Weekly Zero-Day Vulnerability Coverage Bulletin

(4th February – 10th February)

Summary:

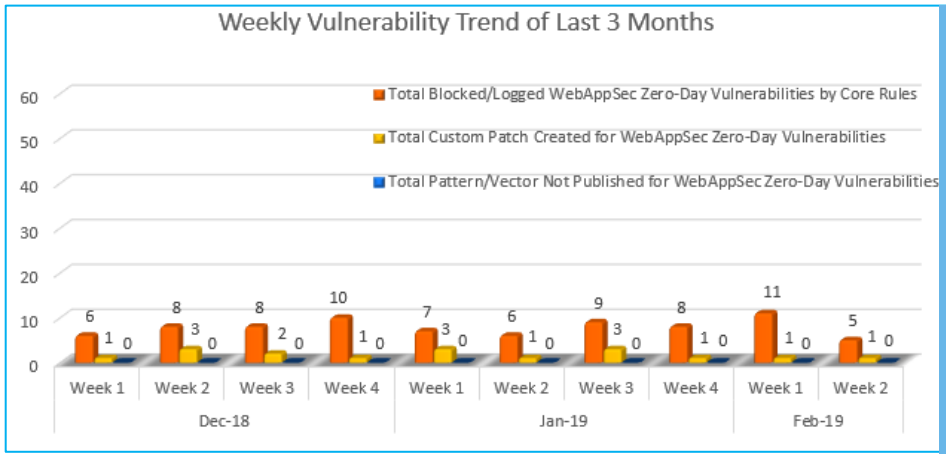
Total **6 Zero-Day Vulnerabilities** were discovered in **4 Categories** previous week

3	1	1	1
Cross Site Scripting	SQL Injection	Command Injection	Cross Site Request Forgery

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**

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

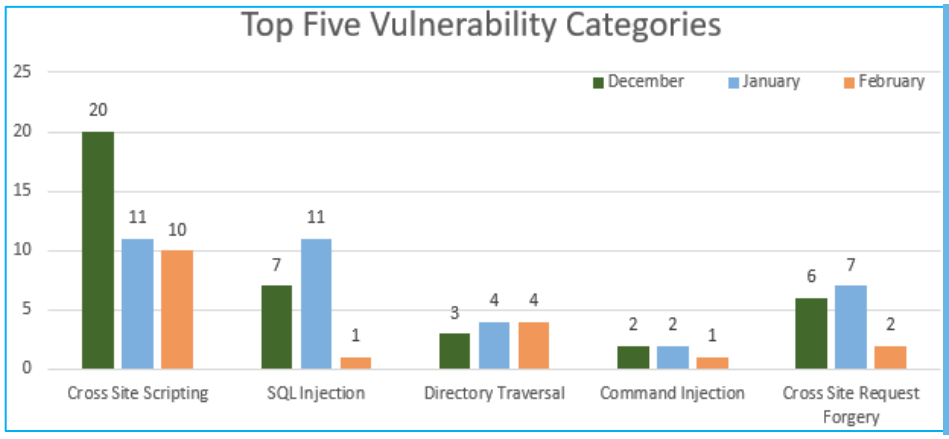
Vulnerability Trend:



Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a 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-2019-7352	ZoneMinder up to 1.32.3 state.php state/newState cross site scripting	A vulnerability was found in ZoneMinder up to 1.32.3 (Video Surveillance Software) and classified as problematic. Affected by this issue is a part of the file *state.php*. The manipulation of the argument state/newState with an unknown input leads to a cross site scripting vulnerability (Stored). Using CWE to declare the problem leads to CWE-79. Integrity is impacted. 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-2019-7349	ZoneMinder up to 1.32.3 monitor.php newMonitor[V4L CapturesPerFram e] cross site scripting	A vulnerability, which was classified as problematic, has been found in ZoneMinder up to 1.32.3 (Video Surveillance Software). This issue affects some functionality of the file *monitor.php*. The manipulation of the argument newMonitor[V4LCaptures PerFrame] as part of a *Parameter* leads to a cross site scripting vulnerability (Reflected). 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-2019-7348	ZoneMinder up to 1.32.3 user.php username cross site scripting	A vulnerability classified as problematic was found in ZoneMinder up to 1.32.3 (Video Surveillance Software). This vulnerability affects the functionality of the file *user.php*. The manipulation of the argument username as part of a *Parameter* 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	Protected by Default Rules.

				attacker might be able to inject arbitrary html and script code into the website.	
2.	SQL Injection	CVE-2019-7316	CSS-TRICKS Chat2 up to 2015-05-05 jumpin.php userid sql injection	A vulnerability classified as critical was found in CSS-TRICKS Chat2 up to 2015-05-05 (Chat Software). Affected by this vulnerability is the functionality of the file *jumpin.php*. The manipulation of the argument userid as part of a *Parameter* 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 would influence the database exchange.	Protected by Default Rules.
3.	Command Injection	CVE-2019-4038	IBM Security Identity Manager up to 6.0/7.0 Code Injection privilege escalation	A vulnerability classified as critical has been found in IBM Security Identity Manager up to 6.0/7.0. Affected is an unknown function. The manipulation with an unknown input leads to a privilege escalation vulnerability (Code Injection). CWE is classifying the issue as CWE-94. This is going to have an impact on confidentiality, integrity, and availability. CVE summarizes:IBM Security Identity Manager 6.0 and 7.0 could allow an attacker to create unexpected control flow paths through the application, potentially bypassing security checks.	Protected by Default Rules.
4.	Cross Site Request Forgery	CVE-2019-1003010	Git Plugin up to 3.9.1 on Jenkins GitTagAction.java cross site	A vulnerability, which was classified as problematic, has been found in Git Plugin up to 3.9.1 on Jenkins (Versioning	Protected by Custom Rules.

		request forgery	Software). This issue affects some functionality of the file *src/main/java/hudson/plugins/git/GitTagAction.java*. The manipulation with an unknown input leads to a cross site request forgery vulnerability. Using CWE to declare the problem leads to CWE-352. Impacted is integrity. An attacker might be able force legitimate users to initiate unwanted actions within the web application. The weakness was released 02/06/2019.