Weekly Zero-Day Vulnerability Coverage Bulletin

(24th June – 30th June)

Summary:

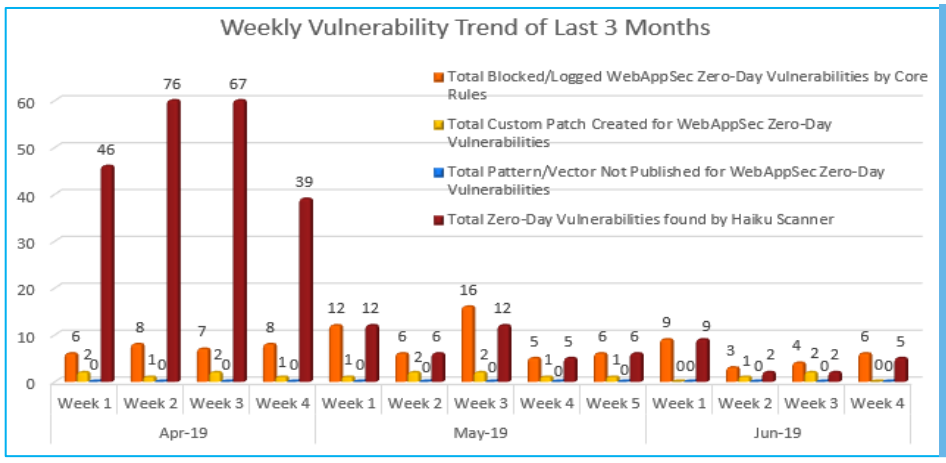
Total **6 Zero-Day Vulnerabilities** were discovered in **3 Categories** this week

3	1	2
Cross Site Scripting	SQL Injection	Command injection

Zero-Day Vulnerabilities Protected through Core Rules	6
Zero-Day Vulnerabilities Protected through Custom Rules	0*
Zero-Day Vulnerabilities for which protection cannot be determined	0**
Zero-Day Vulnerabilities found by Haiku Scanner	5

* 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:

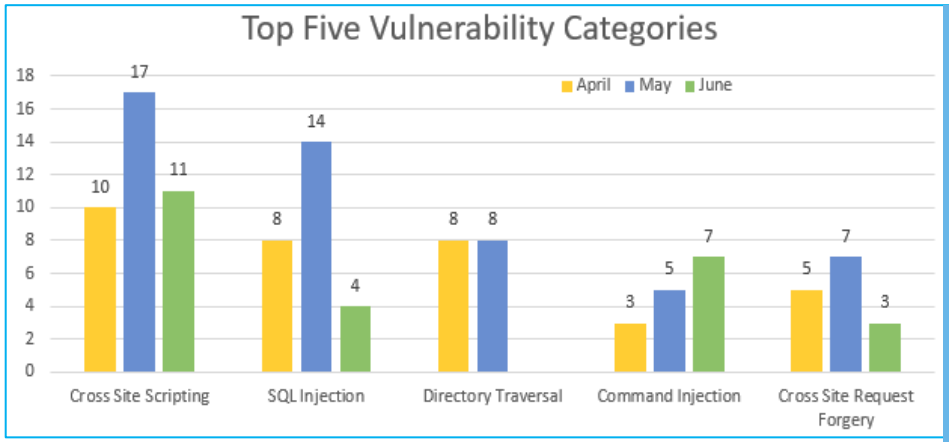


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

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 no. of Cross Site Scripting and SQL Injection 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-2019-1274	SeedDMS up to 5.1.10 out/out.UsrMgr .php name cross site scripting	A vulnerability was found in QEMU up to 4.0.0 (Virtualization Software). It has been rated as very critical. This issue affects some unknown processing of the component *QMP Migrate Command Handler*. The manipulation with an unknown input leads to a privilege escalation vulnerability (Code Execution). Using CWE to declare the problem leads to CWE-78. Impacted is confidentiality, integrity, and availability. The summary by CVE is the QMP migrate command in QEMU version 4.0.0 and earlier is vulnerable to OS command injection.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2019-12935	Shopware up to 5.5.7 Backend Query String cross site scripting	A vulnerability has been found in PIX-Link LV-WR09 v28K.MiniRouter.20180616 and classified as problematic. Affected by this vulnerability is some unknown functionality of the component *ESSID Handler*. 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 website.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2019-4157	IBM Security Access Manager up to 9.0.6 Web UI cross site scripting	A vulnerability classified as critical has been found in QEMU up to 4.0.0 (Virtualization Software). Affected is an unknown function of the component *QMP guest_exec Command Handler*. The manipulation with an unknown input leads to a	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.

				privilege escalation vulnerability (Code Execution). CWE is classifying the issue as CWE-269. This is going to have an impact on confidentiality, integrity, and availability. The weakness was released in 06/24/2019. This vulnerability is traded as CVE-2019-12929 since 06/20/2019.		
2.	SQL Injection	CVE-2019-12939	LiveZilla up to 8.0.1.0 server.php p_ext_rse sql injection	A vulnerability was found in LiveZilla up to 8.0.1.0 and classified as critical. Affected by this issue is an unknown function of the file *server.php*. The manipulation of the argument p_ext_rse as part of a *Parameter* leads to a sql injection vulnerability. Using CWE to declare the problem leads to CWE-89. Impacted is confidentiality, integrity, and availability. An attacker might be able inject and/or alter existing SQL statements which would influence the database exchange. The weakness was published 06/24/2019.	Protected by Default Rules.	NA
3.	Command Injection	CVE-2019-12928	QEMU up to 4.0.0 QMP Migrate Command Remote Code Execution	A vulnerability was found in ToaruOS up to 1.10.9. It has been declared as critical. This vulnerability affects an unknown code block of the file *apps/gsudo.c* of the component *gsudo*. The manipulation of the argument DISPLAY as part of a *Environment Variable* leads to a memory corruption vulnerability. The CWE definition for the vulnerability is CWE-119. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was shared 06/23/2019. This vulnerability was named CVE-2019-12937 since 06/23/2019.	Protected by Default Rules.	Detected by scanner as Command Injection attack.

CVE-2019-12929	QEMU up to 4.0.0 QMP guest_exec Command Code Execution	A vulnerability classified as critical has been found in QEMU up to 4.0.0 (Virtualization Software). Affected is an unknown function of the component *QMP guest_exec Command Handler*. The manipulation with an unknown input leads to a privilege escalation vulnerability (Code Execution). CWE is classifying the issue as CWE-269. This is going to have an impact on confidentiality, integrity, and availability. The weakness was released 06/24/2019. This vulnerability is traded as CVE-2019-12929 since 06/20/2019.	Protected by Default Rules.	Detected by scanner as Command Injection attack.