Weekly Zero-Day Vulnerability Coverage Bulletin

(15th July – 21st July)

Summary:

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

2
Cross Site Scripting

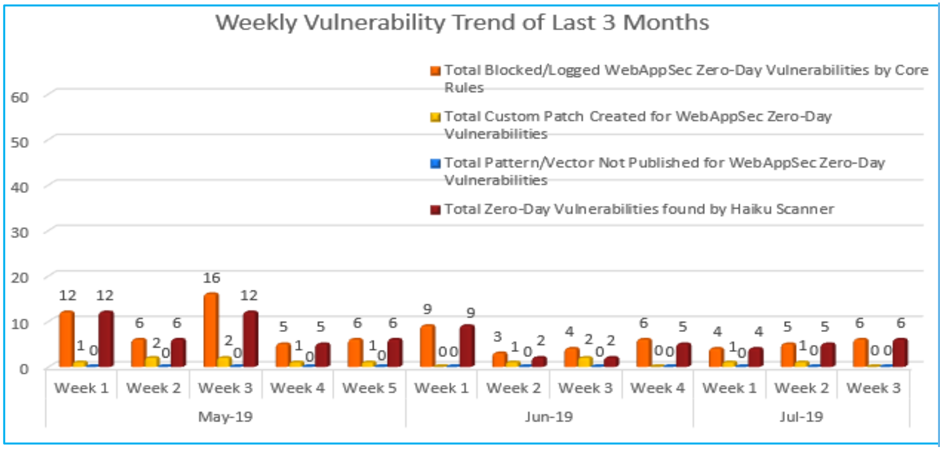
1
SQL Injection

3
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	6

* 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:

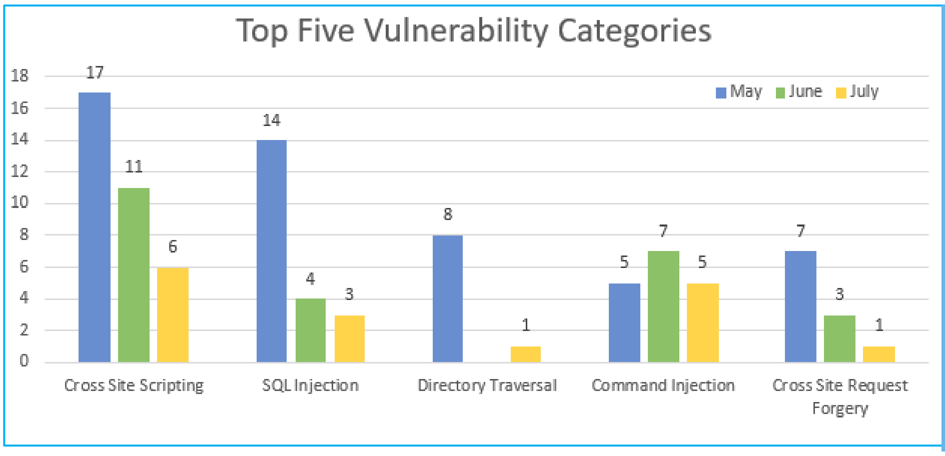


Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a quarter.

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 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	NA	Magento 2.3.1: Unauthenticated Stored XSS to RCE	A successful attack enables an unauthenticated adversary to persistently inject a JavaScript payload into the administrator backend of a Magento store. When triggered, this JavaScript payload can then perform automated exploit steps in the browser of a victim. We visualize these steps in our video in form of our JavaScript-based RIPS shell.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		NA	Icegram Persistent Cross-Site Scripting	Icegram is a plugin that helps you collect email addresses for your newsletter. Other features include light-box popup offers, header action bars, toast notifications, and slide-in messengers. Versions 1.10.28.2 and lower are affected by a persistent Cross-Site Scripting in the admin area. This plugin has over 40,000 installations and any attacker with a subscriber account can leverage this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	SQL Injection	NA	MAGENTO 2.2.0 <= 2.3.0 UNAUTHENTICATED SQLI	The Magento application running on the remote web server is affected by a SQL injection vulnerability due to failing to properly sanitize the user-supplied 'from' and 'to' inputs to the 'prepareSqlCondition' function of the 'Magento\Framework\DB\Adapter\Pdo\Mysql' class. An unauthenticated, remote attacker can exploit this to execute arbitrary SQL statements against the back-end database, leading to the execution of arbitrary code, manipulation of data,	Protected by Default Rules.	Detected by scanner as SQL Injection attack.

				or disclosure of sensitive information.		
3.	Command Injection	NA	Critical Bug in WordPress Plugin Lets Hackers Execute Code	A critical security issue found in the Ad Inserter WordPress plugin currently installed on over 200,000 websites allows authenticated attackers to remotely execute PHP code.	Protected by Default Rules.	Detected by scanner as Command Injection attack.
		CVE-2019-11580	Atlassian Crowd RCE Vulnerability (CVE-2019-11580)	A vulnerability was found in Exim up to 4.92 (Mail Server Software) and classified as critical. Affected by this issue is a part. 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. The current price for an exploit might be approx. USD $0-$5k (estimation calculated on 06/04/2019).	Protected by Default Rules.	Detected by scanner as Command Injection attack.
		CVE-2019-11581	Critical Template Injection Vulnerability in Atlassian Jira Server and Data Centre (CVE-2019-11581)	CVE-2019-11581 is a server-side template injection vulnerability in “various resources” of Jira Server and Data Centre. According to the advisory, the vulnerability was introduced in version 4.4.0, which was released in August 2011, making this vulnerability nearly eight years old.	Protected by Default Rules.	Detected by scanner as Command Injection attack.