Weekly Zero-Day Vulnerability Coverage Bulletin

(4th June – 10th June)

Summary:

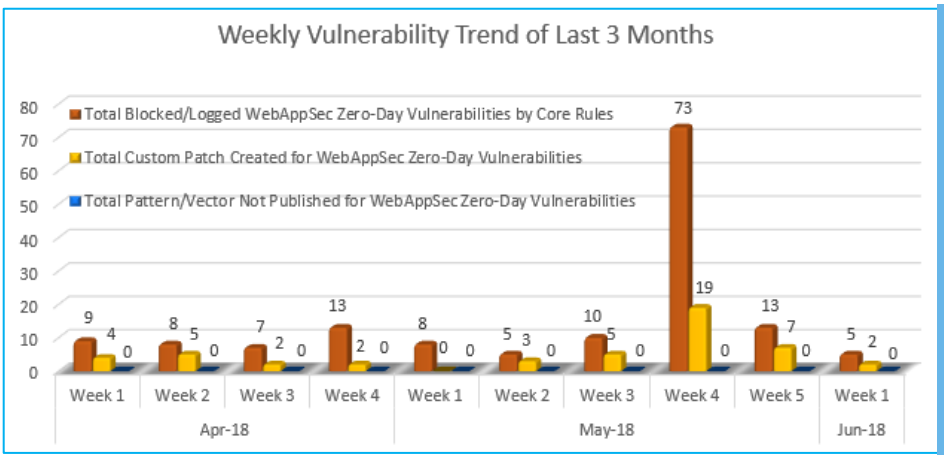
Total **7 Zero-Day Vulnerabilities** were discovered in **4 Categories** previous week

3	1	1	2
Cross Site Scripting	SQL Injection	Local File Inclusion	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	5
Zero-Day Vulnerabilities Protected through Custom Rules	2*
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:

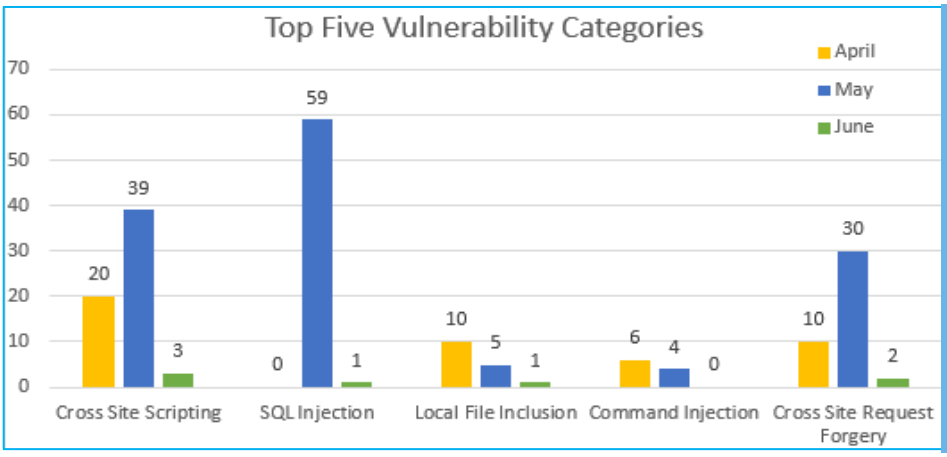


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

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

75% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

25% 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 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-2018-11709	wpForo Forum plugin up to 1.4.11 on WordPress functions.php Cross Site Scripting	A vulnerability classified as problematic was found in wpForo Forum plugin up to 1.4.11 on WordPress. This vulnerability affects an unknown function of the file *wpf-includes/functions.php*. The manipulation with an unknown input leads to a cross site scripting vulnerability (Reflected). 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 website.	Protected by Default Rules.
		CVE-2017-7636	QNAP Proxy Server up to 1.2.0 cross site scripting [CVE-2017-7636]	A vulnerability was found in QNAP Proxy Server up to 1.2.0 and classified as problematic. This issue affects an unknown function. The manipulation with an unknown input leads to a cross site scripting vulnerability. Using CWE to declare the problem leads to CWE-80. Impacted is integrity. An attacker might be able to inject arbitrary html and script code into the web site. This would alter the appearance and would make it possible to initiate further attacks against site visitors.	Protected by Default Rules.
		CVE-2016-9490	ManageEngine Applications Manager 12/13 LIMIT cross site scripting	A vulnerability was found in ManageEngine Applications Manager 12/13 and classified as problematic. This issue affects an unknown function of the file */DiagAlertAction.do?REQTYPE=AJAX/LIMIT=1233*. The manipulation of the argument LIMIT as part of a *Parameter* leads to a cross site scripting vulnerability (Reflected). Using CWE to declare the problem leads to CWE-80.	Protected by Default Rules.

				Impacted in integrity. An attacker might be able to inject arbitrary html and script code into the web site. This would alter the appearance and would make the attack possible.	
2.	SQL Injection	CVE-2018-12055	PHP Scripts Mall Schools Alert Management Script contact_us.php Contact SQL Injection	A vulnerability classified as critical has been found in PHP Scripts Mall Schools Alert Management Script (the affected version is unknown). Affected is an unknown function of the file *contact_us.php*. The manipulation as part of a *Contact* leads to a SQL Injection vulnerability. CWE is classifying the issue as CWE-89. This is going to have an impact on confidentiality, integrity, and availability. An attacker might be able to inject and/or alter existing SQL statements which would influence the database exchange.	Protected by Default Rules.
3.	Local File Inclusion	CVE-2018-10615	GE MDS PulseNET/MDS PulseNET Enterprise 3.2.1 directory traversal	A vulnerability classified as critical has been found in GE MDS PulseNET and MDS PulseNET Enterprise 3.2.1. This affects an unknown function. The manipulation with an unknown input leads to a directory traversal vulnerability. 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 Directory traversal may lead to files being exfiltrated or deleted on the GE MDS PulseNET and MDS PulseNET Enterprise version 3.2.1 and prior.	Protected by Default Rules.

4.	Cross Site Request Forgery	CVE-2017-7635	QNAP Proxy Server up to 1.2.0 cross site request forgery [CVE-2017-7635]	A vulnerability has been found in QNAP Proxy Server up to 1.2.0 and classified as problematic. This vulnerability affects an unknown function. The manipulation with an unknown input leads to a cross site request forgery vulnerability. The CWE definition for the vulnerability is CWE-352. As an impact it is known to affect integrity. An attacker might be able force legitimate users to initiate unwanted actions within the web application. The weakness was shared on 06/01/2018 in *NAS-201806-01* as confirmed security advisory.	Protected by Custom Rules.
		CVE-2018-8925	Synology Photo Station up to 6.8.5 admin/user.php modify_admin cross site request forgery	A vulnerability was found in Synology Photo Station up to 6.8.5 and classified as problematic. This issue affects an unknown function of the file *admin/user.php*. The manipulation of the argument to modify admin as part of a *Parameter* leads to a cross site request forgery vulnerability. Using CWE to declare the problem leads to CWE-352. Impacted in integrity. An attacker might be able force legitimate users to initiate unwanted actions within the web application. The weakness was released in 06/08/2018.	Protected by Custom Rules.