Weekly Zero-Day Vulnerability Coverage Bulletin

(3rd June – 9th June)

Summary:

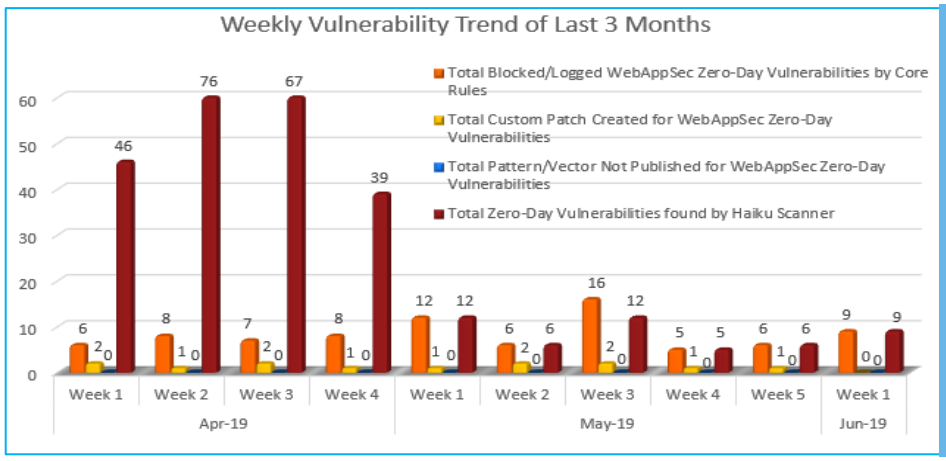
Total **9 Zero-Day Vulnerabilities** were discovered in **2 Categories** this week

5	**4**
Cross Site Scripting	Command Injection

Zero-Day Vulnerabilities Protected through Core Rules	9
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	9

* 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:

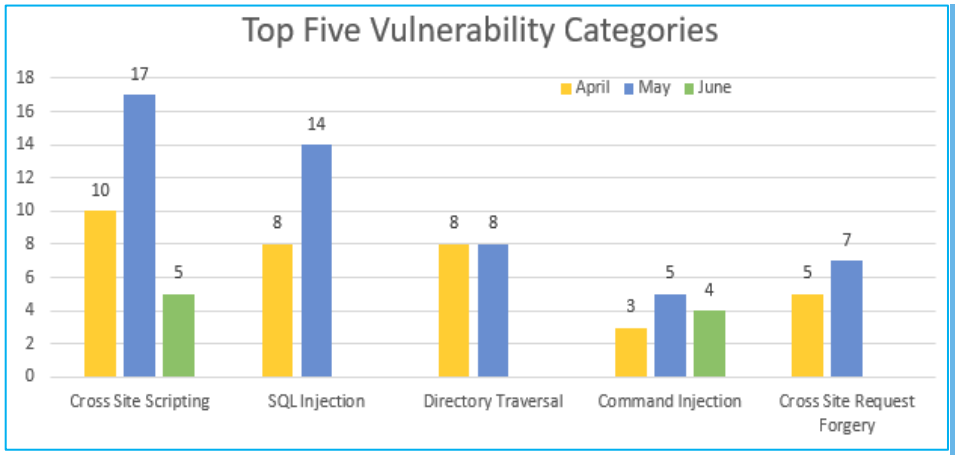


Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.

75% 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

13% Of Zero-Day Vulnerabilities were reported by Haiku Scanner in last quarter



From the graph, we infer that maximum Cross Site Scripting, SQL Injection vulnerabilities were discovered in May compared to other months and categories so far.

Zero Directory Traversal and CSRF vulnerabilities are found in June so far.

