Weekly Zero-Day Vulnerability Coverage Bulletin

(4th November – 10th November)

Summary:

Total **6 Zero-Day Vulnerabilities** were discovered in **5 Categories** this week

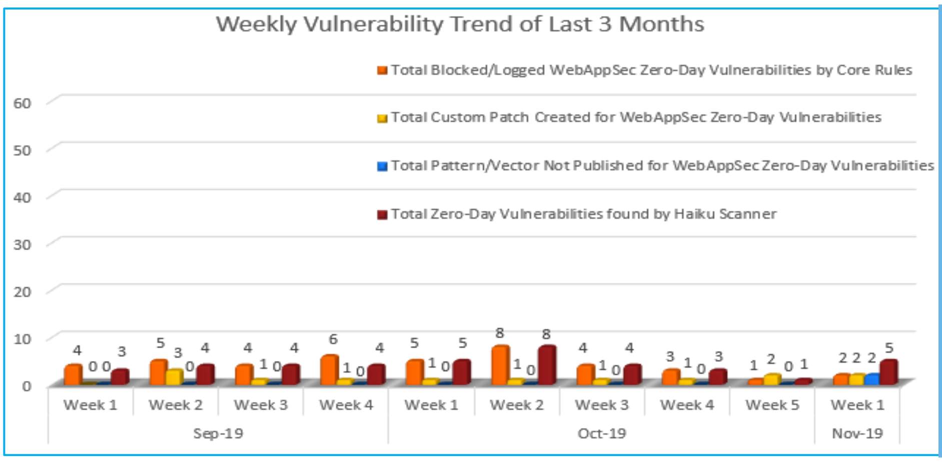
1	1	2	1	1
Cross Site Scripting	Unvalidated Redirects and Forwards	XML External Entities	Cross Site Request Forgery	Directory Traversal

Zero-Day Vulnerabilities Protected through Core Rules	2
Zero-Day Vulnerabilities Protected through Custom Rules	2*
Zero-Day Vulnerabilities for which protection cannot be determined	2**
Zero-Day Vulnerabilities found by Haiku Scanner	5

* 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:

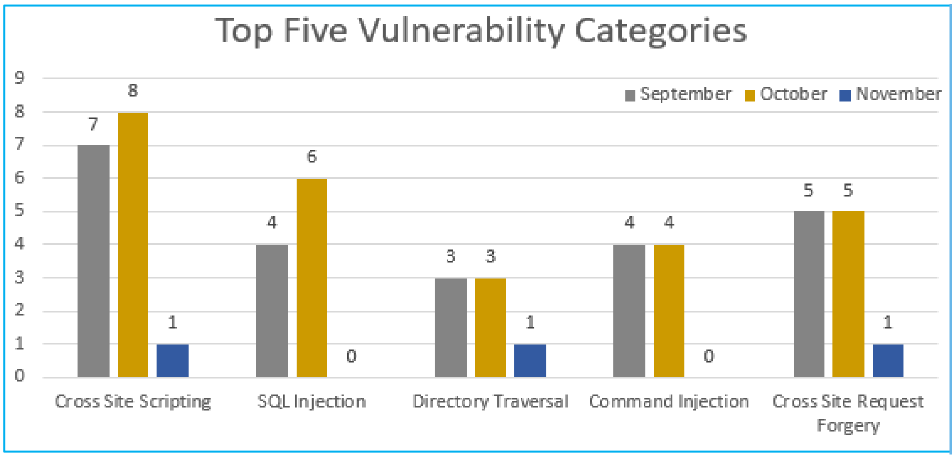


Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.

43% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

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

42% 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 October compared to other months.

Zero SQL Injection & Command Injection is found so far.

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	JBoss AeroGear password Reflected cross site scripting	A vulnerability was found in <a href="https://vuldb.com/?product.jboss:aerogear">JBoss AeroGear</a> (Application Server Software) (<a href="https://vuldb.com/?doc.version">affected version not known</a>). It has been rated as problematic. Affected by this issue is some unknown functionality. 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 Cross Site Scripting attack.
2.	XML External Entities	CVE-2019-12331	PHPOffice PhpSpreadsheet up to 1.7.x XML Data std_table.php XML External Entity	A vulnerability, which was classified as critical, has been found in <a href="https://vuldb.com/?product.phpoffice:phpspreadsheet">PHPOffice PhpSpreadsheet up to 1.7.x</a>. Affected by this issue is an unknown function of the file <em>nagvis-master/share/userfiles/gadgets/std_table.php</em> of the component <em>XML Data Handler</em>. Upgrading to version 1.8.0 eliminates this vulnerability.	Protected by Custom Rules.	Detected by scanner as XML External Entities attack.
		CVE-2019-12415	CVE-2019-12415: XML processing vulnerability in Apache POI	A vulnerability, which was classified as critical, was found in Apache POI 4.1.0. This affects an unknown code block of the component XSSFExportToXml. The manipulation as part of a document leads to a privilege escalation	NA	Detected by scanner as XML External Entities attack.

				vulnerability (XXE). CWE is classifying the issue as CWE-611. This is going to have an impact on confidentiality, integrity, and availability. The weakness was presented in 10/23/2019. This vulnerability is uniquely identified as CVE-2019-12415 since 05/28/2019. It is possible to initiate the attack remotely. No form of authentication is needed for exploitation. Neither technical details nor exploit are publicly available.		
3.	Cross Site Request Forgery	CVE-2019-18411	Zoho ManageEngine ADSelfService Plus up to 5.x User Profile Page cross site request forgery	A vulnerability, which was classified as problematic, has been found in <a href="https://vuldb.com/?product.zoho_manageengine:adselfservice_plus">Zoho ManageEngine ADSelfService Plus up to 5.x</a>. This issue affects an unknown function of the component <em>User Profile Page</em>. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Custom Rules.	NA
4.	Directory Traversal	NA	Samba up to 4.9.14/4.10.9/4.11.1 Client directory traversal	A vulnerability was found in <a href="https://vuldb.com/?product.samba">Samba up to 4.9.14/4.10.9/4.11.1</a> (File Transfer Software). It has been classified as critical. This affects some unknown functionality of the component <em>Client</em>. Upgrading to version 4.9.15, 4.10.10 or 4.11.2	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.

				eliminates this vulnerability.		
5.	Unvalidated Redirects and Forwards	NA	Drupal 6.16 Open Redirect [CVE-2010-2471]	A vulnerability was found in <a href="https://vuldb.com/?product.drupal">Drupal 6.16</a> (Content Management System). It has been declared as problematic. Affected by this vulnerability is an unknown code block. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	NA	Detected by scanner as Unvalidated Redirects and Forwards attack.