Weekly Zero-Day Vulnerability Coverage Bulletin

(9th July – 15th July)

Summary:

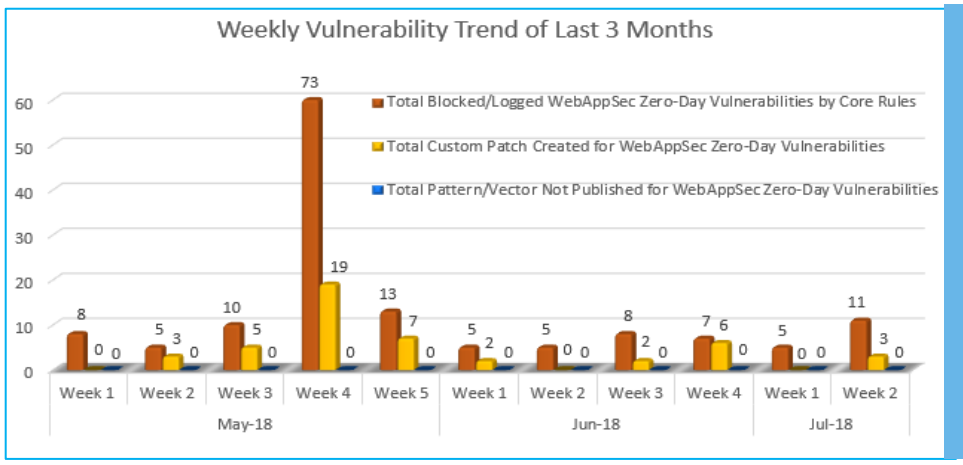
Total **14 Zero-Day Vulnerabilities** were discovered in **5 Categories** previous week

7	1	2	2	2
Cross Site Scripting	Cross Site Request Forgery	Arbitrary File Upload	Local File Inclusion	SQL Injection

Zero-Day Vulnerabilities Protected through Core Rules	11
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:

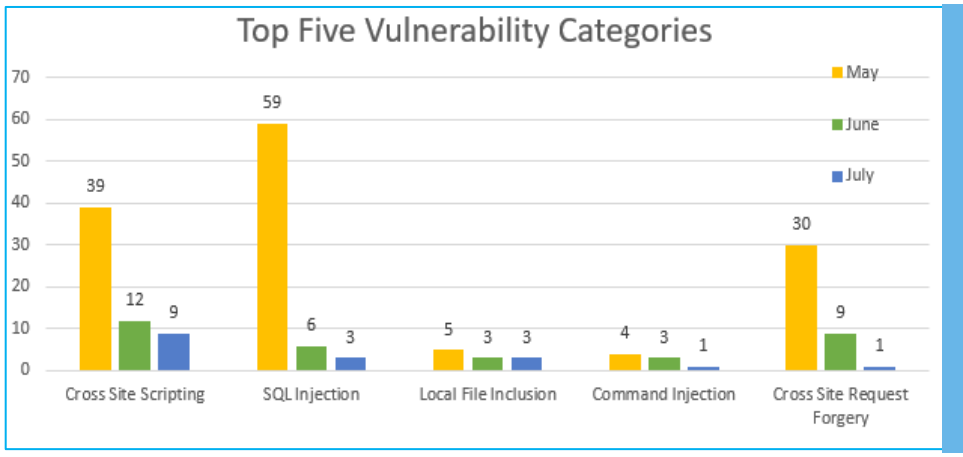


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

May 4th Week has multiple vulnerabilities blocked by Core Rules.

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 multiple SQL Injection vulnerabilities were discovered in May compared to other months and categories.

Medium no. of Cross Site Scripting attacks was found in May compared to June.

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: 44988	Umbraco CMS SeoChecker Plugin 1.9.2 - Cross-Site Scripting	SeoChecker Umbraco CMS Plug-in version 1.9.2 is vulnerable to stored cross-site scripting vulnerability in two parameters which are SEO title and SEO description	Protected by Default Rules.
		EDB-ID: 148499	Barracuda ADC 5.x Filter Bypass / Cross Site Scripting	Barracuda ADC versions 5.x suffer from filter bypass and cross site scripting vulnerabilities.	Protected by Default Rules.
		EDB-ID: 148500	Barracuda ADC 5.x Client-Side Script Insertion	Barracuda ADC versions 5.x suffer from a client-side script insertion vulnerability.	Protected by Default Rules.
		CVE-2018-13849	Instagram Clone Script 2.0 Cross Site Scripting	Instagram Clone Script version 2.0 suffers from a cross site scripting vulnerability.	Protected by Default Rules.
		EDB-ID: 148495	Secutech DSL WR RIS 330 Cross Site Scripting	Secutech DSL WR RIS 330 suffers from bypass and cross site scripting vulnerabilities.	Protected by Default Rules.
		EDB-ID: 148497	AT&T Bizcircle Cross Site Scripting	AT&T Bizcircle suffered from a persistent cross site scripting vulnerability.	Protected by Default Rules.
		EDB-ID: 148498	ASUS WRT-AC66U 3.x Cross Site Scripting	ASUS WRT-AC66U version 3.x suffers from a cross site scripting vulnerability.	Protected by Default Rules.
2.	SQL Injection	EDB-ID: 44999	Elektronischer Leitz-Ordner 10 - SQL Injection	We have discovered a time-based blind SQL injection vulnerability in the ELO Access Manager (<= 9.17.120 and <= 10.17.120) component that makes it possible to read all database content.	Protected by Default Rules.
		EDB-ID: 44997	WolfSight CMS 3.2 - SQL Injection	WolfSight CMS 3.2 - SQL Injection (Error Based)	Protected by Default Rules.
3.	Local File Inclusion	EDB-ID: 45007	Dicoogle PACS 2.5.0 - Directory Traversal	Dicoogle is an open source medical imaging repository with an extensible indexing system and distributed mechanisms. In version 2.5.0, it is vulnerable to local file inclusion. This allows an attacker to read arbitrary files that the web user has access to. Admin credentials aren't required. The 'UID' parameter via GET is vulnerable.	Protected by Default Rules.

		CVE-2018-13980	Zeta Producer Desktop CMS 14.2.0 - Remote Code Execution / Local File Disclosure	The attacker can upload .php5 or .phtml to the server without any restriction. These alternative file extensions can be executed as PHP code.	Protected by Default Rules.
4.	Cross Site Request Forgery	CVE-2018-13989	Grundig Smart Inter@ctive 3.0 - Cross-Site Request Forgery	Grundig Smart Inter@ctive 3.0 - Cross-Site Request Forgery	Protected by Custom Rules.
5.	Arbitrary File Upload	CVE-2017-18048	Monstra CMS Authenticated Arbitrary File Upload	Monstra CMS 3.0.4 allows users to upload arbitrary files which leads to remote command execution on the remote server. An attacker may choose to upload a file containing PHP code and run this code by accessing the resulting PHP file. This Metasploit module was tested against Monstra CMS 3.0.4.	Protected by Custom Rules.
		CVE-2018-12979, CVE-2018-12980, CVE-2018-12981	WAGO e!DISPLAY 7300T XSS / File Upload / Code Execution	WAGO e!DISPLAY 7300T WP 4.3 480x272 PIO1 version FW 01 - 01.01.10(01) suffer from code execution, cross site scripting, weak permission, and remote file upload vulnerabilities.	Protected by Custom Rules.