Weekly Zero-Day Vulnerability Coverage Bulletin

(5th November – 11th November)

Summary:

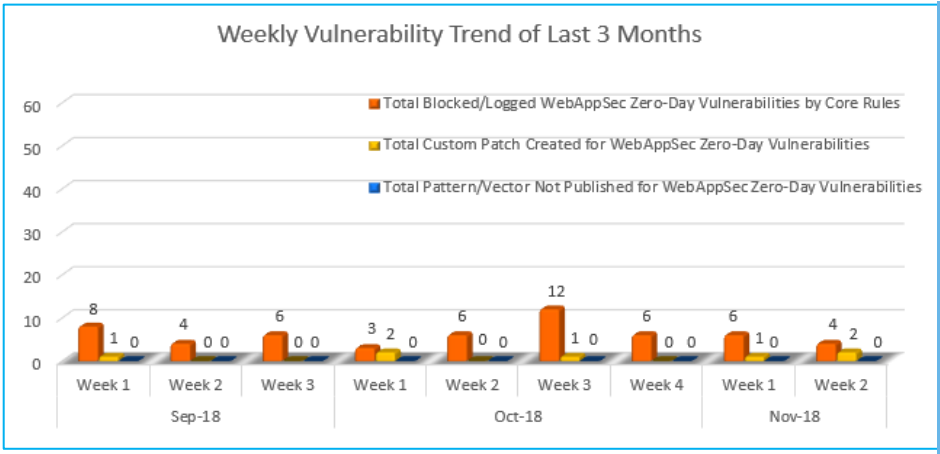
Total **6 Zero-Day Vulnerabilities** were discovered in **4 Categories** previous week

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

Zero-Day Vulnerabilities Protected through Core Rules	4
Zero-Day Vulnerabilities Protected through Custom Rules	2*
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

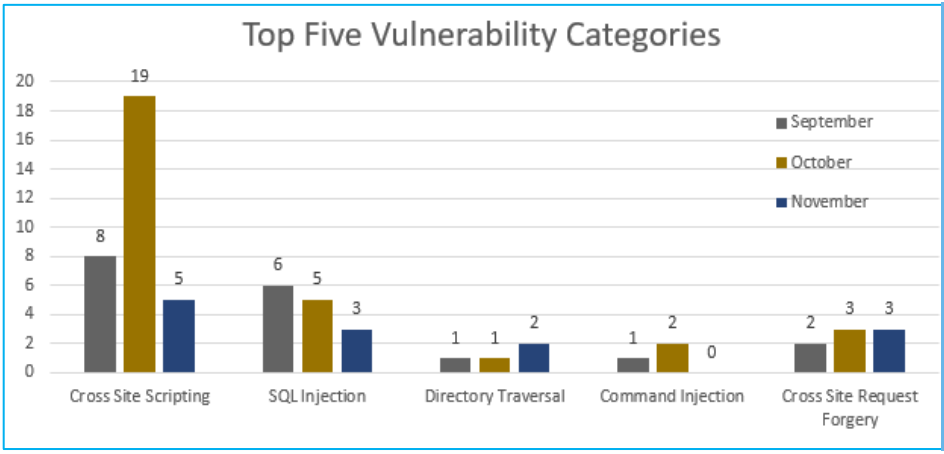
Vulnerability Trend:



Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a quarter.

88% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

12% 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 was found in all the 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-2018-18943	BaserCMS up to 4.1.3 edit data[UploaderCategory][name] cross site scripting	A vulnerability was found in BaserCMS up to 4.1.3 and classified as problematic. This issue affects an unknown function of the file *admin/uploader/uploader_categories/edit*. The manipulation of the argument data[UploaderCategory][name] as part of a *Parameter* 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.	Protected by Default Rules.
		CVE-2018-19090	tianti 2.3 Article Management Module Stored cross site scripting	A vulnerability, which was classified as problematic, has been found in tianti 2.3. An unknown function of the component *Article Management Module* is affected by this issue. The manipulation with an unknown input leads to a cross site scripting vulnerability (Stored). 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.	Protected by Default Rules.
2.	SQL Injection	CVE-2018-15447	Cisco Integrated Management Controller Web Framework SQL Injection	A vulnerability was found in Cisco Integrated Management Controller (the affected version is unknown). It has been rated as critical. Affected by this issue is an unknown function of the component *Web Framework*. The manipulation with an unknown input lead to a sql injection vulnerability. Using CWE to declare the problem leads to CWE-89. Impacted is confidentiality, integrity, and availability. An	Protected by Default Rules.

				attacker might be able inject and/or alter existing SQL statements which would influence the database exchange.	
3.	Directory Traversal	CVE-2018-18950	KindEditor up to 4.1.11 php/upload_json .php path directory traversal	A vulnerability was found in KindEditor up to 4.1.11. It has been declared as problematic. Affected by this vulnerability is an unknown function of the file *php/upload_json.php*. The manipulation of the argument path with an unknown input leads to a directory traversal vulnerability. The CWE definition for the vulnerability is CWE-22. As an impact it is known to affect confidentiality. The summary by CVE is:KindEditor through 4.1.11 has a path traversal vulnerability in php/upload_json.php.	Protected by Default Rules
4.	Cross Site Request Forgery	CVE-2018-18935	PopojiCMS 2.0.1 route.php cross site request forgery	A vulnerability was found in PopojiCMS 2.0.1. It has been rated as problematic. This issue affects an unknown function of the file *po-admin/route.php?mod=component&act=addnew*. The manipulation with an unknown input leads to a cross site request forgery vulnerability. Using CWE to declare the problem leads to CWE-352. Impacted is integrity. An attacker might be able force legitimate users to initiate unwanted actions within the web application. The weakness was shared 11/05/2018. The identification of this vulnerability is CVE-2018-18935 since 11/05/2018.	Protected by Custom Rules.
		CVE-2018-12413	TIBCO 1.0.0 tibschemad cross site request forgery	A vulnerability was found in TIBCO Messaging - Apache Kafka Distribution - Schema Repository 1.0.0.	Protected by Custom Rules.

		It has been rated as problematic. An unknown function of the component *tibschemad* is affected by this issue. The manipulation with an unknown input leads to a cross site request forgery vulnerability. Using CWE to declare the problem leads to CWE-352. Impacted is integrity. An attacker might be able force legitimate users to initiate unwanted actions within the web application. The weakness was released in 11/06/2018.