Weekly Zero-Day Vulnerability Coverage Bulletin

(28th January – 3rd February)

Summary:

Total **12 Zero-Day Vulnerabilities** were discovered in **3 Categories** previous week

7
Cross Site Scripting

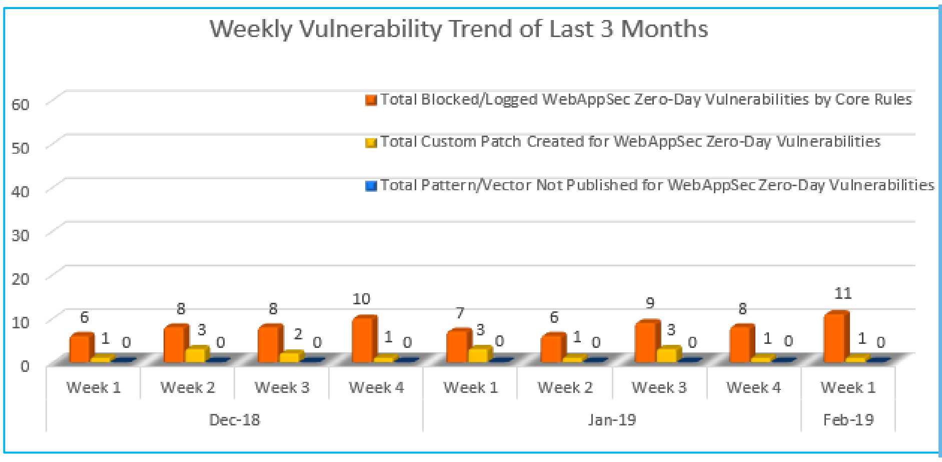
4
Directory Traversal

1
Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	11
Zero-Day Vulnerabilities Protected through Custom Rules	1*
Zero-Day Vulnerabilities for which protection cannot be determined	0**

* To enable custom rules please contact support@indusface.com
** Since attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected

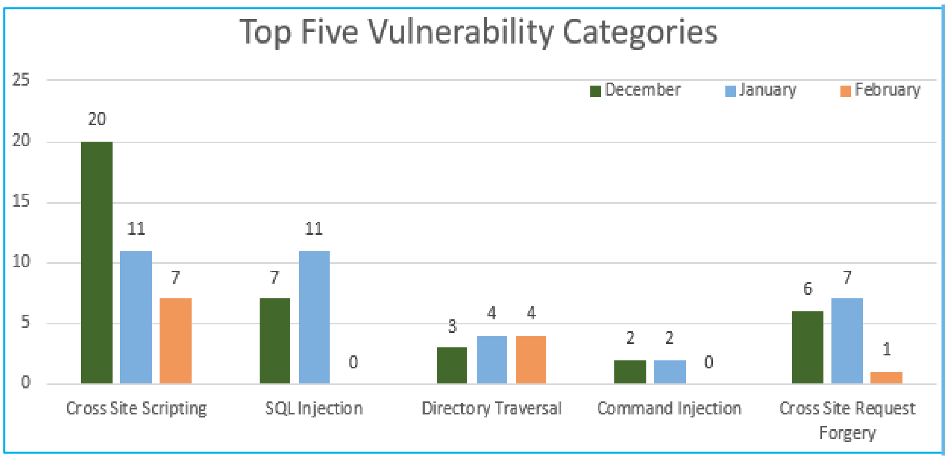
Vulnerability Trend:



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

82% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

18% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



From the graph, we infer that maximum Cross Site Scripting vulnerabilities were discovered in December compared to other months and categories so far.

Medium no. of SQL Injection and CSRF attacks was found in all the months.

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
1.	Cross Site Scripting	CVE-2019-6979	User IP History Logs 1.0.2 on MyBB ip_history_logs.php useragent cross site scripting	A vulnerability, which was classified as problematic, has been found in User IP History Logs 1.0.2 on MyBB (Network Encryption Software). This issue affects some functionality of the file *admin/modules/tools/ip_history_logs.php*. The manipulation of the argument useragent with an unknown input leads to a cross site scripting vulnerability. Using CWE to declare the problem leads to CWE-80. Impacted is integrity. An attacker might be able to inject arbitrary html and script code into the website. This would alter the appearance.	Protected by Default Rules.
		CVE-2019-7172	ATutor up to 2.2.4 my_edit.php cross site scripting	A vulnerability, which was classified as problematic, was found in a Tutor up to 2.2.4 (Network Encryption Software). This affects a function of the file */mods/_core/users/admins/my_edit.php*. The manipulation with an unknown input leads to a cross site scripting vulnerability (Stored). CWE is classifying the issue as CWE-79. This is going to have an impact on integrity. An attacker might be able to inject arbitrary html and script code into the website. This would alter the appearance.	Protected by Default Rules.
		CVE-2019-7171	Croogo up to 3.0.5 Title Field 8 cross site scripting	A vulnerability, which was classified as problematic, has been found in Croogo up to 3.0.5. Affected by this issue is some functionality of the file */admin/blocks/blocks/ed	Protected by Default Rules.

