Weekly Zero-Day Vulnerability Coverage Bulletin

(25th November – 1st December)

Summary:

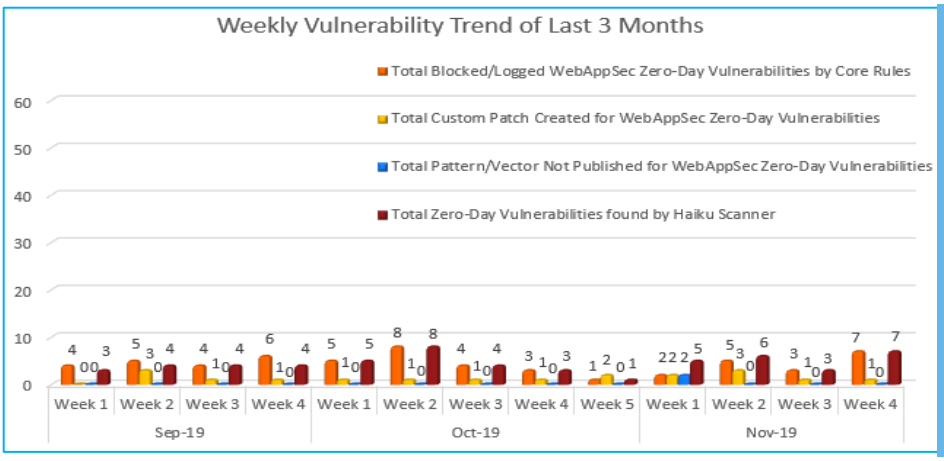
Total **8** Zero-Day Vulnerabilities were discovered in **6** categories this week

1	2	2	1	1	1
Cross Site Scripting	SQL Injection	Directory Traversal	Host Header Injection	Command Injection	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	7
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	7

* 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:

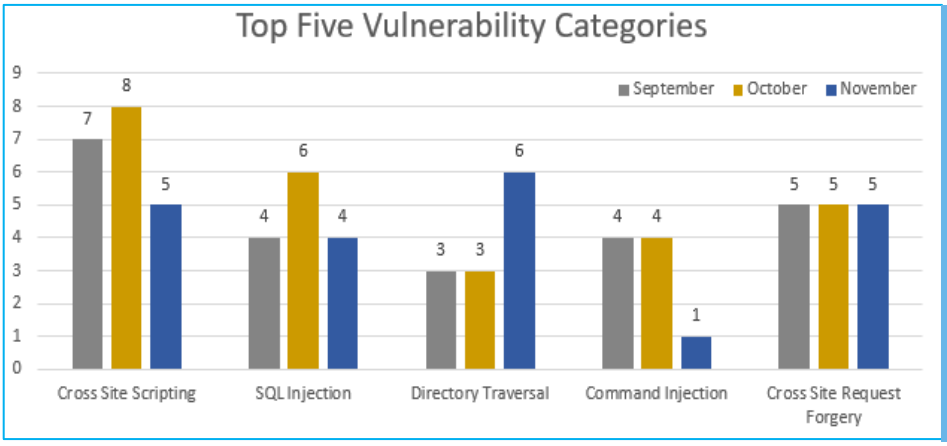


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

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

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 October compared to other months.

Only 1 Command Injection attack is discovered in November 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	CVE-2019-10771	iobroker.web up to 2.4.9 on npm GET Reflected cross site scripting	A vulnerability was found in iobroker.web up to 2.4.9 on npm and classified as problematic. This issue affects some unknown processing of the component GET Handler. Upgrading to version 2.4.10 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	SQL Injection	CVE-2019-19250	OpenTrade server/modules/api/v1.js sql injection	A vulnerability, which was classified as critical, has been found in OpenTrade (affected version not known). Affected by this issue is an unknown code block of the file server/modules/api/v1.js. Upgrading eliminates this vulnerability. A possible mitigation has been published even before and not after the disclosure of the vulnerability.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
		CVE-2011-3583	TYPO3 up to 4.5.5 Parameter sql injection	A vulnerability was found in TYPO3 up to 4.5.5 (Content Management System). It has been classified as critical. Affected is an unknown part. There is no information about possible countermeasures	Protected by Default Rules.	Detected by scanner as SQL Injection attack.

				known. It may be suggested to replace the affected object with an alternative product.		
3.	Command Injection	CVE-2019-8144	Magento Urges Users to Apply Security Update for RCE Bug CVE-2019-8144	A vulnerability was found in Magento up to 2.3.2. It has been declared as critical. This vulnerability affects some unknown functionality of the component PageBuilder Template Handler. The manipulation with an unknown input leads to a privilege escalation vulnerability (Code Execution). The CWE definition for the vulnerability is CWE-269. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was disclosed in 11/06/2019. This vulnerability was named as CVE-2019-8144 since 02/12/2019. The attack can be initiated remotely. No form of authentication is required for a successful exploitation.	Protected by Default Rules.	Detected by scanner as Command Injection attack.
4.	Cross Site Request Forgery	CVE-2011-3609	Red Hat JBoss Application Server up to 7.0.x cross site request forgery	A vulnerability, which was classified as problematic, has been found in Red Hat JBoss Application Server up to 7.0.x (Application Server Software). This issue affects an unknown functionality. Upgrading to version 7.1.0 eliminates this vulnerability.	Protected by Custom Rules.	NA
5.	Directory Traversal	CVE-2011-4350	Yaws 1.91 URL directory traversal	A vulnerability has been found in Yaws 1.91 and classified	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.

				as critical. This vulnerability affects an unknown code block of the component URL Handler. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.		
		CVE-2019-18253	Relion 670 directory traversal [CVE-2019-18253]	A vulnerability was found in Relion 670 up to 1p1r26/1.2.3.17/2.0.0.10/RES670 2.0.0.4/2.1.0.1. It has been classified as critical. Affected is an unknown code. 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.
6.	Host Header Injection	CVE-2019-17392	Progress Sitefinity 12.1 Password Recovery HTTP Host Header unknown vulnerability	A vulnerability was found in Progress Sitefinity 12.1. It has been classified as critical. This affects an unknown code of the component Password Recovery. 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 Host Header Injection attack.