Weekly Zero-Day Vulnerability Coverage Bulletin

(29th October – 4th November)

Summary:

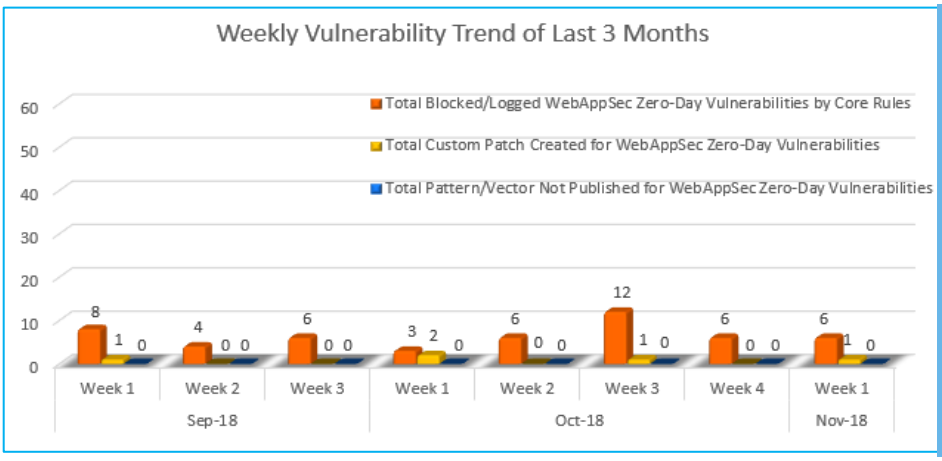
Total **7 Zero-Day Vulnerabilities** were discovered in **4 Categories** previous week

3	2	1	1
Cross Site Scripting	SQL Injection	Directory Traversal	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	6
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

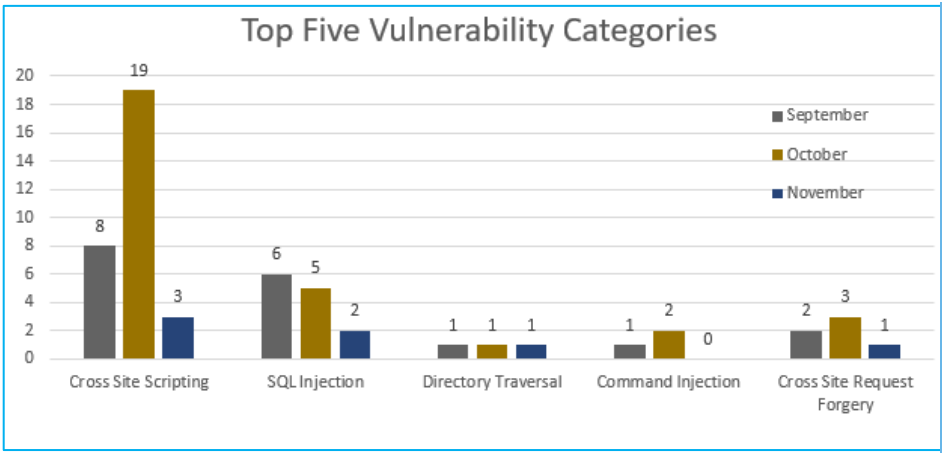
Vulnerability Trend:



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

90% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

10% 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 October compared to other months and categories so far.

Medium no. of SQL Injection is found in all 3 months.

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-2018-1766	IBM Team Concert up to 6.0.5 Web UI cross site scripting	A vulnerability classified as problematic has been found in IBM Team Concert up to 6.0.5. This affects an unknown function of the component *Web UI*. 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. This would alter the appearance.	Protected by Default Rules.
		CVE-2018-15707	Advantech WebAccess 8.3.1/8.3.2 Bwmainleft.asp cross site scripting	A vulnerability was found in Apple iOS up to 12.0.1. It has been rated as critical. Affected by this issue is an unknown function of the component WebKit. Upgrading to version 12.1 eliminates this vulnerability. A possible mitigation has been published immediately after the disclosure of the vulnerability.	Protected by Default Rules.
		CVE-2018-18927	PublicCMS 4.0 attached cross site scripting	A vulnerability was found in Apple iOS up to 12.0.1. It has been rated as critical. An unknown function of the component WebKit is affected by this issue. Upgrading to version 12.1 eliminates this vulnerability. A possible mitigation has been published immediately after the disclosure of the vulnerability.	Protected by Default Rules.
2.	SQL Injection	CVE-2018-18792	zzcms 8.3 Cookie zs/zs_list.php sql injection	A vulnerability, which was classified as critical, has been found in zzcms 8.3. This issue affects an unknown function of the file *zs/zs_list.php* of the component *Cookie Handler*. The manipulation with an unknown input lead to a sql injection vulnerability.	Protected by Default Rules.

				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. The weakness was presented 10/28/2018. The identification of	
		CVE-2018-18887	X-CMS PHP 1.0 member/member_news.php type sql injection	A vulnerability was found in Apple iOS up to 12.0.1. It has been rated as critical. Affected by this issue is an unknown function of the component WebKit. Upgrading to version 12.1 eliminates this vulnerability. A possible mitigation has been published immediately after the disclosure of the vulnerability.	Protected by Default Rules.
3.	Cross Site Request Forgery	CVE-2018-18711	wuzhi cms 4.1.0 index.php Cross Site Request Forgery	A vulnerability has been found in WUZHI CMS 4.1.0 and classified as problematic. Affected by this vulnerability is an unknown function of the file index.php?m=core&f=panel&v=edit_info. The manipulation with an unknown input leads to a cross site request forgery vulnerability.	Protected by Custom Rules.
4.	Directory Traversal	CVE-2018-18778	Acme mini_httpd up to 1.29 directory traversal	A vulnerability was found in Acme mini_httpd up to 1.29. It has been rated as critical. This issue affects an unknown function. Upgrading to version 1.30 eliminates this vulnerability.	Protected by Default Rules.