Weekly Zero-Day Vulnerability Coverage Bulletin

(22nd July – 28th July)

Summary:

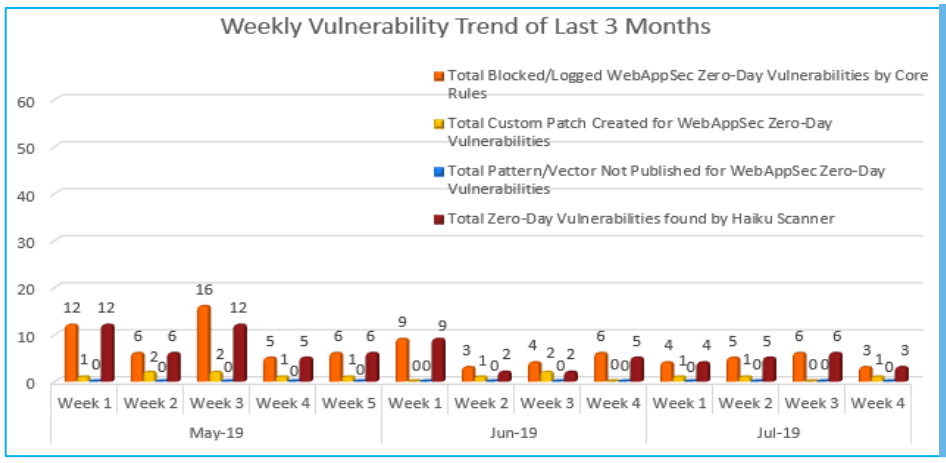
Total **4 Zero-Day Vulnerabilities** were discovered in **3 Categories** this week

1	1	2
Cross Site Scripting	Cross Site Request Forgery	Command injection

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	3

* 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:

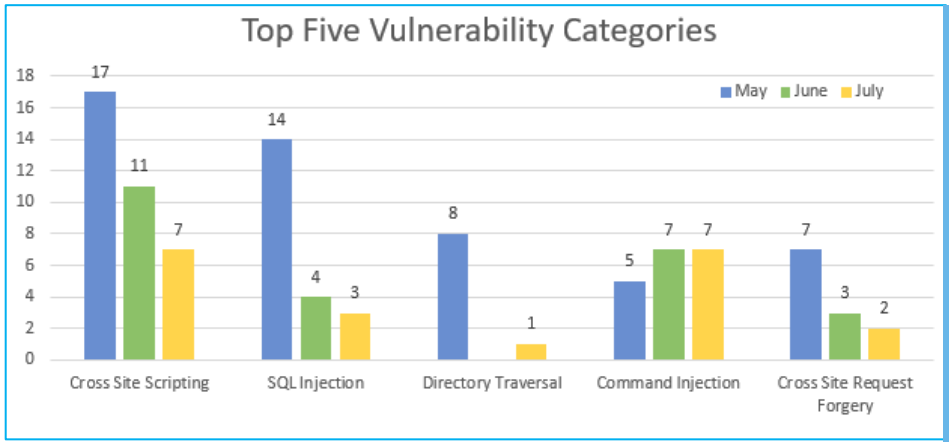


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

49% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

7% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

44% 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	NA	Recent WordPress Vulnerabilities Targeted by Malvertising Campaign	An ongoing malvertising campaign is targeting an unauthenticated stored cross-site scripting (XSS) vulnerability in the Coming Soon Page & Maintenance Mode WordPress plugin. The now patched flaw allows unauthenticated attackers to inject JavaScript or HTML code into the blog front-end of WordPress sites running the plugin's version 1.7.8 or below.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	Cross Site Request Forgery	CVE-2019-14240	WCMS 0.3.2 /wex/html.php finish cross site request forgery	A vulnerability was found in WCMS 0.3.2. It has been declared as problematic. This vulnerability affects some unknown processing of the file */wex/html.php*. The manipulation of the argument finish with the input value ../index.html 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 presented in 07/23/2019.	Protected by Command Rules.	NA
3.	Command Injection	CVE-2019-13980	Directus 7 API uploads/_/originals Code Execution	A vulnerability was found in Directus 7 and classified as critical. This issue affects some unknown functionality of the file *uploads/_/originals* of the component *API*. 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	Protected by Default Rules.	Detected by scanner as Command Injection attack.

		weakness was released in 07/19/2019. The identification of this vulnerability is CVE-2019-13980 since 07/19/2019. Technical details of the vulnerability are known, but there is no availability.		
NA	ProFTPD Remote Code Execution Bug Exposes Over 1 Million Servers	A vulnerability was found in ProFTPD 1.3.5b (File Transfer Software) and classified as critical. Affected by this issue is an unknown code of the component mod_copy. 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 weakness was published in 07/19/2019. This vulnerability is handled as CVE-2019-12815 since 06/13/2019. The attack may be launched remotely. There are neither technical details nor any exploit publicly available.	Protected by Default Rules.	Detected by scanner as Command Injection attack.