Weekly Zero-Day Vulnerability Coverage Bulletin

(10th June – 16th June)

Summary:

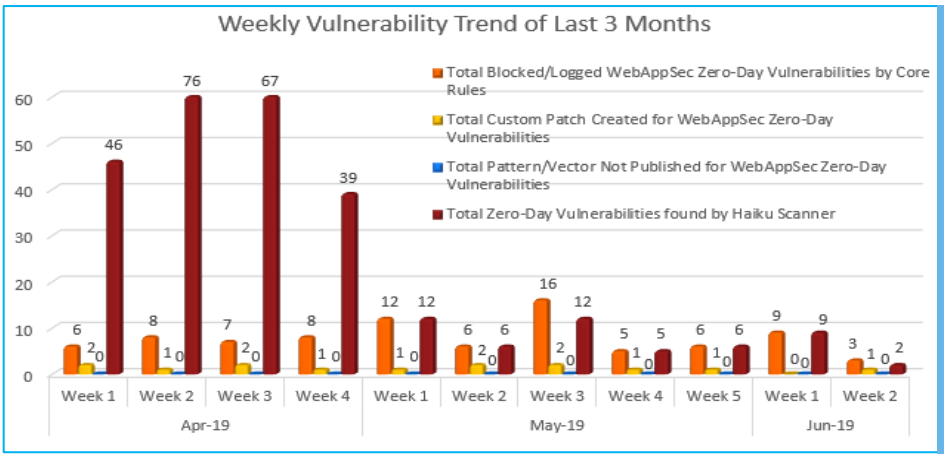
Total **4 Zero-Day Vulnerabilities** were discovered in **3 Categories** this week

2	1	1
Cross Site Scripting	SQL Injection	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	3
Zero-Day Vulnerabilities Protected through Custom Rules	1*
Zero-Day Vulnerabilities for which protection cannot be determined	0**
Zero-Day Vulnerabilities found by Haiku Scanner	2

* 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:

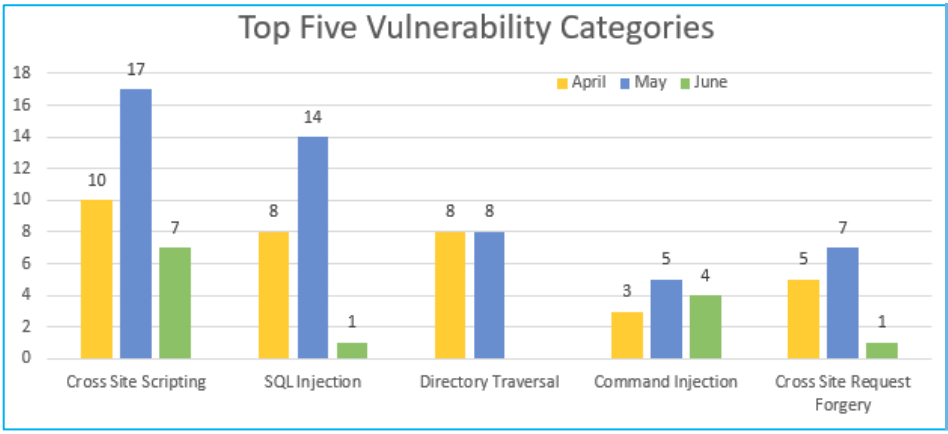


Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a quarter.

74% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

12% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

14% Of Zero-Day Vulnerabilities were reported by Haiku Scanner in last quarter



From the graph, we infer that maximum Cross Site Scripting vulnerabilities are discovered in May compared to other months.

No Directory Traversal vulnerabilities are found in 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	Haiku Scanner Coverage
1.	Cross Site Scripting	CVE-2019-10226	Fat Free CRM 0.19.0 /comments cross site scripting	A vulnerability classified as problematic has been found in Fat Free CRM 0.19.0 (Customer Relationship Management System). This affects an unknown part of the file */comments*. The manipulation with an unknown input leads to a cross site scripting vulnerability (HTML Injection). CWE is classifying the issue as CWE-79. This is going to have an impact on integrity. An attacker might be able to inject arbitrary html and script code into the website. This would alter the appearance.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2019-12765	Joomla CMS up to 3.9.6 Subform cross site scripting	A vulnerability classified as problematic has been found in Joomla CMS up to 3.9.6 (Content Management System). This affects an unknown function of the component *Subform Handler*. The manipulation with an unknown input 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 website. This would alter the appearance.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	SQL Injection	CVE-2019-9087	HotelDruid up to 2.3.0 /tab_tariffe.php numtariffa1 sql injection	A vulnerability was found in HotelDruid up to 2.3.0 (Hospitality Software). It has been declared as critical. This vulnerability affects some unknown processing of the file	Protected by Default Rules.	NA

				/tab_tariffe.php. The manipulation of the argument numtariffa1 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.		
3.	Cross Site Request Forgery	CVE-2019-11517	WampServer up to 3.1.8 Synchronizer Pattern add_vhost.php cross site request forgery	A vulnerability, which was classified as problematic has been found in WampServer up to 3.1.8. This issue affects an unknown code block of the file *add_vhost.php* of the component *Synchronizer Pattern Handler*. The manipulation with an unknown input leads to a cross site request forgery vulnerability. Using CWE to declare the problem leads to CWE-352. Impacted is integrity. An attacker might be able force legitimate users to initiate unwanted actions within the web application. The weakness was presented in 06/10/2019.	Protected by Custom Rules.	NA