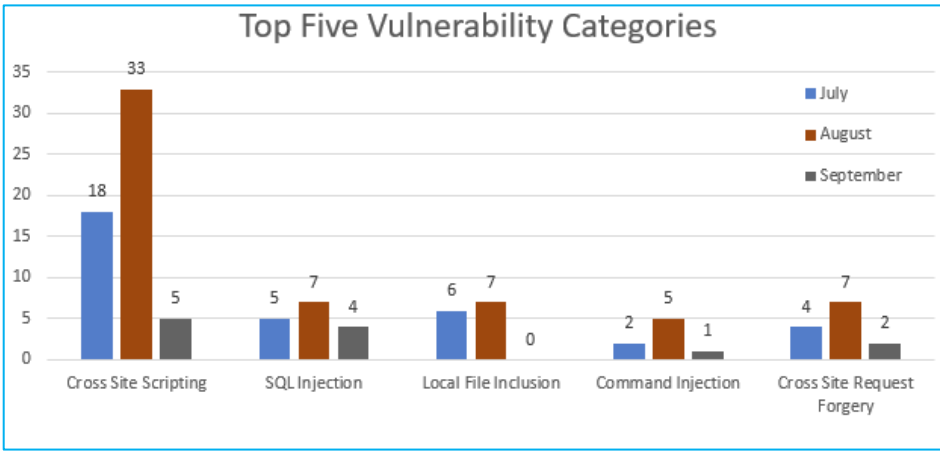
Vulnerability Trend:



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

87% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

13% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



From the graph, we infer that maximum Cross Site Scripting vulnerabilities were discovered in July compared to other months and categories so far.

Medium no. of SQL, LFI and CSRF attacks are found.

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
1.	Cross Site Scripting	CVE-2018-17140	Quizlord Plugin up to 2.0 on WordPress wp-admin/admin.php title cross site scripting	A vulnerability, which was classified as problematic, was found in Quizlord Plugin up to 2.0 on WordPress. This affects an unknown function of the file *wp-admin/admin.php*. The manipulation of the argument title as part of a *Parameter* leads to a cross site scripting vulnerability (Stored). CWE is classifying the issue as CWE-80. This is going to have an impact on integrity. An attacker might be able to inject arbitrary html and script code into the web site. This would alter	Protected by Default Rules.
		CVE-2018-17138	Jibu Pro Plugin up to 1.7 on WordPress quiz_action.php Quiz Name cross site scripting	A vulnerability classified as problematic was found in Jibu Pro Plugin up to 1.7 on WordPress. Affected by this vulnerability is an unknown function of the file *wp-content/plugins/jibu-pro/quiz_action.php*. The manipulation of the argument Quiz Name with an unknown input leads to a cross site scripting vulnerability (Stored). The CWE definition for the vulnerability is CWE-80. As an impact it is known to affect integrity. An attacker might be able to inject arbitrary html and script code into the web site.	Protected by Default Rules.
		EDB-ID: 45422	Netis ADSL Router DL4322D RTK 2.1.1 – Cross Site Scripting	Improper input validation on the router web interface allows attackers add a persistent Cross Site scripting attack on the Dynamic DNS hostname field. Simply intercept a renaming request and add in the Cross Site Scripting.	Protected by Default Rules.
2.	SQL Injection	CVE-2018-17110	Simple POS 4.0.24 Management Panel products/get_products/ columns[0][searc	A vulnerability was found in Simple POS 4.0.24 and classified as critical. This issue affects an unknown function of the file *products/get_products/* of the component *Management Panel*.	Protected by Default Rules.

			h][value sql injection	The manipulation of the argument columns[0][search][value as part of a *Parameter* leads to a sql injection vulnerability. Using CWE to declare the problem leads to CWE-89. Impacted is confidentiality, integrity, and availability. An attacker might be able inject and/or alter existing SQL statements which would influence the database exchange.	
		CVE-2018-17254	Joomla Component JCK Editor 6.4.4 - 'parent' SQL Injection	Joomla Component JCK Editor 6.4.4 - 'parent' SQL Injection	Protected by Default Rules.
3.	Command Injection	CVE-2018-17139	UltimatePOS 2.5 /products privilege escalation	A vulnerability, which was classified as critical, has been found in UltimatePOS 2.5. Affected by this issue is an unknown function of the file */products*. The manipulation with an unknown input leads to a privilege escalation vulnerability (File Upload). Using CWE to declare the problem leads to CWE-269. Impacted is confidentiality, integrity, and availability. The weakness was published 09/17/2018 as *EDB-ID 45253* as uncorroborated exploit (Exploit-DB). The advisory is available at exploit-db.com. This vulnerability is handled as CVE-2018-17139 since 09/17/2018.	Protected by Default Rules.