Weekly Zero-Day Vulnerability Coverage Bulletin

(2nd December – 8th December)

Summary:

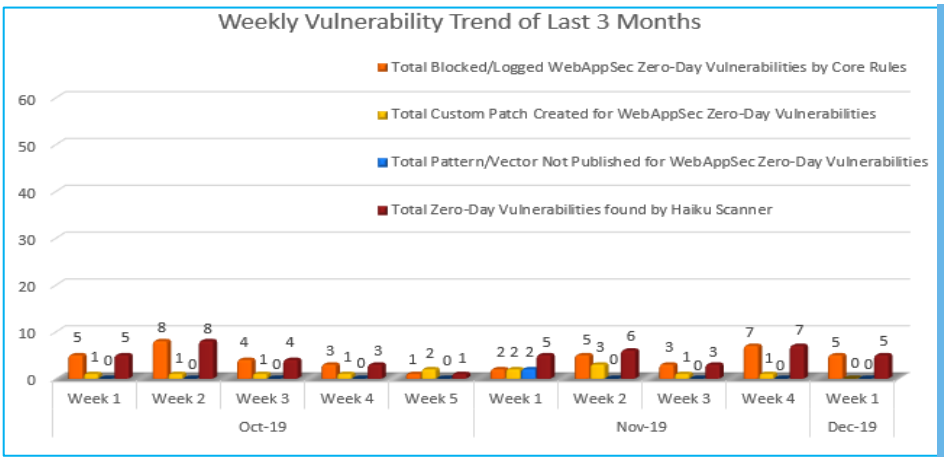
Total **5 Zero-Day Vulnerabilities** were discovered in **3 Categories** this week

3	1	1
SQL Injection	Command Injection	Directory Traversal

Zero-Day Vulnerabilities Protected through Core Rules	5
Zero-Day Vulnerabilities Protected through Custom Rules	0*
Zero-Day Vulnerabilities for which protection cannot be determined	0**
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:

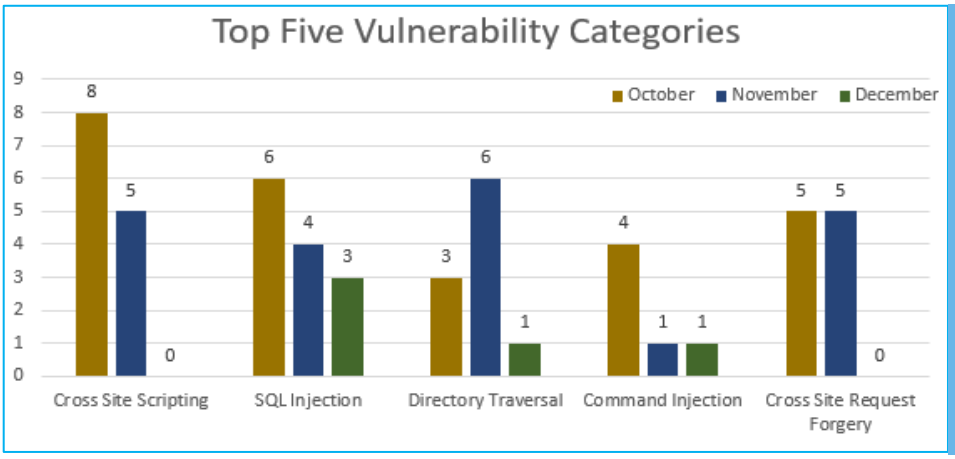


Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.

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

12% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

46% 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 and zero in December.

Zero Cross Site Request Forgery is found in December 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.	SQL Injection	CVE-2019-5112	Forma LMS 2.2.1 /appLms/ajax.server.php filter_status sql injection	A vulnerability classified as critical was found in Forma LMS 2.2.1. Affected by this vulnerability is an unknown code of the file /appLms/ajax.server.php. 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-2019-5111	Forma LMS 2.2.1 /appLms/ajax.server.php filter_cat sql injection	A vulnerability classified as critical has been found in Forma LMS 2.2.1. Affected is an unknown part of the file /appLms/ajax.server.php. 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-2019-5110	Forma LMS 2.2.1 sql injection [CVE-2019-5110]	A vulnerability was found in Forma LMS 2.2.1. It has been rated as critical. This issue affects 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 SQL Injection attack.
2.	Directory Traversal	CVE-2015-2060	cabextract up to 1.5 File Extraction	A vulnerability was found in cabe	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.

			directory traversal	xtract up to 1.5. It has been declared as critical. Affected by this vulnerability is some unknown processing of the component File Extraction Handler. Upgrading to version 1.6 eliminates this vulnerability. A possible mitigation has been published even before and not after the disclosure of the vulnerability.		
3.	Command Injection	CVE-2017-11882	Microsoft Office Equation Editor Code Execution	A vulnerability, which was classified as critical, has been found in Microsoft Office 2007 SP3/2010 SP2/2013 SP1/2016 (Office Suite Software). Affected by this issue is some unknown processing. The manipulation with an unknown input leads to a memory corruption vulnerability. Using CWE to declare the problem leads to CWE-119. Impacted is confidentiality, integrity, and availability. The bug was discovered in 11/14/2017. The weakness was presented in 11/14/2017 with Embedi as KB4011276 as confirmed security update guide (Website). The advisory is shared for download at portal.msrc.microsoft.com . This vulnerability is handled as CVE-2017-11882 since 07/31/2017. The attack may be launched remotely. No form of authentication is required for exploitation. Technical details are unknown, but a public exploit is available.	Protected by Default Rules.	Detected by scanner as Command Injection attack.