Weekly Zero-Day Vulnerability Coverage Bulletin

(10th September – 16th September)

Summary:

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

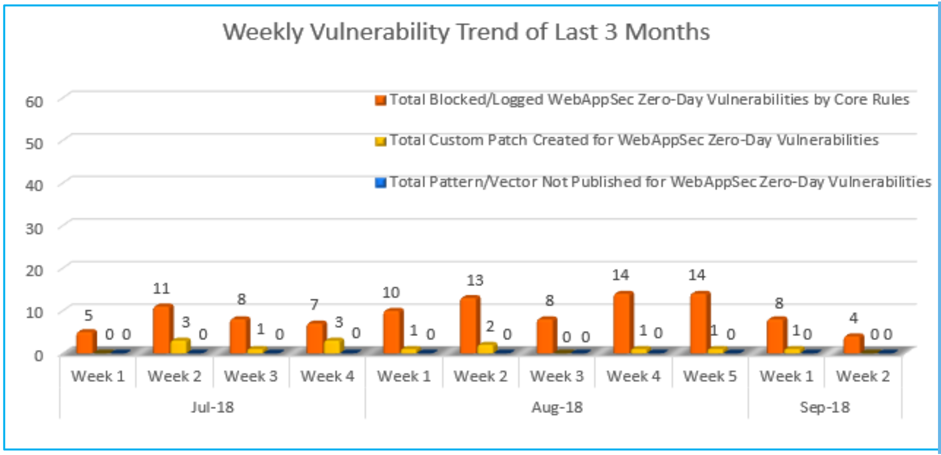
2 Cross Site Scripting	**1** Directory Traversal	**1** Cross Site Request Forgery

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**

* To enable custom rules please contact support@indusface.com

** Since attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected

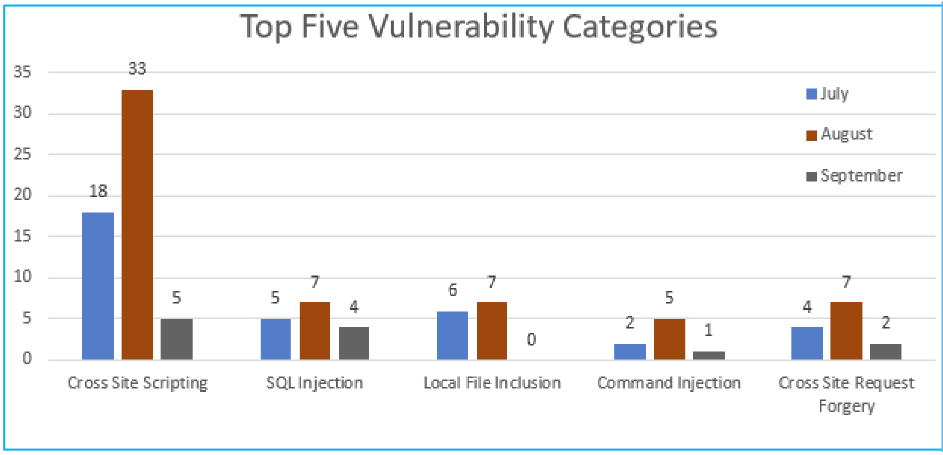
Vulnerability Trend:



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

87% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

13% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



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

Medium no. of SQL, LFI and CSRF attacks are found.

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
1.	Cross Site Scripting	CVE-2018-16454	PHP Scripts Mall Olx Clone 3.4.2 Cross Site Scripting [CVE-2018-16454]	A vulnerability was found in PHP Scripts Mall Olx Clone 3.4.2 and classified as problematic. This issue affects an unknown function. 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 web site. This would alter the appearance and would make it possible to initiate further attacks against site visitors.	Protected by Default Rules.
		CVE-2018-16772	Hoosk 1.7.0 Navigation Title cross site scripting	A vulnerability was found in Hoosk 1.7.0. It has been classified as problematic. This affects an unknown function of the component *Navigation Title Handler*. The manipulation with an unknown input leads to a Cross Site Scripting vulnerability. 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.	Protected by Default Rules.
2.	Cross Site Request Forgery	CVE-2018-16650	phpMyFAQ up to 2.9.10 cross site request forgery [CVE-2018-16650]	A vulnerability was found in phpMyFAQ up to 2.9.10. It has been declared as problematic. Affected by this vulnerability is an unknown function. 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	Protected by Custom Rules.

				application. The weakness was shared 09/07/2018.	
3.	Directory Traversal	CVE-2018-16059	Endress+Hauser WirelessHART Fieldgate SWG70 3.x fcgi-bin/wgsetcgi filename directory traversal	A vulnerability, which was classified as critical, was found in Endress+Hauser WirelessHART Fieldgate SWG70 3.x. This affects an unknown function of the file *fcgi-bin/wgsetcgi*. The manipulation of the argument filename with an unknown input leads to a directory traversal vulnerability. CWE is classifying the issue as CWE-22. This is going to have an impact on confidentiality, integrity, and availability. The weakness was published 09/07/2018 as *EDB-ID 45342* as uncorroborated exploit (Exploit-DB). It is possible to read the advisory at exploit-db.com.	Protected by Default Rules.