Weekly Zero-Day Vulnerability Coverage Bulletin

(21st October – 27th October)

Summary:

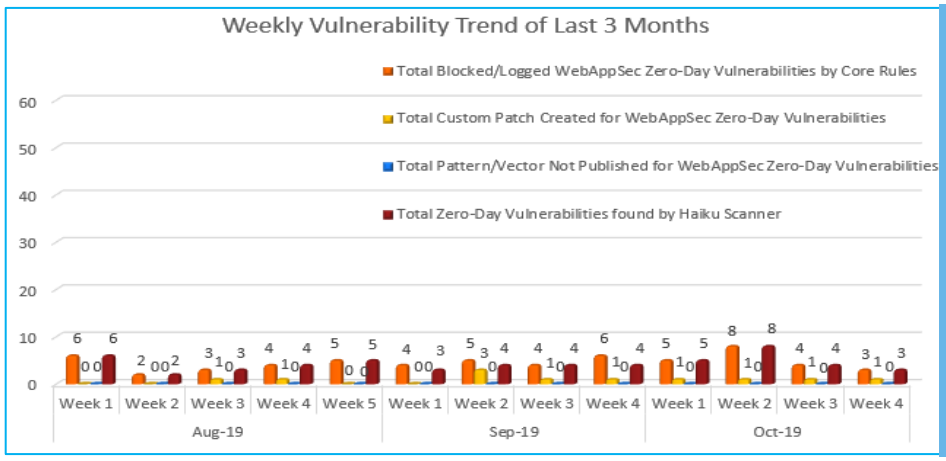
Total **4 Zero-Day Vulnerabilities** were discovered in **4 Categories** this week

1 Cross Site Scripting	**1** SQL Injection	**1** Command Injection	**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**
Zero-Day Vulnerabilities found by Haiku Scanner	3

* 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:

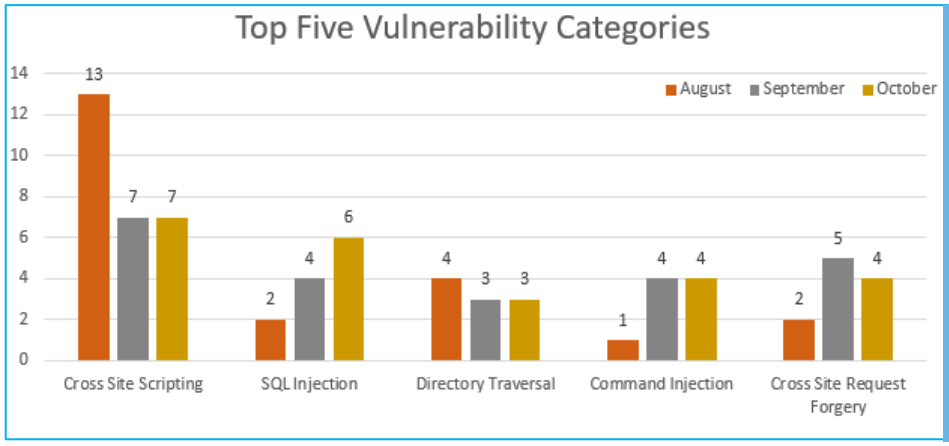


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

47% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

10% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

43% Of Zero-Day Vulnerabilities were reported by Haiku Scanner in last quarter



From the graph, we infer that maximum Cross Site Scripting vulnerabilities are discovered in August compared to other months.

Only 1 Command Injection attack is discovered in August compared to other months and categories.

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	Running a few dozens of new magic Cross Site Scripting payloads	73 new cross site scripting payloads tried out against default CRS installation	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	SQL Injection	NA	OpenEMR up to 5.0.2 eye_base.php providerID sql injection	A vulnerability classified as critical has been found in OpenEMR up to 5.0.2 (Business Process Management Software). This affects an unknown functionality of the file interface/forms/eye_mag/js/eye_base.php. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
3.	Command Injection	NA	PHP Bug Allows Remote Code-Execution on NGINX Servers (CVE-2019-11043)	A vulnerability was found in PHP up to 7.1.32 (Programming Language Software). It has been classified as critical. This affects the function env_path_info of the file fpm_main.c of the component FPM. The manipulation with an unknown input lead to a memory corruption vulnerability (Underflow). CWE is classifying the issue as CWE-124. This is going to have an impact on confidentiality, integrity, and availability. The weakness was released 10/24/2019 as Version 7.1.33 as confirmed changelog (Website). It is possible to read the advisory at php.net. This vulnerability is uniquely identified as CVE-2019-11043. It is possible to initiate the attack remotely. No form of authentication is needed for exploitation. Technical details and a public exploit are known.	Protected by Default Rules.	Detected by scanner as Host Header Injection attack.
4.	Cross Site Request Forgery	CVE-2019-18220	Sitemagic CMS 4.4.1 cross site request forgery	A vulnerability was found in Sitemagic CMS 4.4.1 (Content Management	Protected by Custom Rules.	NA

	[CVE-2019-18220]	System). It has been rated as problematic. Affected by this issue is an unknown code. Upgrading to version 4.4.2 eliminates this vulnerability.