Weekly Zero-Day Vulnerability Coverage Bulletin

(11th November – 17th November)

Summary:

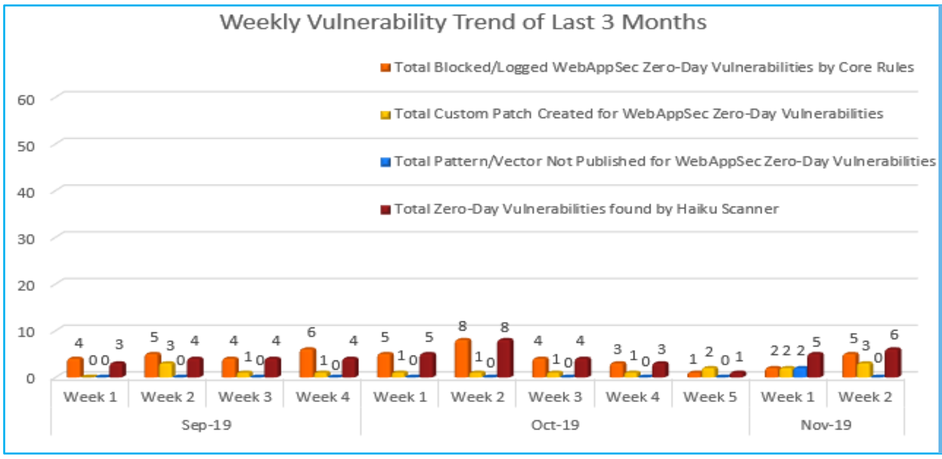
Total **8 Zero-Day Vulnerabilities** were discovered in **5 Categories** this week

1	2	1	2	2
Cross Site Scripting	SQL Injection	XML External Entities	Directory Traversal	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	5
Zero-Day Vulnerabilities Protected through Custom Rules	3*
Zero-Day Vulnerabilities for which protection cannot be determined	0**
Zero-Day Vulnerabilities found by Haiku Scanner	6

* 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:

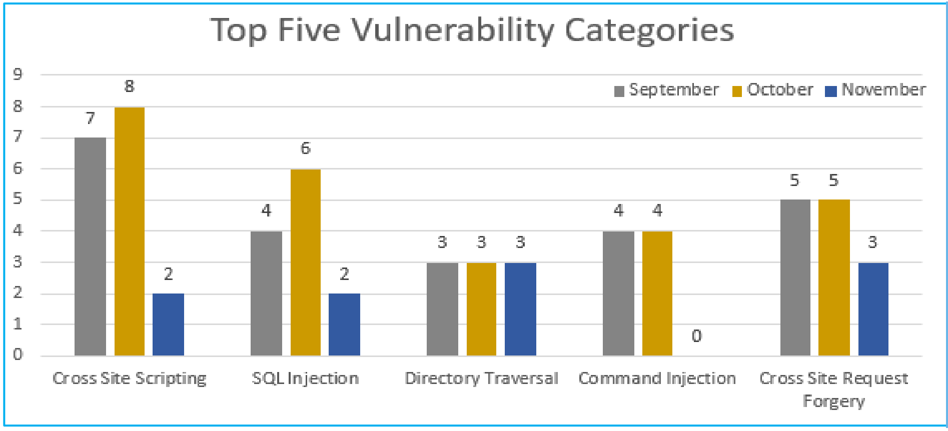


Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a quarter.

42% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

14% 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 so far.

Zero Command Injection is found in November 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	CVE-2019-18873	FUDForum 3.0.9 admsession.php User-Agent cross site scripting	A vulnerability classified as problematic has been found in <a href="https://vuldb.com/?product.subrion_cms">Subrion CMS 4.2.1</a> (Content Management System). This affects an unknown functionality of the file <em>panel/members/</em>. 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.	SQL Injection	CVE-2011-2936	Elgg up to 1.7.10 sql injection [CVE-2011-2936]	A vulnerability was found in <a href="https://vuldb.com/?product.elgg">Elgg up to 1.7.10</a>. It has been classified as critical. This affects 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.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
		CVE-2019-12720	AUO SunVeillance Monitoring System up to 1.1.9 mvc_send_mail.aspx plant_no sql injection	A vulnerability classified as critical was found in <a href="https://vuldb.com/?product.auo:sunveillance_monitoring_system">AUO SunVeillance Monitoring System up to 1.1.9</a>. This vulnerability affects an unknown part of the file <em>mvc_send_mail.aspx</em>. Upgrading to version 1.1.9e eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
3.	XML External Entity	NA	XML External Entity (XXE) Injection Payload List	An XML External Entity (XXE) attack (sometimes called an XXE injection attack) is a type of attack that abuses a widely available but rarely used feature of XML parsers.	Protected by Custom Rules.	Detected by scanner as XML External Entity attack.

				Using XXE, an attacker can cause Denial of Service (DoS) as well as access local and remote content and services. XXE can be used to perform Server Side Request Forgery (SSRF) inducing the web application to make requests to other applications. In some cases, XXE may even enable port scanning and lead to remote code execution. There are two types of XXE attacks: in-band and out-of-band (OOB-XXE).		
4.	Cross Site Request Forgery	CVE-2019-18884	Rise Ultimate Project Manager 2.3 add_team_member cross site request forgery	A vulnerability classified as problematic has been found in <a href="https://vuldb.com/?product.rise:ultimate_project_manager">Rise Ultimate Project Manager 2.3</a> (Project Management Software). This affects an unknown functionality of the file <em>index.php/team_members/add_team_member</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
		CVE-2014-3655	JBoss KeyCloak Soft Token cross site request forgery [CVE-2014-3655]	A vulnerability was found in <a href="https://vuldb.com/?product.jboss_keycloak">JBoss KeyCloak</a> (Application Server Software) (<a href="https://vuldb.com/?doc.version">the affected version is unknown</a>). It has been declared as problematic. This vulnerability affects an unknown function of the component <em>Soft Token Handler</em>. There is no information about possible countermeasures known. It may be suggested to	Protected by Custom Rules.	NA

				replace the affected object with an alternative product.		
5.	Directory Traversal	CVE-2019-18924	Systematic IRIS WebForms 5.4 directory traversal [CVE-2019-18924]	A vulnerability classified as critical has been found in <a href="https://vuldb.com/?product.systematic:iris_webforms">Systematic IRIS WebForms 5.4</a>. This affects some unknown processing. 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 Directory Traversal attack.
		CVE-2019-18951	SibSoft Xfilesharing up to 2.5.1 tmpl directory traversal	A vulnerability was found in <a href="https://vuldb.com/?product.sibsoft:xfilesharing">SibSoft Xfilesharing up to 2.5.1</a> and classified as problematic. Affected by this issue is some unknown processing. 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 Directory Traversal attack.