Weekly Zero-Day Vulnerability Coverage Bulletin

(20th August – 26th August)

Summary:

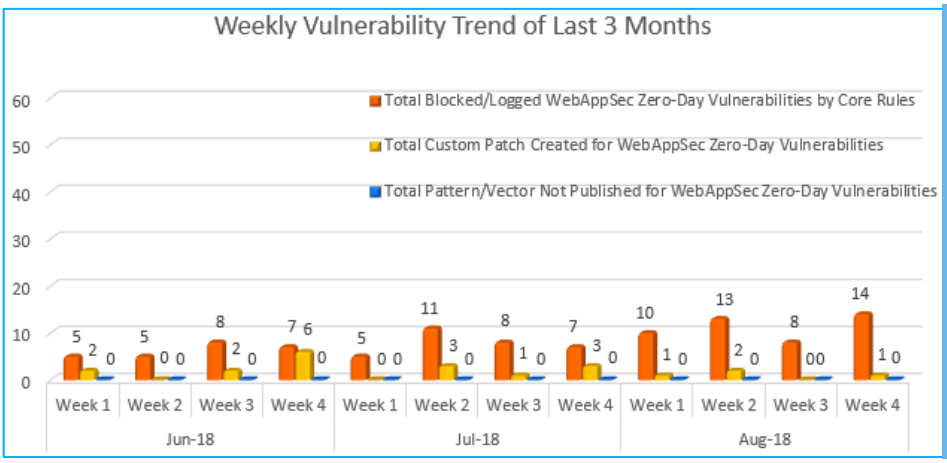
Total **15 Zero-Day Vulnerabilities** were discovered in **6 Categories** previous week

8	2	1	2	1	1
Cross Site Scripting	SQL Injection	Cross Site Request Forgery	Command Injection	Local File Inclusion	Apache Structs

Zero-Day Vulnerabilities Protected through Core Rules	14
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

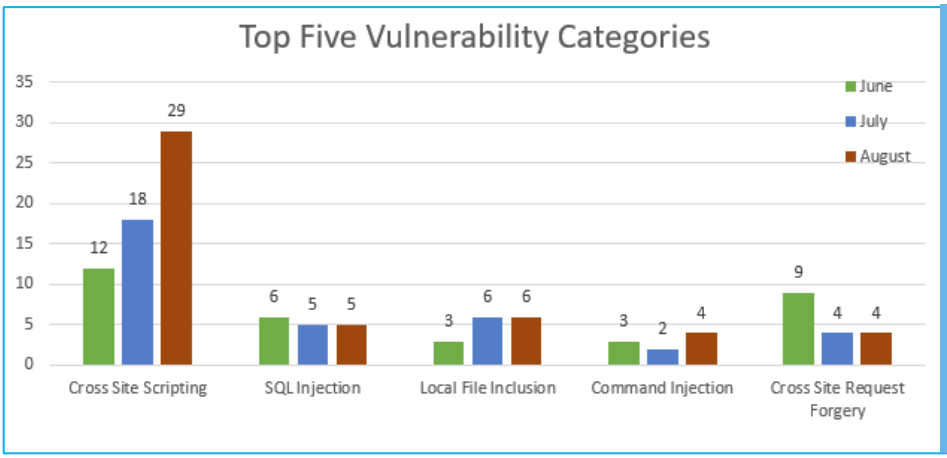
Vulnerability Trend:



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

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.

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	CVE-2018-15533	Geutebrueck re_porter 16 - Cross-Site Scripting	Geutebrueck re_porter 16 - Cross-Site Scripting	Protected by Default Rules.
		EDB-ID: 45236	ZyXEL VMG3312-B10B - Cross-Site Scripting	ZyXEL VMG3312-B10B - Cross-Site Scripting	Protected by Default Rules.
		EDB-ID: 149020	Countly Cross Site Scripting	Countly suffers from a persistent cross site scripting vulnerability.	Protected by Default Rules.
		EDB-ID: 149017	Subrion CMS 4.2.1 Cross Site Scripting	A content management system (CMS) is a computer application that supports the creation and modification of digital content. It is often used to support multiple users working in a collaborative environment. CMS features vary widely. Most CMS include Web-based publishing, format management, history editing and version control, indexing, search, and retrieval. By their nature, content management systems support the separation of content and presentation.	Protected by Default Rules.
		CVE-2018-10752	WordPress Tagregator 0.6 Cross Site Scripting	WordPress Tagregator plugin version 0.6 suffers from a cross site scripting vulnerability.	Protected by Default Rules.
		CVE-2014-0114	OSCAR EMR 15.21beta361 XSS / Disclosure / CSRF / Insecure Direct Object Reference	OSCAR EMR version 15.21beta361 suffers from remote code execution, cross site request forgery, cross site scripting, denial of service, deserialization, remote SQL injection, and path traversal vulnerabilities.	Protected by Default Rules.
		CVE-2018-15608	ManageEngine ADManager Plus 6.5.7 - HTML Injection	ZOHO Corp ManageEngine ADManager Plus 6.5.7 allows HTML Injection on # the "AD Delegation" "Help Desk Technicians" screen.	Protected by Default Rules.

		EDB-ID: 45256	ManageEngine ADManager Plus 6.5.7 - Cross-Site Scripting	Zoho ManageEngine ADManager Plus 6.5.7 allows Cross-Site Scripting on the "Workflow Delegation" "Requesters" screen.	Protected by Default Rules.
2.	SQL Injection	EDB-ID: 149035	Twitter-Clone 1 SQL Injection	Twitter-Clone version 1 suffers from a remote SQL injection vulnerability.	Protected by Default Rules.
		EDB-ID: 45255	WordPress Plugin Gift Voucher 1.0.5 - 'template_id' SQL Injection	The vulnerability allows an attacker to inject SQL commands # on 'template_id' parameter.	Protected by Default Rules.
3.	Local File Inclusion	EDB-ID: 149036	PCViewer vt1000 Directory Traversal	PCViewer vt1000 suffers from a directory traversal vulnerability.	Protected by Default Rules.
4.	Cross Site Request Forgery	EDB-ID: 45232	Twitter-Clone 1 - Cross-Site Request Forgery (Delete Post)	An issue was discovered in Twitter-Clone 1 which allows a remote # attacker to force any victim to delete posts.	Protected by Custom Rules.
5.	Command Injection	EDB-ID: 45234	Wordpress Plugin Ninja Forms 3.3.13 - CSV Injection	WordPress Ninja Forms plugin version 3.3.13 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 forms 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.
		CVE-2018-15576	Easylogin Pro 1.3.0 Remote Code Execution	Easylogin Pro version 1.3.0 suffers from a deserialization issue in Encryptor.php that permits a code execution vulnerability.	Protected by Default Rules.
6.	Apache Structs	CVE-2018-11776	Apache Struts up to 2.3.34/2.5.16 Namespace Code Execution	A vulnerability was found in Apache Struts up to 2.3.34/2.5.16. It has been declared as critical. Affected by this vulnerability is an unknown function of the component *Namespace Handler*. The manipulation with an unknown input leads to a privilege escalation	Protected by Default Rules.

		vulnerability (Code Execution). The CWE definition for the vulnerability is CWE-269. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was published in 08/22/2018. The advisory is shared at cwiki.apache.org. This vulnerability is known as CVE-2018-11776.