Weekly Zero-Day Vulnerability Coverage Bulletin

(2nd July – 8th July)

Summary:

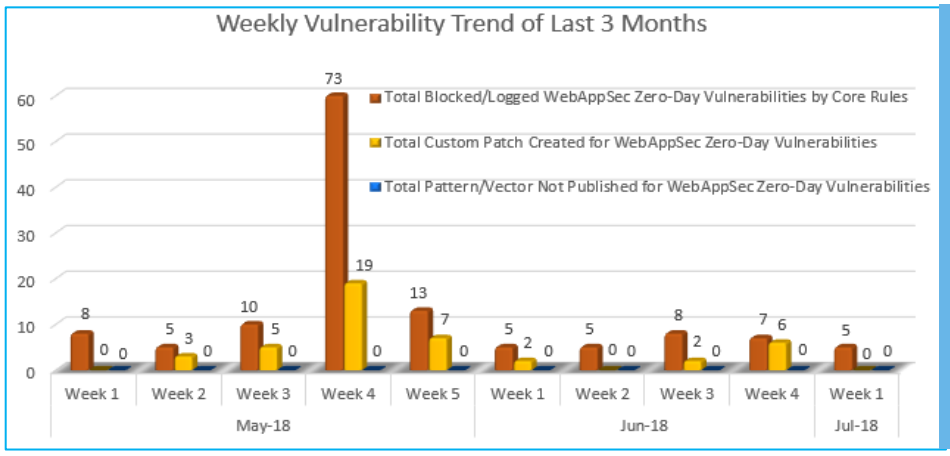
Total **5 Zero-Day Vulnerabilities** were discovered in **4 Categories** previous week

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

Zero-Day Vulnerabilities Protected through Core Rules	5
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:

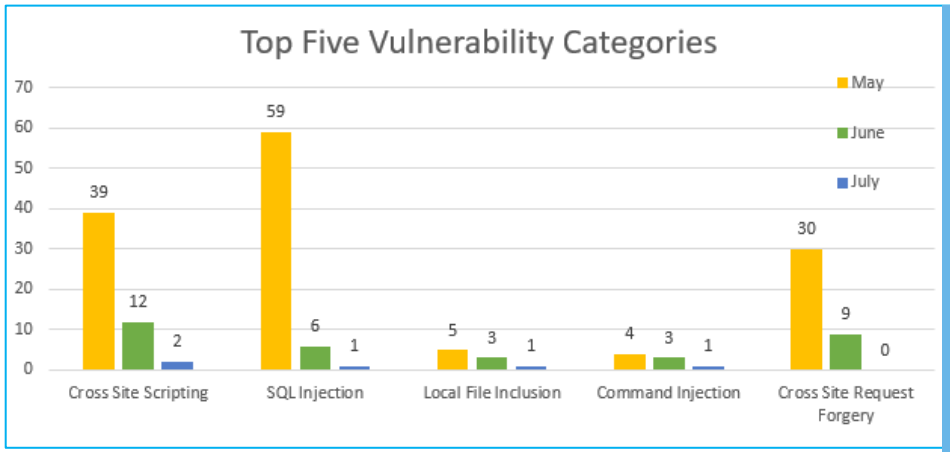


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

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 were 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	CVE-2018-8046	Sencha Ext JS up to 4.x/5.x/6.5.x XSS Protection getTip() cross site scripting	A vulnerability was found in Sencha Ext JS up to 4.x/5.x/6.5.x. It has been declared as problematic. Affected by this vulnerability is the function getTip() of the component *XSS Protection*. 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 web site. This would alter the	Protected by Default Rules.
		CVE-2017-11175	J2 Innovations FIN Stack 4.0 Webform /auth/ariosa/login Query String cross site scripting	A vulnerability, which was classified as problematic, was found in J2 Innovations FIN Stack 4.0. This affects an unknown function of the file */auth/ariosa/login* of the component *Webform*. The manipulation as part of a *Query String* leads to a cross site scripting vulnerability (Reflected). CWE is classifying the issue as CWE-80. This is going to have an impact on integrity. An attacker might be able to inject arbitrary html and script code into the web site. This would alter the	Protected by Default Rules.
2.	SQL Injection	EDB-ID: 44981	SoftExpert Excellence Suite 2.0 - 'cddocument' SQL Injection	A SQL injection vulnerability in the SoftExpert (SE) Excellence Suite 2.0 allows remote authenticated users to perform SQL heuristics by pulling information from the database with the "cddocument" parameter in the "Downloading Electronic Documents" section.	Protected by Default Rules.
3.	Local File Inclusion	CVE-2018-12976	Go Doc Dot Org up to 2018-06-	A vulnerability was found in Go Doc Dot Org	Protected by Default Rules.

			27 Package Code Execution directory traversal	up to 2018-06-27. It has been classified as critical. This affects an unknown function of the component *Package Handler*. The manipulation with an unknown input leads to a directory traversal vulnerability (Code Execution). CWE is classifying the issue as CWE-22. This is going to have an impact on confidentiality, integrity, and availability. The summary by CVE is:In Go Doc Dot Org (gddo) through 2018-06-27, an attacker could use specially crafted tags.	
4.	Command Injection	CVE-2018-11526	Wordpress Plugin Comments Import & Export < 2.0.4 - CSV Injection	WordPress Comments Import & Export plugin version 2.0.4 and before are affected by the vulnerability Remote Command Execution using CSV Injection. This allows a public user to inject commands as a part of form fields and when a user with higher privilege exports the form data in CSV opens the file on their machine, the command is executed.	Protected by Default Rules.