Weekly Zero-Day Vulnerability Coverage Bulletin

(3rd September – 9th September)

Summary:

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

3
Cross Site Scripting

4
SQL Injection

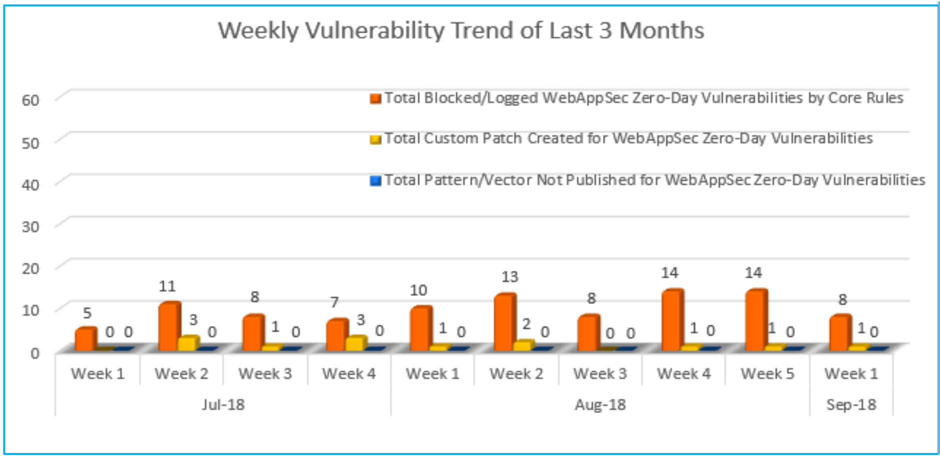
1
Cross Site Request Forgery

1
Command Injection

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**

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

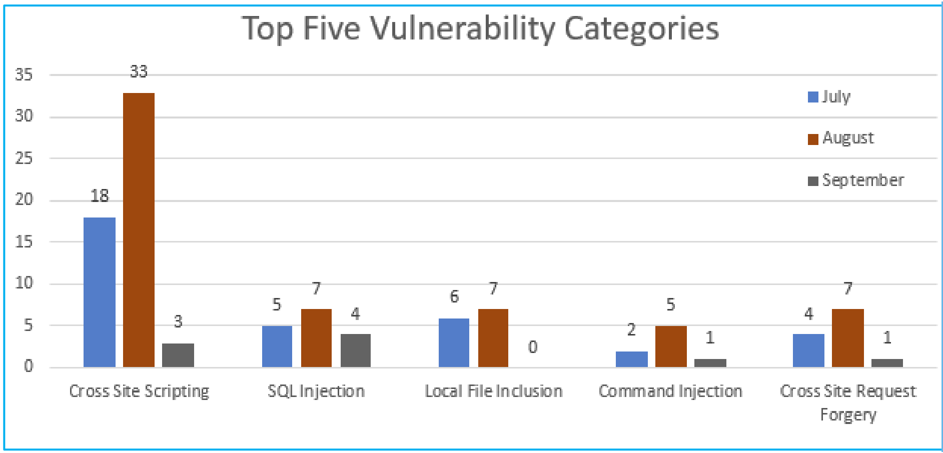
Vulnerability Trend:



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

86% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

14% 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 Injection attacks was found in all the months.

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	EDB-ID: 149179	WordPress Quizlord 2.0 Cross Site Scripting	WordPress Quizlord plugin version 2.0 suffers from a cross site scripting vulnerability.	Protected by Default Rules.
		EDB-ID: 149180	WordPress Jibu Pro 1.7 Cross Site Scripting	WordPress Jibu Pro plugin version 1.7 suffers from a cross site scripting vulnerability.	Protected by Default Rules.
		EDB-ID: 149186	Vox TG790 ADSL Router Cross Site Scripting	The Vox TG790 ADSL router suffers from a cross site scripting vulnerability.	Protected by Default Rules.
2.	SQL Injection	EDB-ID: 149189	AZORult Stealer 2 Botnet SQL Injection	AZORult Stealer version 2 suffers from a remote SQL injection vulnerability.	Protected by Default Rules.
		45330	mooSocial Store Plugin 2.6 - SQL Injection	mooSocial Store Plugin is affected by Blind SQL Injection in the product parameter used with URL Rewrite	Protected by Default Rules.
		45328	Simple POS 4.0.24 - 'columns[0][search][value]' SQL Injection	The vulnerability allows an attacker to inject SQL commands on 'columns[0][search][value]' parameters in the management panel.	Protected by Default Rules.
		45323	Online Quiz Maker 1.0 - 'catid' SQL Injection	An attacker can execute SQL commands through parameters that contain vulnerable. An authorized user can use the filtering feature and can fully authorize the database or other server information. Also, there are XSS vulnerabilities.	Protected by Default Rules.
3.	Cross Site Request Forgery	45322	Admidio 3.3.5 - Cross-Site Request Forgery (Change Permissions)	Low Privilege users will be able to increase their permissions due to improper origin checking by the vendor.	Protected by Custom Rules.
4.	Command Injection	CVE-2018-16308	Ninja Forms Plugin up to 3.3.14.0 on WordPress CSV Injection privilege escalation	A vulnerability classified as critical has been found in Ninja Forms Plugin up to 3.3.14.0 on WordPress. This affects an unknown function. The manipulation with an unknown input leads to a privilege escalation vulnerability (CSV Injection). CWE is classifying the issue as CWE-269. This is going to have an impact on confidentiality, integrity,	Protected by Default Rules.

and availability. The weakness was released 09/01/2018 as *EDB-ID 45234* as uncorroborated exploit (Exploit-DB). It is possible to read the advisory at exploit-db.com.