Weekly Zero-Day Vulnerability Coverage Bulletin

(1st July – 7th July)

Summary:

Total **5 Zero-Day Vulnerabilities** were discovered in **5 Categories** this week

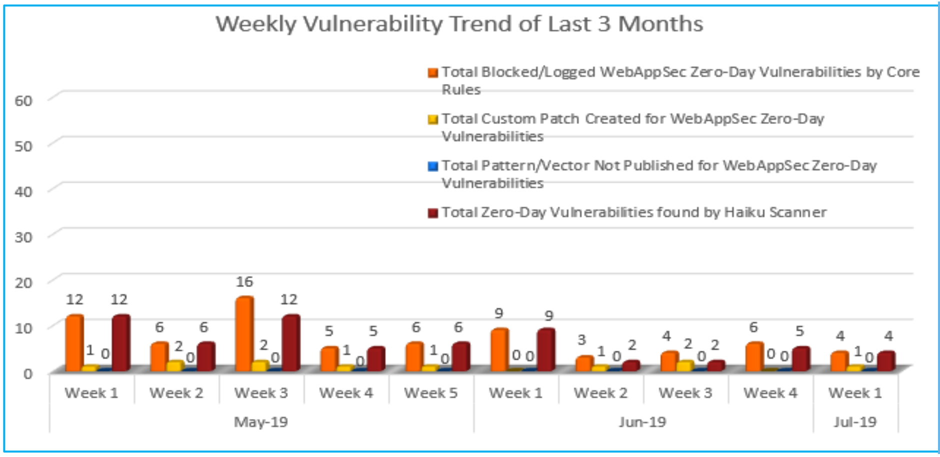
1	**1**	**1**	**1**	**1**
Cross Site Scripting	SQL Injection	Directory Traversal	Cross Site Request Forgery	Command Injection

Zero-Day Vulnerabilities Protected through Core Rules	4
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	4

* 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:

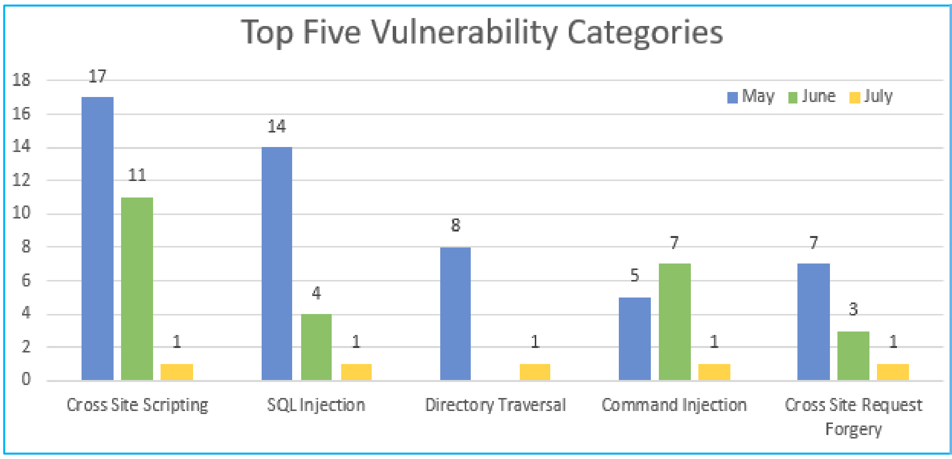


Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.

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, SQL Injection vulnerabilities were discovered in May compared to other months and categories so far.

Zero Directory Traversal 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-2019-12970	SquirrelMail up to 1.4.22/1.5.2 HTML Email cross site scripting	A vulnerability was found in SquirrelMail up to 1.4.22/1.5.2 (Mail Client Software). It has been rated as problematic. Affected by this issue is an unknown code block of the component *HTML Email Handler*. 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.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	SQL Injection	CVE-2019-11821	Synology Photo Station up to 6.8.11 synophoto_csPhotoDB.php type sql injection	A vulnerability was found in Synology Photo Station up to 6.8.11 (Network Attached Storage Software). It has been rated as critical. This issue affects some unknown processing of the file *synophoto_csPhotoDB.php*. The manipulation of the argument type 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.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
3.	Command Injection	CVE-2019-7669	Prima Systems FlexAir command injection [CVE-2019-7669]	A vulnerability was found in Prima Systems FlexAir (affected version unknown). It has been declared as critical. Affected by this vulnerability is some unknown functionality. The manipulation with an unknown input leads to a privilege escalation vulnerability (Command	Protected by Default Rules.	Detected by scanner as Command Injection attack.

				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 disclosed in 07/01/2019. This vulnerability is known as CVE-2019-7669 since 02/09/2019. The exploitation doesn't need any form of authentication.		
4.	Cross Site Request Forgery	CVE-2019-7273	Optergy Proton/Enterprise cross site request forgery [CVE-2019-7273]	A vulnerability has been found in Optergy Proton and Enterprise (affected version unknown) and classified as problematic. Affected by this vulnerability is an unknown code. The manipulation with an unknown input 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 published in 07/01/2019.	Protected by Custom Rules.	NA
5.	Directory Traversal	CVE-2019-10717	BlogEngine.NET 3.3.7.0 /api/filemanager path directory traversal	A vulnerability was found in BlogEngine.NET 3.3.7.0. It has been declared as critical. This vulnerability affects an unknown function of the file */api/filemanager*. The manipulation of the argument path as part of a *Parameter* leads to a directory traversal vulnerability. The CWE definition for the vulnerability is CWE-22. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was shared in 07/03/2019 as mailinglist post (Full-Disclosure).	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.