Weekly Zero-Day Vulnerability Coverage Bulletin

(27th January – 2nd February)

Summary:

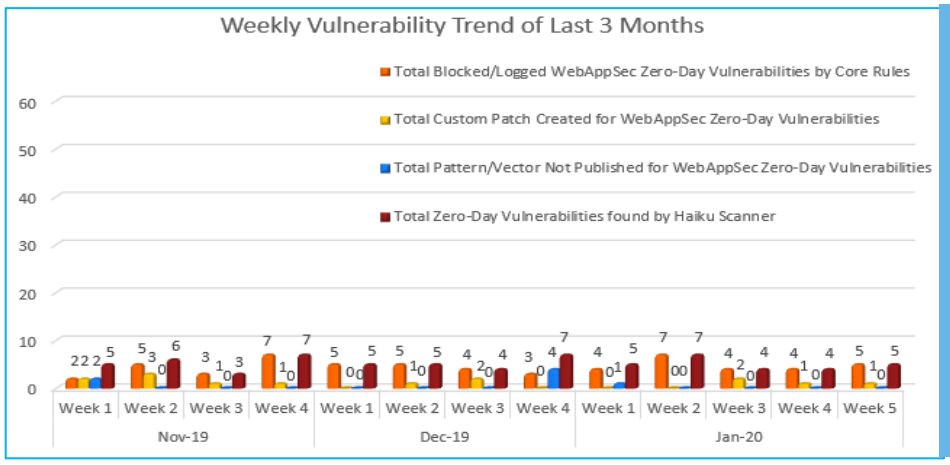
Total **6 Zero-Day Vulnerabilities** were discovered in **4 Categories** this week

2	2	1	1
Cross Site Scripting	Command Injection	Cross Site Request Forgery	Directory Traversal

Zero-Day Vulnerabilities Protected through Core Rules	5
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	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:

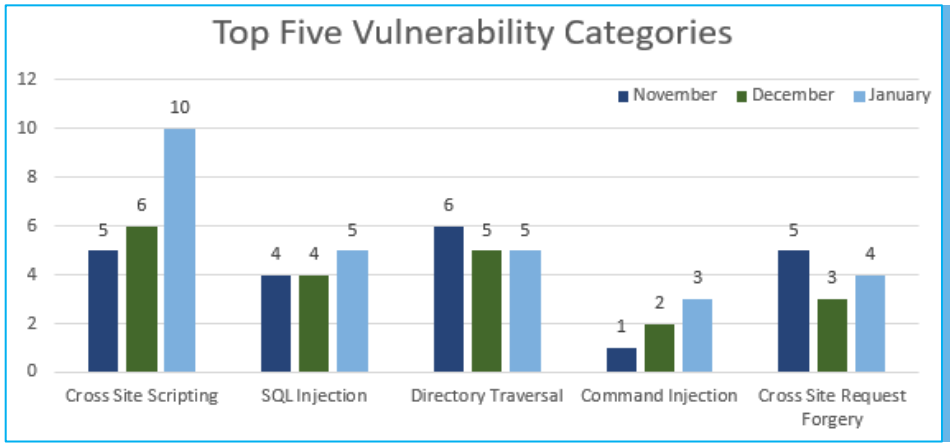


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

39% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

9% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

47% 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 January 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-2020-7994	Dolibarr ERP CRM 10.0.6 dict.php Parameter cross site scripting	A vulnerability classified as problematic has been found in Dolibarr ERP CRM 10.0.6 (Enterprise Resource Planning Software). This affects an unknown function of the file /htdocs/admin/dict.php?id=3. 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.
		CVE-2020-7996	Dolibarr ERP CRM 10.0.6 passwordforgotten.php Referer cross site scripting	A vulnerability, which was classified as problematic, has been found in Dolibarr ERP CRM 10.0.6 (Enterprise Resource Planning Software). This issue affects some unknown functionality of the file htdocs/user/passwordforgotten.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 Cross Site Scripting attack.
2.	Command Injection	CVE-2019-17095	BitDefender BOX 2 2.1.47.42 API /api/download_image command injection	A vulnerability was found in BitDefender BOX 2 2.1.47.42. It has been rated as critical. Affected by this issue is an unknown function of the file /api/download_image of the component API. 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.
		CVE-2020-7799	FusionAuth up to 1.10.x E-Mail Template OS Command Injection	A vulnerability has been found in FusionAuth up to 1.10.x and classified as critical. Affected by this vulnerability is an unknown	Protected by Default Rules.	Detected by scanner as Command Injection attack.

			privilege escalation	code of the component E-Mail Template Handler. Upgrading to version 1.11.0 eliminates this vulnerability.		
3.	Cross Site Request Forgery	CVE-2020-8420	Joomla CMS up to 3.9.14 com_templates cross site request forgery	A vulnerability, which was classified as problematic, has been found in Joomla CMS up to 3.9.14 (Content Management System). Affected by this issue is an unknown code of the component com_templates. Upgrading to version 3.9.15 eliminates this vulnerability.	Protected by Custom Rules.	NA
4.	Directory Traversal	CVE-2020-3717	Magento up to 1.9.4.3/1.14.4.3 /2.2.10/2.3.3 directory traversal	A vulnerability was found in Magento up to 1.9.4.3/1.14.4.3/2.2.10/2.3.3. It has been rated as problematic. 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 Directory Traversal attack.