Weekly Zero-Day Vulnerability Coverage Bulletin

(13th August – 19th August)

Summary:

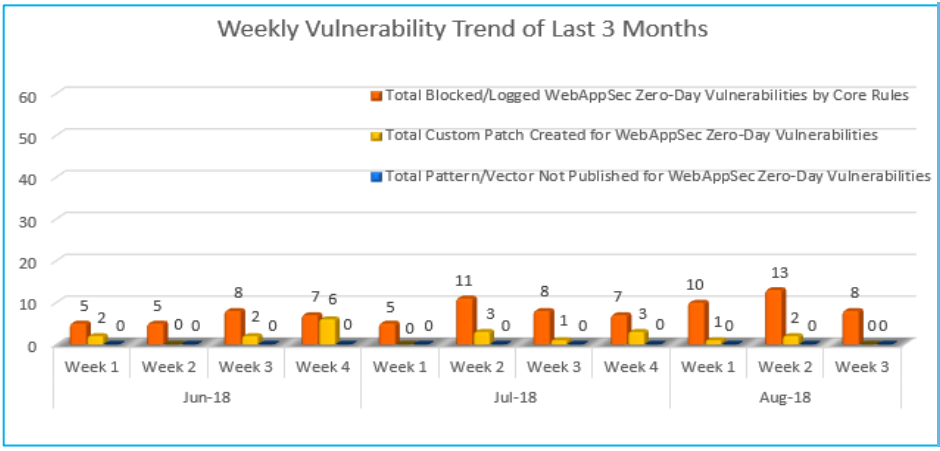
Total **8 Zero-Day Vulnerabilities** were discovered in **4 Categories** in this week

4	1	2	1
Cross Site Scripting	SQL Injection	Local File Inclusion	Command Injection

Zero-Day Vulnerabilities Protected through Core Rules	8
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

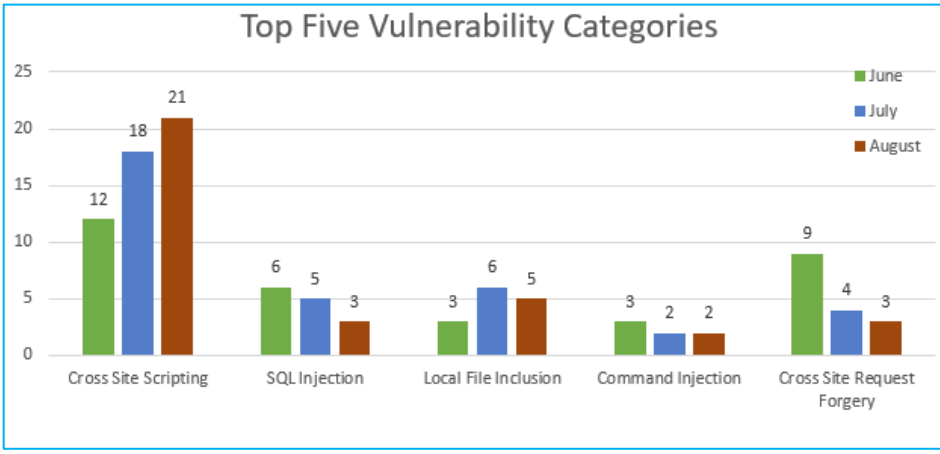
Vulnerability Trend:



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

76% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

24% 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 so far.

Very less SQL Injection attacks were 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: 148948	Atmosphere 1.x / 2.x Cross Site Scripting	Async-IO.org Atmosphere suffers from a Cross Site Scripting vulnerability. Versions affected include 2.4.0 through 2.4.28, 2.3.0 through 2.3.9, 2.2.0 through 2.2.12, 2.1.0 through 2.1.13, 2.0.0 through 2.0.11, and 1.0.0 through 1.0.20.	Protected by Default Rules.
		EDB-ID: 148949	ownCloud iOS Application 3.7.3 Cross Site Scripting	HTML pages will be rendered in a WebView in the ownCloud iOS application. JavaScript will be executed in this WebView when previewing an HTML file. The webview is run in a sandbox, so no other data can be read in a priory. However, in case the WebView itself were to have a vulnerability, an attacker could access other data of the application. The HTML rendering could also be misused for phishing.	Protected by Default Rules.
		CVE-2018-14057, CVE-2018-14058, CVE-2018-14059	Pimcore 5.2.3 CSRF / Cross Site Scripting / SQL Injection	Pimcore is an award-winning consolidated open source enterprise platform for master data management (PIM/MDM), user experience management (CMS/UX), digital asset management (DAM) and eCommerce.	Protected by Default Rules.
		EDB-ID: 148980	Silver Peak EdgeConnect 8.1.4.9_65644 XSS / DoS / Disclosure / Traversal	Silver Peak EdgeConnect version 8.1.4.9_65644 suffers from brute force, information leakage, cross site request forgery, cross site scripting, denial of service, default SNMP community string, and path traversal vulnerabilities.	Protected by Default Rules.
2.	SQL Injection	CVE-2018-11509	ASUSTOR ADM 3.1.0. RFQ3 - Remote Command Execution / SQL Injection	The Asustor NAS appliance on ADM 3.1.0 and the versions before having suffered from multiple critical vulnerabilities. The vulnerabilities were	Protected by Default Rules.

				submitted to Asustor in January and February 2018. Several follow-up requests were made in the attempt to obtain vendor acknowledgement, however no correspondence was ever received. Nevertheless, the vendor did patch the RCE issue in the 3.1.3 ADM release on May 31, 2018.	
3.	Local File Inclusion	CVE-2018-15140	OpenEMR 5.0.1.3 - Arbitrary File Actions	OpenEMR 5.0.1.3 - Arbitrary File Actions.	Protected by Default Rules.
		EDB-ID: 148979	WordPress Dreamsmiths Themes 0.0.1 Arbitrary File Download	WordPress Dreamsmiths Themes 0.0.1 Arbitrary File Download.	Protected by Default Rules
4.	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.