Weekly Zero-Day Vulnerability Coverage Bulletin

(25th February – 3rd March)

Summary:

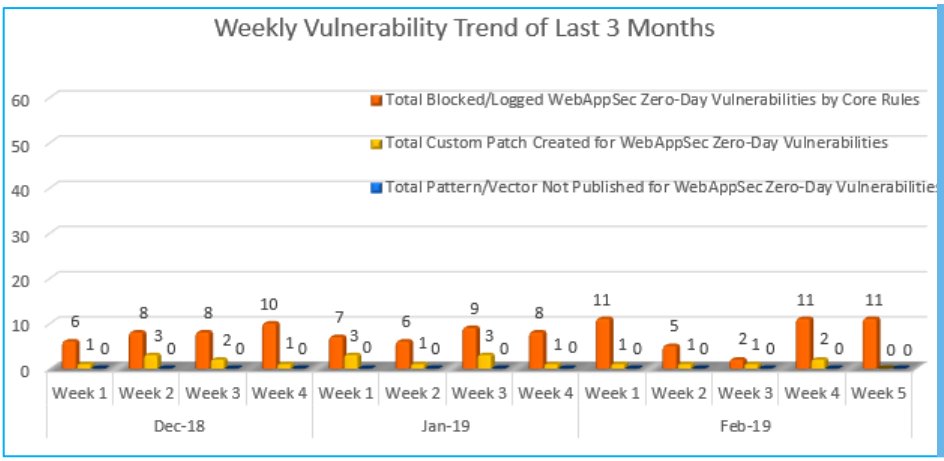
Total **11 Zero-Day Vulnerabilities** were discovered in **4 Categories** this week

2	1	7	1
Cross Site Scripting	SQL Injection	Directory Traversal	Command Injection

Zero-Day Vulnerabilities Protected through Core Rules	11
Zero-Day Vulnerabilities Protected through Custom Rules	0*
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

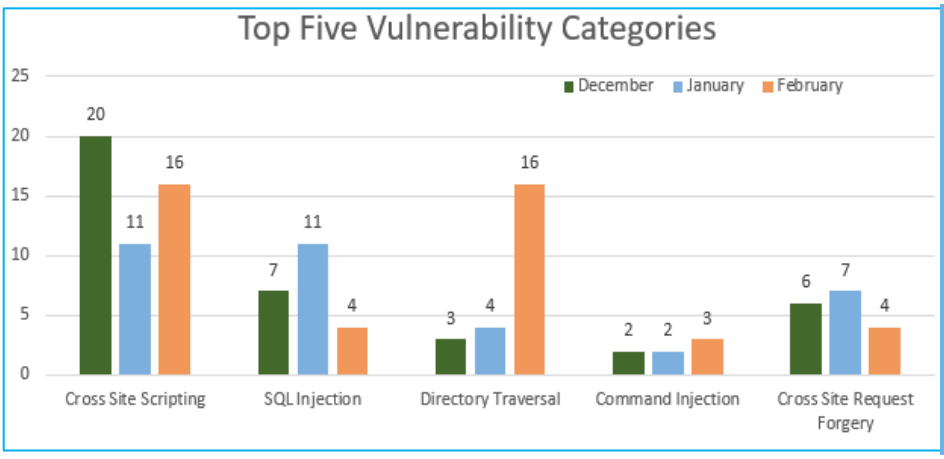
Vulnerability Trend:



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

84% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

16% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



From the graph, we infer that maximum no. of Cross Site Scripting vulnerabilities were discovered in October compared to other months and categories so far.

Medium no. of SQL Injection and CSRF 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-2019-8410	MacCMS 8.0 inc/config/cache.php t_name cross site scripting	A vulnerability classified as problematic was found in MacCMS 8.0 (Content Management System). This vulnerability affects the functionality of the file *inc/config/cache.php*. The manipulation of the argument t_name as part of a *Parameter* leads to a cross site scripting vulnerability. 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. This would alter the appearance.	Protected by Default Rules.
		CVE-2019-8278	Invision Power Board up to 3.3.x/3.4.8 Stored cross site scripting	A vulnerability classified as problematic was found in Invision Power Board up to 3.3.x/3.4.8 (Forum Software). Affected by this vulnerability is the functionality. 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 web site. This would alter the appearance and would make it possible.	Protected by Default Rules.
2.	SQL Injection	CVE-2019-9184	J2Store Plugin up to 3.3.6 on Joomla! product_option[] sql injection	A vulnerability has been found in J2Store Plugin up to 3.3.6 on Joomla! (Network Encryption Software) and classified as critical. This vulnerability affects a functionality. The manipulation of the argument product_option[] with an unknown input leads to a sql injection vulnerability. The CWE definition for the vulnerability is CWE-89. As an impact it is known to affect confidentiality, integrity, and availability. An attacker might be able inject and/or alter existing SQL statements which	Protected by Default Rules.

