Weekly Zero-Day Vulnerability Coverage Bulletin

(29th July – 4th August)

Summary:

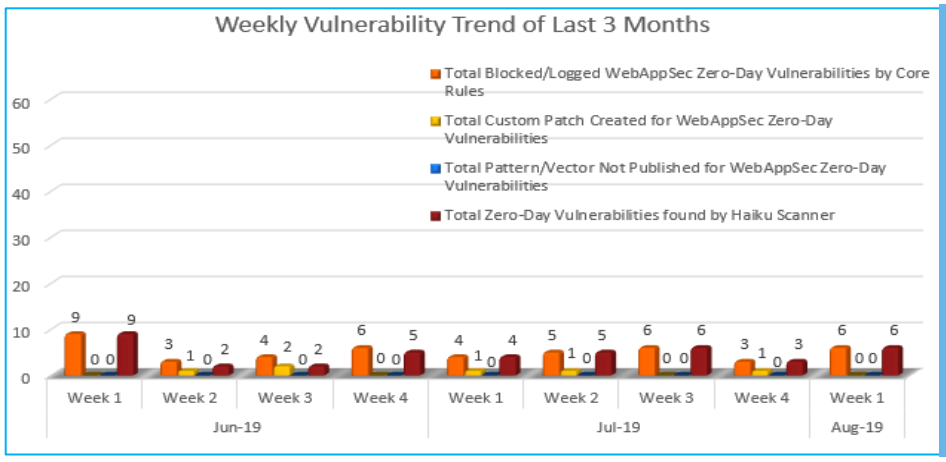
Total **6 Zero-Day Vulnerabilities** were discovered in **3 Categories** this week

4	1	1
Cross Site Scripting	Directory Traversal	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:

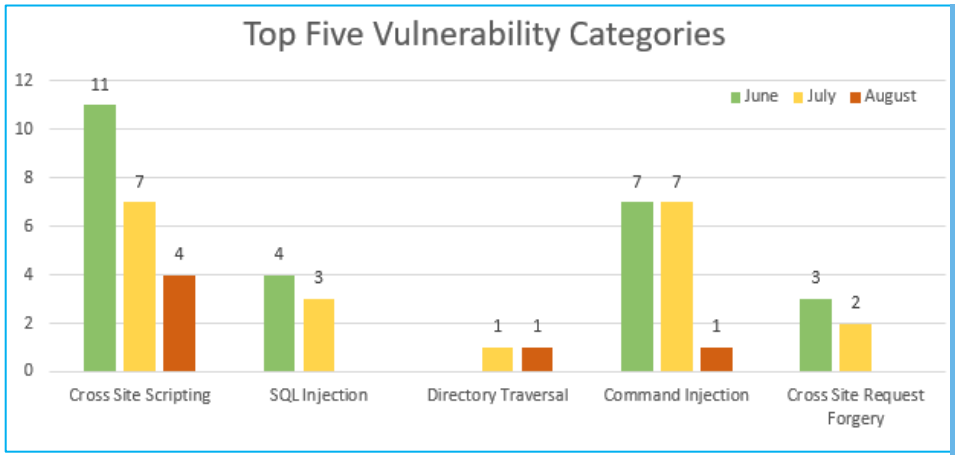


Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.

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

6% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

45% Of Zero-Day Vulnerabilities were reported by Haiku Scanner in last quarter



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

Zero Directory Traversal vulnerabilities were 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-2019-14349	EspoCRM 5.6.4 api/v1/Document cross site scripting	A vulnerability has been found in EspoCRM 5.6.4 and classified as problematic. This vulnerability affects an unknown code block of the file *api/v1/Document*. The manipulation with an unknown input leads to a cross site scripting 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 and would make it possible.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2019-14331	EspoCRM up to 5.6.5 Create User firstName/lastName Stored cross site scripting	A vulnerability, which was classified as problematic, was found in EspoCRM up to 5.6.5. This affects an unknown code of the component *Create User Handler*. The manipulation of the argument firstName/lastName with an unknown input leads to a cross site scripting vulnerability (Stored). CWE is classifying the issue as CWE-80. This is going to have an impact on 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-2019-14330	EspoCRM up to 5.6.5 Create Case firstName/lastName Stored cross site scripting	A vulnerability, which was classified as problematic, has been found in EspoCRM up to 5.6.5. Affected by this issue is an unknown part of the component *Create Case Handler*. The manipulation of the argument firstName/lastName with an unknown input leads to a cross site scripting vulnerability (Stored). Using	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.

				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.		
		CVE-2019-14329	EspoCRM up to 5.6.5 Create Task name Stored cross site scripting	A vulnerability classified as problematic was found in EspoCRM up to 5.6.5. Affected by this vulnerability is some unknown functionality of the component *Create Task Handler*. The manipulation of the argument name as part of a *Parameter* leads to a cross site scripting 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.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	Command Injection	CVE-2019-11201	Dolibarr 9.0.1 WYSIWYG Editor Code Execution	A vulnerability was found in Dolibarr 9.0.1 (Enterprise Resource Planning Software). It has been declared as critical. This vulnerability affects an unknown code of the component *WYSIWYG Editor*. 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 published in 07/29/2019. This vulnerability was named as CVE-2019-11201 since 04/11/2019.	Protected by Default Rules.	Detected by scanner as Command Injection attack.
3.	Directory Traversal	CVE-2019-14371	libav 12.3 libavformat/mov.c mov_probe directory traversal	A vulnerability was found in libav 12.3 (Multimedia Player Software) and classified as critical. Affected by this issue is the function mov_probe of the file *libavformat/mov.c*. The manipulation with an unknown input lead to a	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.

	directory traversal vulnerability (Loop). Using CWE to declare the problem leads to CWE-835. Impacted is confidentiality, integrity, and availability. The weakness was disclosed in 07/28/2019. This vulnerability is handled as CVE-2019-14371 since 07/28/2019. Technical details are known, but there is no available exploit.