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-2019-12584	apcupsd up to 0.3.91_5 apcupsd_status.php cross site scripting	A vulnerability was found in apcupsd up to 0.3.91_5 (Printing Software). It has been rated as problematic. This issue affects some processing of the file *apcupsd_status.php*. 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 website. This would alter the appearance and would make it possible to initiate further problems.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2019-9839	VFront 0.99.5 admin/menu_registri.php azzera cross site scripting	A vulnerability, which was classified as problematic, has been found in VFront 0.99.5. This issue affects some functionality of the file *admin/menu_registri.php*. The manipulation of the argument azzera as part of a *Parameter* 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.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2019-9838	VFront 0.99.5 admin/sync_reg_tab.php azzera cross site scripting	A vulnerability classified as problematic was found in VFront 0.99.5. This vulnerability affects the functionality of the file *admin/sync_reg_tab.php*. The manipulation of the argument azzera as a part of a *Parameter* leads to a cross site scripting	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.

				vulnerability (Stored). 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. This would alter the appearance.		
		NA	Multiple Vulnerabilities in the WordPress Ultimate Member Plugin	The Ultimate member plugin version 2.0.45 and lower is affected by multiple vulnerabilities, among them is a critical vulnerability allowing malicious users to read and delete your wp-config.php file, which can lead to a complete website takeover.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		NA	Malicious JavaScript injected into WordPress sites using the latest plugin vulnerability	A stored cross-site script vulnerability was discovered last week in the popular WordPress Live Chat Support plugin. The vulnerability allows an unauthenticated attacker to update the plugin settings by calling an unprotected "admin_init hook" and injecting malicious JavaScript code everywhere on the site where Live Chat Support appears. All versions of this plugin prior to version 8.0.27 are vulnerable. The patched version for this vulnerability was released on 16th May 2019 and has been fixed for version 8.0.27 and higher.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	Command Injection	CVE-2019-12585	apcupsd up to 0.3.91_5 apcupsd_status.php Code Execution	A vulnerability classified as critical has been found in apcupsd up to 0.3.91_5 (WordPress Plugin). Affected is an unknown function of the file *apcupsd_status.php*. 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,	Protected by Default Rules.	Detected by scanner as Command Injection attack.

		integrity, and availability. The weakness was released 06/03/2019. This vulnerability is traded as CVE-2019-12585 since 06/02/2019. Technical details are known, but there is no available exploit.		
CVE-2019-9156	Gemalto DS3 Authentication Server 2.6.1-SP01 OS Command Injection privilege escalation	A vulnerability has been found in Gemalto DS3 Authentication Server 2.6.1-SP01 and classified as critical. This vulnerability affects a functionality. The manipulation with an unknown input leads to a privilege escalation vulnerability (OS Command Injection). The CWE definition for the vulnerability is CWE-77. As an impact it is known to affect confidentiality, integrity, and availability. The bug was discovered in 05/09/2019. The weakness was disclosed in 06/05/2019. This vulnerability was named as CVE-2019-9156 since 02/25/2019. The technical details are unknown.	Protected by Default Rules.	Detected by scanner as Command Injection attack.
CVE-2019-5393	HPE Intelligent Management Center PLAT up to 7.3 E0506P09 Remote Code Execution	A vulnerability was found in HPE Intelligent Management Center PLAT up to 7.3 E0506P09 (Log Management Software). It has been declared as critical. This vulnerability affects a code block. The manipulation with an unknown input leads to a privilege escalation vulnerability (Code Execution). The CWE definition for the vulnerability is CWE-269. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was released in 05/09/2019 as *HPESBHF03930* as confirmed security bulletin (Website).	Protected by Default Rules.	Detected by scanner as Command Injection attack.

CVE-2019-5390	HPE Intelligent Management Center PLAT up to 7.3 E0506P09 command injection	A vulnerability has been found in HPE Intelligent Management Center PLAT up to 7.3 E0506P09 (Log Management Software) and classified as critical. Affected by this vulnerability is a functionality. The manipulation with an unknown input leads to a privilege escalation vulnerability (Command Injection). The CWE definition for the vulnerability is CWE-88. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was presented in 05/09/2019 as *HPESBHF03930* as confirmed security bulletin (Website).	Protected by Default Rules.	Detected by scanner as Command Injection attack.