				would influence the database exchange.	
3.	Directory Traversal	CVE-2018-20795	Tecrail Responsive FileManager up to 9.13.4 ajax_calls.php path directory traversal	A vulnerability was found in Tecrail Responsive FileManager up to 9.13.4. It has been classified as critical. This affects code of the file *ajax_calls.php*. The manipulation of the argument path as part of a *Parameter* leads to a directory traversal vulnerability. CWE is classifying the issue as CWE-22. This is going to have an impact on confidentiality. The weakness was released 02/25/2019 as *EDB-ID 45987* as uncorroborated exploit (Exploit-DB). The advisory is shared at exploit-db.com. This vulnerability is uniquely identified	Protected by Default Rules.
		CVE-2018-20794	Tecrail Responsive FileManager 9.13.4 ajax_calls.php save_img path directory traversal	A vulnerability was found in Tecrail Responsive FileManager 9.13.4 and classified as critical. Affected by this issue is the function save_img of the file *ajax_calls.php*. The manipulation of the argument path as part of a *Image File* leads to a directory traversal vulnerability. Using CWE to declare the problem leads to CWE-22. Impacted is integrity, and availability. The weakness was published 02/25/2019 as *EDB-ID 45987* as uncorroborated exploit (Exploit-DB). The advisory is shared for download at exploit-db.com.	Protected by Default Rules.
		CVE-2018-20793	Tecrail Responsive FileManager 9.13.4 execute.php create_file paths[0] directory traversal	A vulnerability has been found in Tecrail Responsive FileManager 9.13.4 and classified as critical. Affected by this vulnerability is the function create_file of the file *execute.php*. The manipulation of the argument paths[0] with an unknown input leads to a directory traversal vulnerability. The CWE definition for the vulnerability is CWE-22. As an impact it is known to affect integrity, and availability. The weakness was shared 02/25/2019 as	Protected by Default Rules.

		EDB-ID 45987 as uncorroborated exploit (Exploit-DB). It is possible to read the advisory.	
CVE-2018-20792	Tecrail Responsive FileManager 9.13.4 ajax_calls.php get_file path directory traversal	A vulnerability, which was classified as critical, was found in Tecrail Responsive FileManager 9.13.4. Affected is the function get_file of the file *ajax_calls.php*. The manipulation of the argument path as part of a *Parameter* leads to a directory traversal vulnerability. CWE is classifying the issue as CWE-22. This is going to have an impact on confidentiality. The weakness was presented 02/25/2019 as *EDB-ID 45987* as uncorroborated exploit (Exploit-DB). The advisory is available at exploit-db.com. This vulnerability is traded as CVE-2018-20792.	Protected by Default Rules.
CVE-2018-20790	Tecrail Responsive FileManager 9.13.4 execute.php delete_file paths[0] directory traversal	A vulnerability classified as critical was found in Tecrail Responsive FileManager 9.13.4. This vulnerability affects the function delete_file of the file *execute.php*. The manipulation of the argument paths[0] with an unknown input leads to a directory traversal vulnerability. The CWE definition for the vulnerability is CWE-22. As an impact it is known to affect integrity, and availability. The weakness was released in 02/25/2019 as *EDB-ID 45987* as uncorroborated exploit (Exploit-DB). The advisory is shared for download at exploit-db.com.	Protected by Default Rules.
CVE-2018-20789	Tecrail Responsive FileManager 9.13.4 execute.php delete_folder paths[0] directory traversal	A vulnerability classified as critical has been found in Tecrail Responsive FileManager 9.13.4. This affects the function delete_folder of the file *execute.php*. The manipulation of the argument paths[0] with an unknown input leads to a directory traversal vulnerability. CWE is classifying the issue as CWE-22. This is going to have an impact on	Protected by Default Rules.

				integrity, and availability. The weakness was published 02/25/2019 as *EDB-ID 45987* as uncorroborated exploit (Exploit-DB). It is possible to read the advisory at exploit-db.com.	
		CVE-2018-1775	IBM SAN Volume Controller up to 8.2 directory traversal [CVE-2018-1775]	A vulnerability was found in IBM SAN Volume Controller, Storwize, Spectrum Virtualize and FlashSystem up to 8.2 (Network Encryption Software). It has been classified as problematic. This affects code. The manipulation with an unknown input leads to a directory traversal vulnerability. CWE is classifying the issue as CWE-22. This is going to have an impact on confidentiality. The weakness was published in 02/27/2019. It is possible to read the advisory at exchange.xforce.ibmcloud .com. This vulnerability is uniquely identified as CVE-2018-1775 since 12/13/2017.	Protected by Default Rules.
4.	Command Injection	CVE-2019-9194	elFinder up to 2.1.47 PHP Connector command injection	A vulnerability classified as critical has been found in elFinder up to 2.1.47. This affects an unknown function of the component *PHP Connector*. The manipulation with an unknown input leads to a privilege escalation vulnerability (Command Injection). CWE is classifying the issue as CWE-88. This is going to have an impact on confidentiality, integrity, and availability. The weakness was shared 02/26/2019 (GitHub Repository). The advisory is shared at github.com. This vulnerability is uniquely identified as CVE-2019-9194 since 02/26/2019.	Protected by Default Rules.