Weekly Zero-Day Vulnerability Coverage Bulletin

(27th August – 2nd September)

Summary:

Total **12 Zero-Day Vulnerabilities** were discovered in **6 Categories** in this week

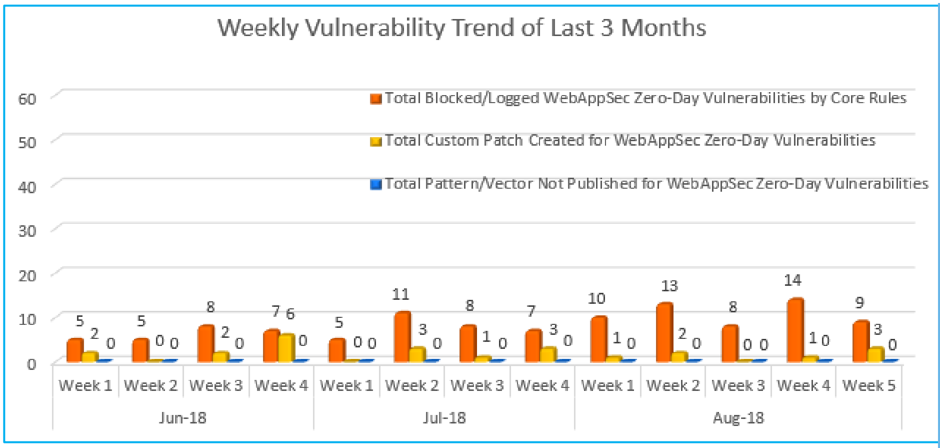
4	2	1	1	3	1
Cross Site Scripting	SQL Injection	Remote File Inclusion	Local File Inclusion	Cross Site Request Forgery	Command Injection

Zero-Day Vulnerabilities Protected through Core Rules	9
Zero-Day Vulnerabilities Protected through Custom Rules	3*
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

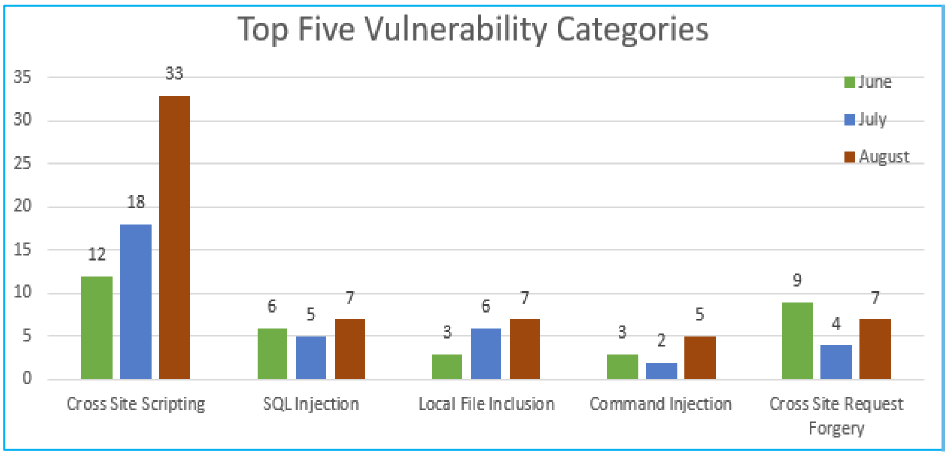
Vulnerability Trend:



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

80% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

20% 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 August compared to other months and categories.

The vulnerabilities found in all the other categories for 3 months is almost same.

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-2018-15847	puppyCMS 5.1 Add Page/URL menu.php cross site scripting	A vulnerability classified as problematic was found in puppyCMS 5.1. This vulnerability affects an unknown function of the file *menu.php* of the component *Add Page/URL*. The manipulation with an unknown input leads to a cross site scripting vulnerability. 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 website. This would alter the appearance.	Protected by Default Rules.
		CVE-2018-15562	CMS ISWEB 3.5.3 Cross Site Scripting	CMS ISWEB version 3.5.3 suffers from a cross site scripting vulnerability.	Protected by Default Rules.
		CVE-2018-15494	Dojo Toolkit 1.13 Cross Site Scripting	Dojo Toolkit version 1.13 suffers from a cross site scripting vulnerability.	Protected by Default Rules.
		EDB-ID: 45305	WordPress Plugin Jibu Pro 1.7 - Cross-Site Scripting	Jibu Pro is prone to Stored Cross Site Scripting vulnerabilities because it fails to properly sanitize user-supplied input.	Protected by Default Rules.
2.	SQL Injection	EDB-ID: 149083	Sentrifugo HRMS 3.2 SQL Injection	Sentrifugo HRMS version 3.2 suffers from a remote SQL injection vulnerability.	Protected by Default Rules.
		CVE-2018-16159	Gift Vouchers Plugin up to 2.0.1 on WordPress wp-admin/admin-ajax.php template_id sql injection	A vulnerability was found in Gift Vouchers Plugin up to 2.0.1 on WordPress and classified as critical. Affected by this issue is an unknown function of the file *wp-admin/admin-ajax.php*. The manipulation of the argument template_id 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	Protected by Default Rules.

				inject and/or alter existing SQL statements which would influence the database exchange.	
3.	Local File Inclusion	CVE-2018-15745	Argus Surveillance DVR 4.0.0.0 Directory Traversal	Argus Surveillance DVR version 4.0.0.0 suffers from file disclosure and traversal vulnerabilities.	Protected by Default Rules.
4.	Remote File Inclusion	EDB-ID: 149126	Schneider Electric BMX P34 CPU B Open Redirect	Schneider Electric BMX P34 CPU B suffers from an open redirection vulnerability.	Protected by Default Rules.
5.	Command Injection	EDB-ID: 45206	Wordpress Plugin Export Users to CSV 1.1.1 - CSV Injection	WordPress Export users to CSV plugin version 1.1.1. and before are affected by Remote Code Execution # through the CSV injection vulnerability. This allows an application user to inject commands as part # of the fields of his profile and these commands are executed when a user with greater privilege # exports the data in CSV and opens that file on his machine.	Protected by Default Rules.
6.	Cross Site Request Forgery	CVE-2018-15845	Gleez CMS 1.2.0 admin/users/add cross site request forgery	A vulnerability was found in Gleez CMS 1.2.0. It has been rated as problematic. Affected by this issue is an unknown function of the file *admin/users/add*. The manipulation with an unknown input leads to a cross site request forgery vulnerability. Using CWE to declare the problem leads to CWE-352. Impacted is integrity. An attacker might be able force legitimate users to initiate unwanted actions within the web application. The weakness was released 08/25/2018. This vulnerability is handled as CVE-2018-15845 since	Protected by Custom Rules.

CVE-2018-11502	Moderator Log Notes Plugin 1.1 on MyBB Mod Note cross site request forgery	A vulnerability was found in Moderator Log Notes Plugin 1.1 on MyBB. It has been classified as problematic. Affected is an unknown function of the component *Mod Note Handler*. The manipulation with an unknown input leads to a cross site request forgery vulnerability. CWE is classifying the issue as CWE-352. This is going to have an impact on integrity, and availability. An attacker might be able force legitimate users to initiate unwanted actions within the web application. The weakness was	Protected by Custom Rules.
CVE-2018-15884	RICOH MP C4504ex Cross Site Request Forgery	The RICOH MP C4504ex printer suffers from a cross site request forgery vulnerability.	Protected by Custom Rules.