Weekly Zero-Day Vulnerability Coverage Bulletin

(16th July – 22nd July)

Summary:

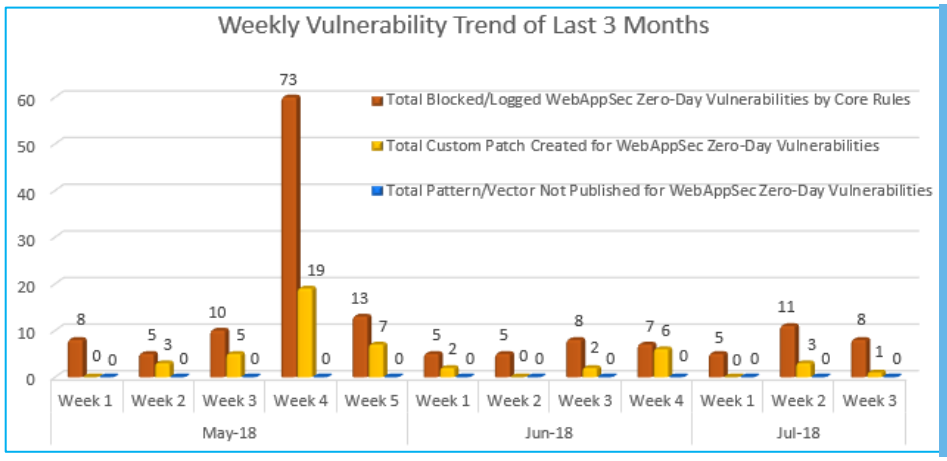
Total **9 Zero-Day Vulnerabilities** were discovered in **3 Categories** previous week

6	2	1
Cross Site Scripting	SQL Injection	Arbitrary File Upload

Zero-Day Vulnerabilities Protected through Core Rules	8
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:

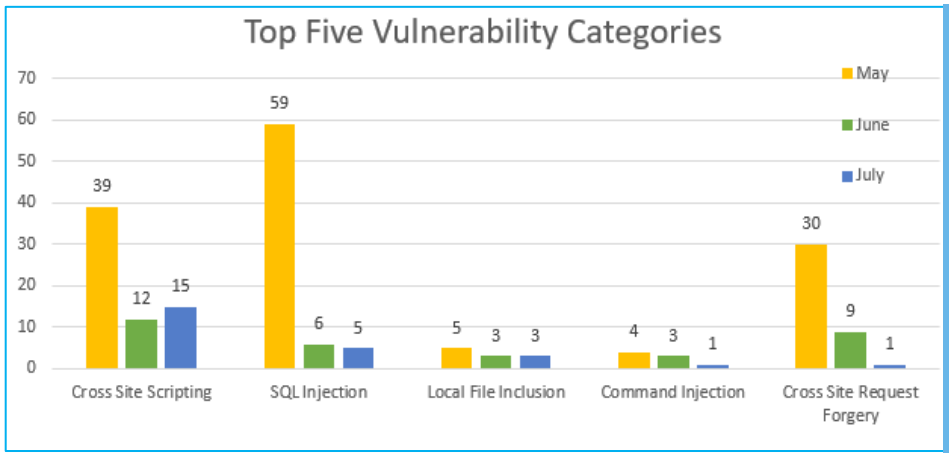


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

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	CVE-2018-5232	Atlassian JIRA up to 7.6.6/7.10.0 EditIssue.jspa issuetype cross site scripting	A vulnerability has been found in Atlassian JIRA up to 7.6.6/7.10.0 and classified as problematic. Affected by this vulnerability is an unknown function of the file *EditIssue.jspa*. The manipulation of the argument issuetype as part of a *Parameter* 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.	Protected by Default Rules.
		CVE-2018-14388	joyplus-cms 1.6.0 manager/admin_ajax.php can_search_device cross site scripting	A vulnerability was found in joyplus-cms 1.6.0. It has been classified as problematic. Affected is an unknown function of the file *manager/admin_ajax.php*. The manipulation of the argument can_search_device as part of a *Parameter* leads to a cross site scripting vulnerability. 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.	Protected by Default Rules.
		EDB-ID: 148604	GhostMail Status Message HTML Injection	GhostMail suffers from an html injection vulnerability.	Protected by Default Rules.
		EDB-ID: 148603	GhostMail Filename to Link Script Insertion	GhostMail suffers from a malicious script insertion vulnerability.	Protected by Default Rules.
		EDB-ID: 148602	Barracuda Cloud Control 3.020 Cross Site Scripting	Barracuda Cloud Control version 3.020 suffers from a cross site scripting vulnerability.	Protected by Default Rules.
		EDB-ID: 148599	Barracuda Cloud Control 7.1.1.003 Cross Site Scripting	Barracuda Cloud Control version 7.1.1.003 suffers from a cross site scripting vulnerability.	Protected by Default Rules.

2.	SQL Injection	CVE-2018-1438	joyplus-cms 1.6.0 manager/admin_ajax.php val sql injection	A vulnerability was found in joyplus-cms 1.6.0. It has been declared as critical. Affected by this vulnerability is an unknown function of the file *manager/admin_ajax.php*. The manipulation of the argument val as part of a *Parameter* leads to a sql injection vulnerability. The CWE definition for the vulnerability is CWE-89. As an impact it is known to affect confidentiality, integrity, and availability. An attacker might be able inject and/or alter existing SQL statements which would influence the database exchange.	Protected by Default Rules.
		EDB-ID: 148600	Smart SMS And Email Manager 3.3 SQL Injection	Smart SMS and Email Manager version 3.3 suffers from a remote SQL injection vulnerability.	Protected by Default Rules.
3.	HTTP Policy Violence	EDB-ID: 148589	FTP2FTP 1.0 Arbitrary File Download	FTP2FTP version 1.0 suffers from an arbitrary file download vulnerability.	Protected by Custom Rules.