		it/8* of the component *Title Field Handler*. The manipulation with an unknown input leads to a cross site scripting vulnerability (Stored). Using CWE to declare the problem leads to CWE-79. Impacted is integrity. An attacker might be able to inject arbitrary html and script code into the website. This would alter the appearance.	
CVE-2019-7170	Croogo up to 3.0.5 Title Field vocabularies cross site scripting	A vulnerability classified as problematic was found in Croogo up to 3.0.5. Affected by this vulnerability is the functionality of the file */admin/taxonomy/vocabularies* of the component *Title Field Handler*. The manipulation with an unknown input leads to a cross site scripting vulnerability (Stored). The CWE definition for the vulnerability is CWE-79. As an impact it is known to affect integrity. An attacker might be able to inject arbitrary html and script code into the website.	Protected by Default Rules.
CVE-2019-7169	Croogo up to 3.0.5 Title Field 3 cross site scripting	A vulnerability classified as problematic has been found in Croogo up to 3.0.5. Affected is an unknown function of the file */admin/menus/menus/edit/3* of the component *Title Field Handler*. The manipulation with an unknown input leads to a cross site scripting vulnerability (Stored). CWE is classifying the issue as CWE-79. This is going to have an impact on integrity. An attacker might be able to inject arbitrary html and script code into the website.	Protected by Default Rules.

		CVE-2019-7168	Croogo up to 3.0.5 Blog Field blog cross site scripting	A vulnerability was found in Croogo up to 3.0.5. It has been rated as problematic. This issue affects some processing of the file */admin/nodes/nodes/add/blog* of the component *Blog Field Handler*. The manipulation with an unknown input leads to a cross site scripting vulnerability (Stored). Using CWE to declare the problem leads to CWE-79. Impacted is integrity. An attacker might be able to inject arbitrary html and script code into the website. This would alter the appearance.	Protected by Default Rules.
		CVE-2019-6992	ZoneMinder up to 1.32.3 controlcaps.php cross site scripting	A vulnerability has been found in ZoneMinder up to 1.32.3 (Log Management Software) and classified as problematic. Affected by this vulnerability is a functionality of the file *web/skins/classic/views/controlcaps.php*. The manipulation with an unknown input leads to a cross site scripting vulnerability (Stored). The CWE definition for the vulnerability is CWE-80. As an impact it is known to affect integrity. An attacker might be able to inject arbitrary html and script code into the website. This would alter the appearance.	Protected by Default Rules.
2.	Directory Traversal	CVE-2019-7237	idreamsoft iCMS 7.0.13 on Windows editor.admincp.php directory traversal	A vulnerability has been found in idreamsoft iCMS 7.0.13 on Windows (Content Management System) and classified as critical. Affected by this vulnerability is a functionality of the file *editor/editor.admincp.php*. The manipulation with the input value ..\	Protected by Default Rules.

		leads to a directory traversal vulnerability. The CWE definition for the vulnerability is CWE-22. As an impact it is known to affect confidentiality, integrity, and availability. The summary by CVE is:An issue was discovered in idreamsoft iCMS 7.0.13 on Windows.	
CVE-2019-7236	idreamsoft iCMS 7.0.13 editor.admincp.php directory traversal	A vulnerability, which was classified as critical, was found in idreamsoft iCMS 7.0.13 (Content Management System). Affected is a function of the file *editor/editor.admincp.php*. The manipulation with the input value ../ leads to a directory traversal vulnerability. CWE is classifying the issue as CWE-22. This is going to have an impact on confidentiality, integrity, and availability. CVE summarizes:An issue was discovered in idreamsoft iCMS 7.0.13. editor/editor.admincp.php allows admincp.php?app=editor&do=fileManager dir=../ Directory Traversal.The weakness was published 01/30/2019.	
CVE-2019-7235	idreamsoft iCMS 7.0.13 admincp.php directory traversal	A vulnerability, which was classified as critical, has been found in idreamsoft iCMS 7.0.13 (Content Management System). This issue affects some functionality of the file *admincp.php?app=apps&do=save*. The manipulation with the input value /../ leads to a directory traversal vulnerability. Using CWE to declare the problem leads to CWE-22. Impacted is integrity, and availability. The summary	Protected by Default Rules.

				by CVE is: An issue was discovered in idreamsoft iCMS 7.0.13. admincp.php?app=apps&do=save allows directory traversal via _app=/../ to designate an arbitrary directory because of an apps.admincp.php.	
		CVE-2019-7234	idreamsoft iCMS 7.0.13 admincp.php directory traversal	A vulnerability classified as problematic was found in idreamsoft iCMS 7.0.13 (Content Management System). This vulnerability affects the functionality of the file *admincp.php?app=apps &do=save*. The manipulation with the input value /../ leads to a directory traversal vulnerability. The CWE definition for the vulnerability is CWE-22. As an impact it is known to affect confidentiality. CVE summarizes: An issue was discovered in idreamsoft iCMS 7.0.13. admincp.php?app=apps&do=save allows directory traversal via _app=/../ to begin the process of creating a ZIP archive file.	Protected by Default Rules.
3.	Cross Site Request Forgery	CVE-2019-3604	McAfee ePO Cloud cross site request forgery [CVE-2019-3604]	A vulnerability has been found in McAfee ePO Cloud (Cloud Software) and classified as problematic. Affected by this vulnerability is a functionality. The manipulation with an unknown input leads to a cross site request forgery vulnerability. The CWE definition for the vulnerability is CWE-352. As an impact it is known to affect confidentiality, integrity, and availability. An attacker might be able force legitimate users to initiate unwanted actions within web application.	Protected by Custom Rules.