Weekly Zero-Day Vulnerability Coverage Bulletin

(17th June – 23rd June)

Summary:

Total **6 Zero-Day Vulnerabilities** were discovered in **4 Categories** in this week

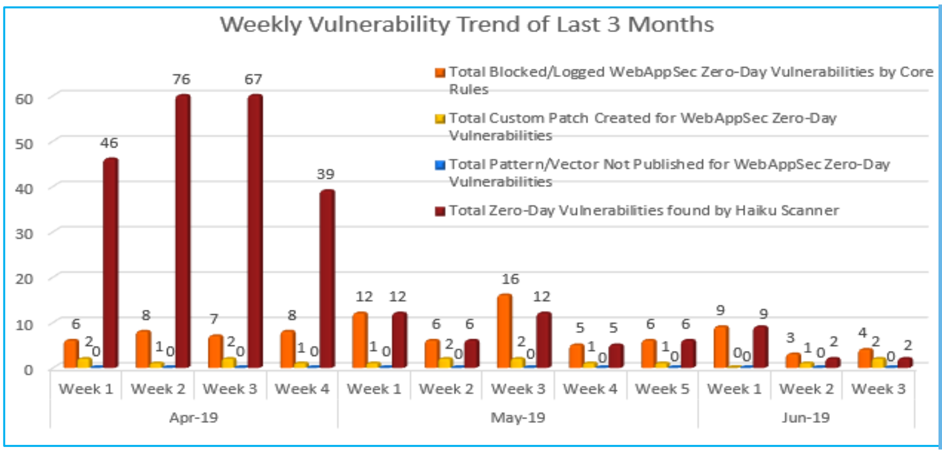
1 Cross Site Scripting	**2** SQL Injection	**1** Command Injection	**2** Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	4
Zero-Day Vulnerabilities Protected through Custom Rules	2*
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

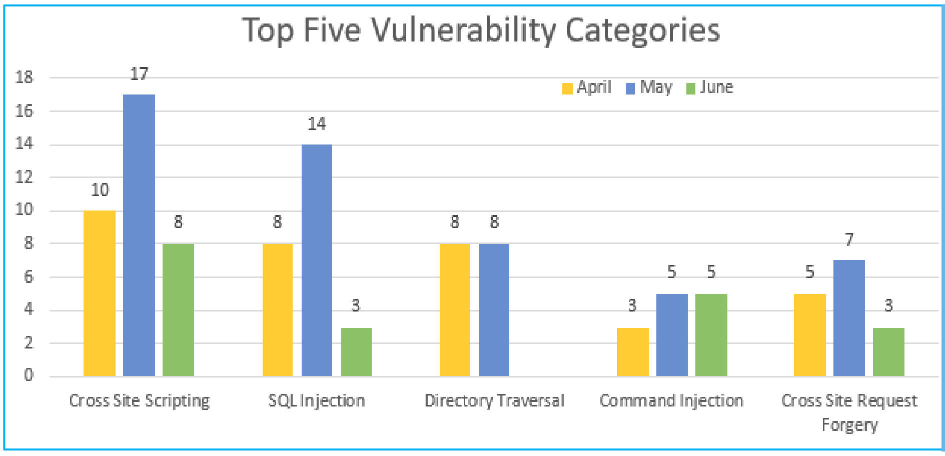
** Since attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected

Vulnerability Trend:



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

86%	Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter	**14%**	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, and SQL Injection vulnerabilities were discovered in May compared to other months and categories so far.

Zero 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-2019-0316	SAP NetWeaver Process Integration up to 7.50 Reflected cross site scripting	A vulnerability was found in SAP NetWeaver Process Integration up to 7.50 (Solution Stack Software) and classified as problematic. Affected by this issue is an unknown functionality. The manipulation with an unknown input leads to a cross site scripting vulnerability (Reflected). 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 website. This would alter the appearance and would make it possible.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	SQL Injection	CVE-2019-12872	dotCMS up to 5.1.5 view_unpushed_bundles.jsp sql injection	A vulnerability classified as critical was found in dotCMS up to 5.1.5 (Content Management System). Affected by this vulnerability is some unknown functionality of the file *view_unpushed_bundles.jsp*. The manipulation with an unknown input lead 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.	NA
		CVE-2018-15892	FreePBX 13.x/14.x DISA Module config.php hangup sql injection	A vulnerability has been found in FreePBX 13.x/14.x and classified as critical. Affected by this vulnerability is an unknown code of the file */admin/config.php?display	Protected by Default Rules.	NA

				=disa&view=form* of the component *DISA Module*. The manipulation of the argument hangup as part of a *Variable* 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 to inject and/or alter existing SQL statements which would influence.		
3.	Command Injection	CVE-2019-8324	RubyGems up to 3.0.2 Code Execution [CVE-2019-8324]	A vulnerability was found in RubyGems up to 3.0.2 (Programming Language Software) and classified as critical. Affected by this issue is an unknown function. The manipulation with an unknown input leads to a privilege escalation vulnerability (Code Execution). Using CWE to declare the problem leads to CWE-269. Impacted is confidentiality, integrity, and availability. The bug was discovered in 03/05/2019. The weakness was presented in 06/17/2019. This vulnerability is handled as CVE-2019-8324 since 02/13/2019. The technical details are unknown.	Protected by Default Rules.	Detected by scanner as Command Injection attack.
4.	Cross Site Request Forgery	CVE-2019-6325	HP Embedded Web Server cross site request forgery [CVE-2019-6325]	A vulnerability was found in HP Color LaserJet Pro M280-M281 Multifunction Printer and LaserJet Pro MFP M28-M31 Printer (Printing Software) (version unknown). It has been classified as problematic. Affected is some unknown processing of the component *Embedded Web Server*. The manipulation with an unknown input leads to a cross site request forgery vulnerability. CWE is classifying the issue as CWE-	Protected by Custom Rules.	NA

			352. This is going to have an impact on integrity. An attacker might be able force legitimate users to initiate unwanted.		
	CVE-2019-4142	IBM Cloud Private 2.1.0/3.1.0/3.1.1/3.1.2 cross site request forgery	A vulnerability, which was classified as critical, has been found in IBM Cloud Private 2.1.0/3.1.0/3.1.1/3.1.2 (Cloud Software). Affected by this issue is an unknown. 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 confidentiality, integrity, and availability. An attacker might be able force legitimate users to initiate unwanted actions within the web application. The weakness was disclosed in 06/18/2019.	Protected by Custom Rules.	NA