Weekly Zero-Day Vulnerability Coverage Bulletin

(8th July – 14th July)

Summary:

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

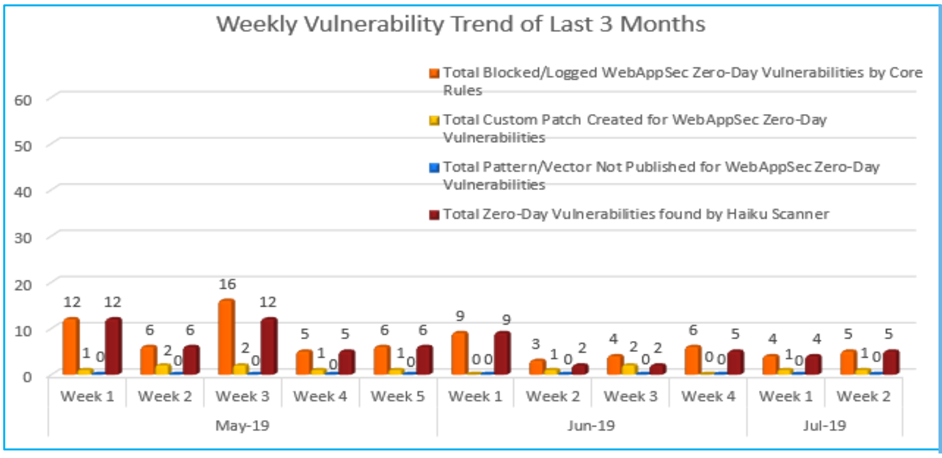
3 Cross Site Scripting	**1** SQL Injection	**1** Command Injection	**1** DOS Attack

Zero-Day Vulnerabilities Protected through Core Rules	5
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	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:

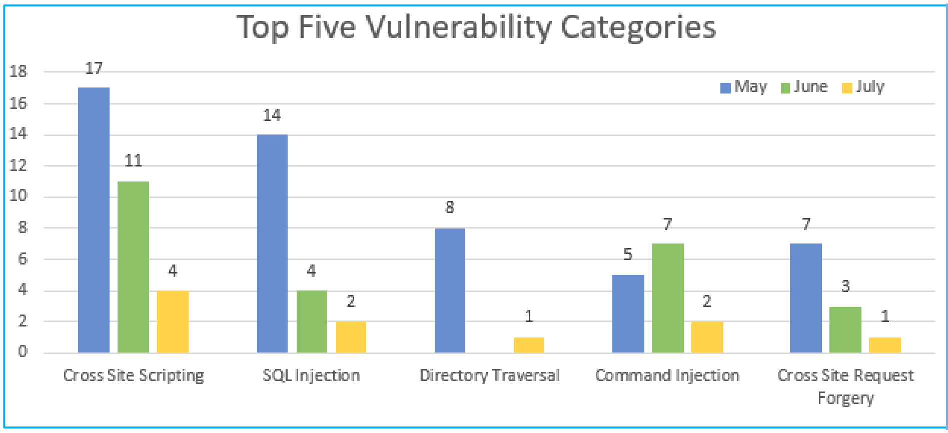


Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a quarter.

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 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-2019-1105	Microsoft Outlook remote code execution vulnerability (CVE-2019-1105)	Very few details of the flaw was available in the advisory, which just revealed that the earlier versions of the email app contained a cross-site scripting (XSS) flaw that could allow attackers to run scripts in the context of the current user just by sending a specially crafted email to the victims. This kind of vulnerability could be exploited by an attacker sending an email with JavaScript in it. The server escapes that JavaScript and does not see it because it's within an iframe. When delivered, the mail client automatically will undo the escaping, and the JavaScript runs on the client device. Bingo – Remote Code Execution.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		NA	Magento fixed security flaws that allow complete site takeover	Attacker would first exploit a Stored Cross-Site Scripting (XSS) vulnerability to inject a JavaScript payload into the administrator backend of a Magento store. In this way, he can hijack the session from a user and then exploit an authenticated Remote Code Execution (RCE) flaw to completely takeover the online store.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		NA	WordPress Plugin WP Statistics: Unauthenticated Stored XSS Under Certain Configurations	The WordPress plugin WP Statistics, which has an active installation base of 500k users, has an unauthenticated stored XSS vulnerability on versions prior to 12.6.7. This vulnerability can only be exploited under certain configurations, the default	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.

				settings are not vulnerable.		
2.	SQL Injection	NA	WP Statistics WordPress Plugin Vulnerable to Unauthenticated Blind SQL Injection	An unauthenticated blind SQL injection (SQLi) in the WP Statistics plugin versions 12.6.6.1 and lower. The vulnerability exists in a non-default configuration of the plugin. By default, the Cache Plugin setting in WP Statistics is disabled.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
3.	Command Injection	CVE-2019-10149	CVE-2019-10149: “Return of the WiZard” Vulnerability: Crooks Start Hitting	A vulnerability was found in Exim up to 4.92 (Mail Server Software) and classified as critical. Affected by this issue is some unknown processing. The manipulation with an unknown input leads to a privilege escalation vulnerability. Using CWE to declare the problem leads to CWE-269. Impacted is confidentiality, integrity, and availability. The weakness was disclosed in 06/03/2019 as CVE-2019-10149 Exim 4.87 to 4.91 as confirmed security advisory (Website). The advisory is shared for download at exim.org. The public release has been coordinated in cooperation with the vendor. This vulnerability is handled as CVE-2019-10149. The attack may be launched remotely. There are neither technical details nor an exploit publicly available.	Protected by Default Rules.	Detected by scanner as Command Injection attack.
4.	DOS Attack	CVE-2019-10072	CVE-2019-10072 Apache Tomcat HTTP/2 DoS	vulnerability has been found in Apache Tomcat up to 8.5.40/9.0.19 (Application Server Software) and classified as problematic. This vulnerability affects an unknown function of the component Incomplete Fix CVE-2019-0199. The	Protected by Custom Rules.	NA

manipulation with an unknown input leads to a denial of service vulnerability (Resource Exhaustion). The CWE definition for the vulnerability is CWE-400. As an impact it is known to affect availability. The weakness was disclosed in 06/21/2019. This vulnerability was named as CVE-2019-10072 since 03/26/2019. The attack can be initiated remotely. No form of authentication is required for a successful exploitation. The technical details are unknown, and an exploit is not available.