Weekly Zero-Day Vulnerability Coverage Bulletin

(23rd December – 29th December)

Summary:

Total **7** Zero-Day Vulnerabilities were discovered in **5** categories this week

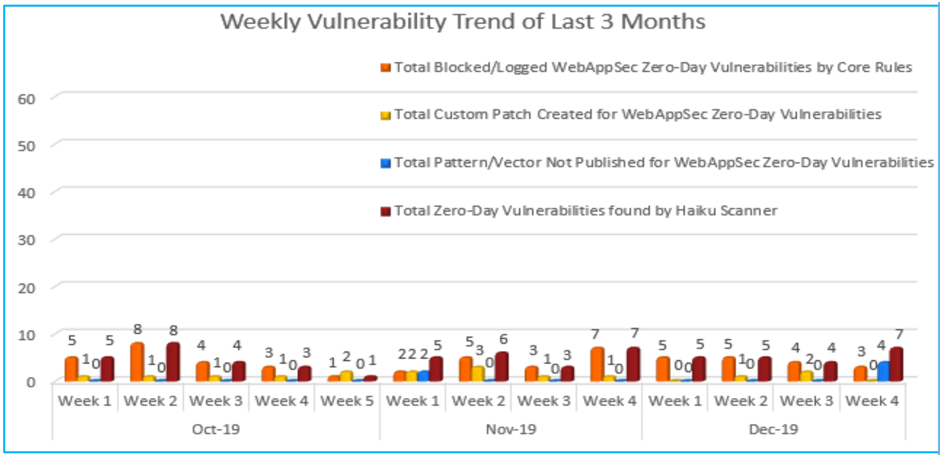
1	**1**	**1**	**3**	**1**
Cross Site Scripting	SQL Injection	Deserialization	Redirection	Command Injection

Zero-Day Vulnerabilities Protected through Core Rules	3
Zero-Day Vulnerabilities Protected through Custom Rules	0*
Zero-Day Vulnerabilities for which protection cannot be determined	4**
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:

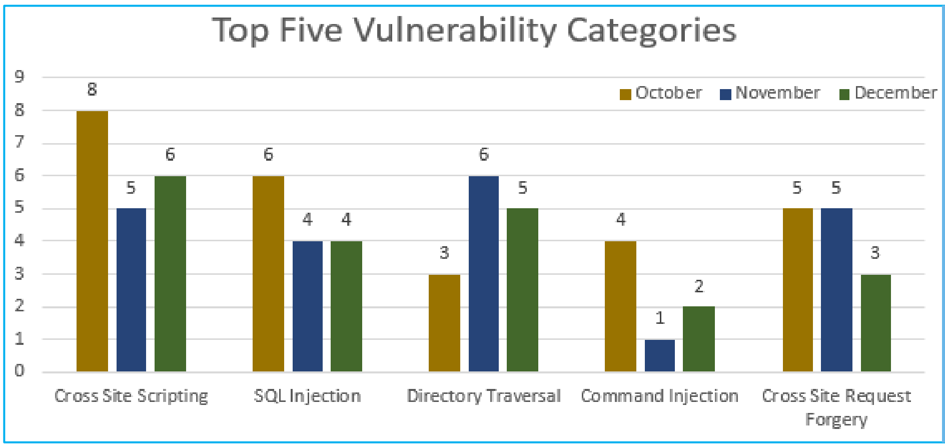


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

40% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

11% 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 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-2019-6011	wpDataTables Lite up to 2.0.11 cross site scripting [CVE-2019-6011]	A vulnerability classified as problematic has been found in <a href="https://vuldb.com/?product.wpdatatables_lite">wpDataTables Lite up to 2.0.11</a>. This affects an unknown function. 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-2019-18234	Equinox Control Expert sql injection [CVE-2019-18234]	A vulnerability, which was classified as critical, has been found in <a href="https://vuldb.com/?product.equinox:control_expert">Equinox Control Expert</a> (<a href="https://vuldb.com/?doc.version">unknown version</a>). 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.
3.	Redirection	CVE-2019-6035	Athenz up to 1.8.24 Open Redirect [CVE-2019-6035]	A vulnerability has been found in <a href="https://vuldb.com/?product.athenz">Athenz up to 1.8.24</a> and classified as critical. Affected by this vulnerability is an	NA	Detected by scanner as Redirection attack.

				unknown functionality. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.		
		CVE-2019-6025	Movable Type Open Redirect [CVE-2019-6025]	A vulnerability has been found in <a href="https://vuldb.com/?product.movable_type">Movable Type</a> (<a href="https://vuldb.com/?doc.version">the affected version is unknown</a>) and classified as critical. This vulnerability 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.	NA	Detected by scanner as Redirection attack.
		CVE-2019-6020	PowerCMS up to 3.293/4.42/5.12 Open Redirect [CVE-2019-6020]	A vulnerability was found in <a href="https://vuldb.com/?product.powercms">PowerCMS up to 3.293/4.42/5.12</a>. It has been rated as critical. This issue affects an unknown functionality. 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 Redirection attack.
4.	Deserialization	CVE-2019-2725	Deserialization vulnerability in Oracle WebLogic Server	A vulnerability classified as very critical has been found in Oracle Fusion Middleware	NA	Detected by scanner as Deserialization attack.

				10.3.6.0.0/12.1.3.0.0 (Middleware). This affects an unknown code of the component WebLogic Server. The manipulation with an unknown input leads to a privilege escalation vulnerability. CWE is classifying the issue as CWE-269. This is going to have an impact on confidentiality, integrity, and availability. The weakness was published in 04/26/2019. This vulnerability is uniquely identified as CVE-2019-2725 since 12/14/2018. The exploitability is told to be easy. It is possible to initiate the attack remotely. No form of authentication is needed for exploitation. Technical details are unknown, but a public exploit is available.		
5.	Command Injection	CVE-2019-19681	Pandora FMS 7.x Alert System Remote Code Execution	A vulnerability was found in <a href="https://vuldb.com/?product.pandora:fms">Pandora FMS 7.x</a>. It has been declared as critical. Affected by this vulnerability is an unknown code block of the component <em>Alert System</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 Command Injection attack.