Weekly Zero-Day Vulnerability Coverage Bulletin

(21st January – 27th January)

Summary:

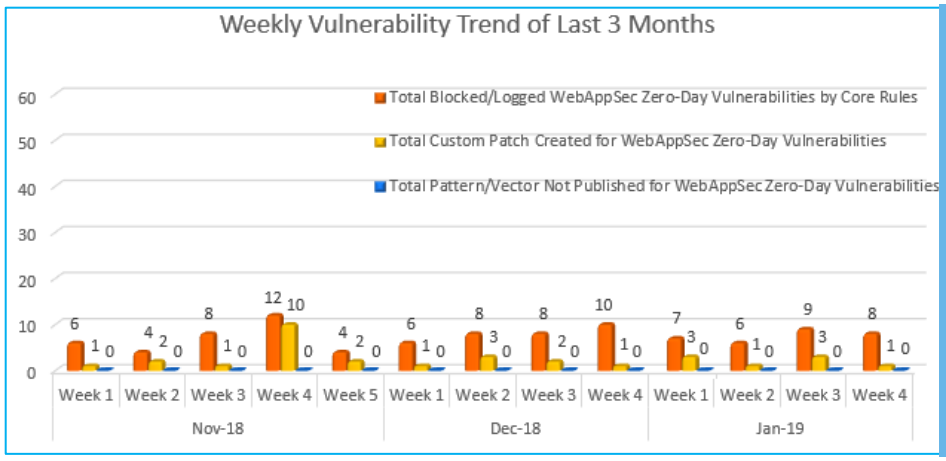
Total **9 Zero-Day Vulnerabilities** were discovered in **5 Categories** this week

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

Zero-Day Vulnerabilities Protected through Core Rules	8
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

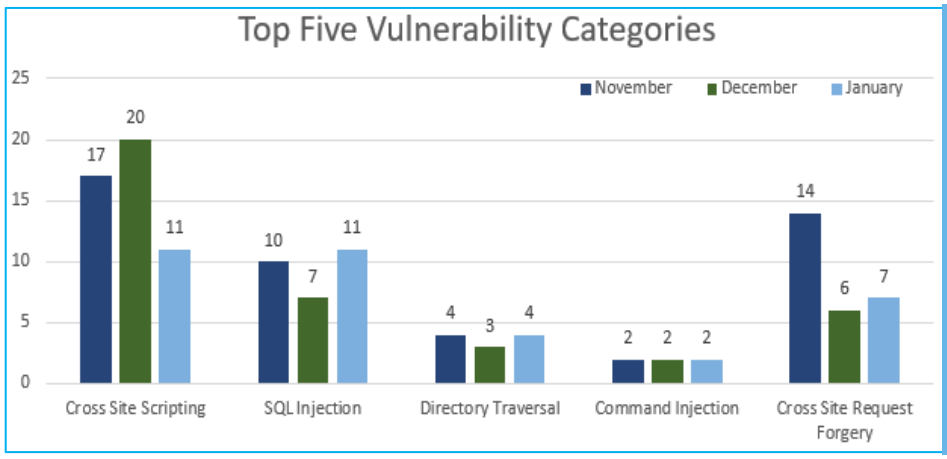
Vulnerability Trend:



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

76% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

24% 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-2019-6229	Apple iCloud for Windows up to 7.9 WebKit cross site scripting	A vulnerability, which was classified as problematic, has been found in Apple iCloud for Windows up to 7.9 (Cloud Software). This issue affects some functionality of the component *WebKit*. The manipulation 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 web site. This would alter the appearance and would make it possible.	Protected by Default Rules.
		CVE-2019-6803	typora up to 0.9.9.20.3 Beta Left Outline Bar cross site scripting	A vulnerability classified as problematic was found in typora up to 0.9.9.20.3 Beta. This vulnerability affects the functionality of the component *Left Outline Bar*. The manipulation with an unknown input leads to a cross site scripting vulnerability. 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.	Protected by Default Rules.
		CVE-2019-1668	Cisco SocialMiner Web-based User Interface HTTP Request cross site scripting	A vulnerability, which was classified as problematic, was found in Cisco SocialMiner. This affects a function of the component *Web-based User Interface*. The manipulation as part of a *HTTP Request* leads to a cross site scripting vulnerability. CWE is classifying the issue as CWE-80. 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.
2.	SQL Injection	CVE-2019-6708	PHPSHE 1.7 admin.php state sql injection	A vulnerability classified as critical has been found in PHPSHE 1.7. Affected is an unknown function of	Protected by Default Rules.

			the file *admin.php?mod=order*. The manipulation of the argument state as part of a *Parameter* leads to a sql injection vulnerability. CWE is classifying the issue as CWE-89. This is going to have an impact on confidentiality, integrity, and availability. An attacker might be able to inject and/or alter existing SQL statements which would influence the database exchange. The weakness was published in 01/23/2019.	
	CVE-2019-6707	PHPSHE 1.7 admin.php product_id[] sql injection	A vulnerability was found in PHPSHE 1.7. It has been rated as critical. This issue affects some processing of the file *admin.php?mod=product&act=state*. The manipulation of the argument product_id[] as part of a *Parameter* leads to a sql injection vulnerability. Using CWE to declare the problem leads to CWE-89. Impacted is confidentiality, integrity, and availability. An attacker might be able inject and/or alter existing SQL statements which would influence the database exchange. The weakness was shared in 01/23/2019.	Protected by Default Rules.
	CVE-2019-6798	phpMyAdmin up to 4.8.5 Designer Username sql injection	A vulnerability has been found in phpMyAdmin up to 4.8.5 (Database Administration Software) and classified as critical. This vulnerability affects a functionality of the component *Designer*. The manipulation as part of a *Username* 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.	Directory Traversal	CVE-2018-1000997	Jenkins up to 2.145 Stapler Web Framework Facet.java directory traversal	A vulnerability, which was classified as critical, was found in Jenkins up to 2.145 (Continuous Integration Software). This affects a function of the file *core/src/main/java/org/kohsuke/stapler/Facet.java* of the component *Stapler Web Framework*. 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, integrity, and availability. The summary by CVE is:A path traversal vulnerability exists in the Stapler web framework used by Jenkins 2.145.	Protected by Default Rules.
4.	Cross Site Request Forgery	CVE-2019-6779	CScms 4.1.8 admin.php/links/save cross site request forgery	A vulnerability was found in CScms 4.1.8 (Content Management System). It has been classified as problematic. Affected is code of the file *admin.php/links/save*. The manipulation with an unknown input leads to a cross site request forgery vulnerability. CWE is classifying the issue as CWE-352. This is going to have an impact on integrity. An attacker might be able force legitimate users to initiate unwanted actions within the web application. The weakness was shared 01/24/2019. This vulnerability is traded as CVE-2019-6779.	Protected by Custom Rules.
5.	Command Injection	CVE-2018-12237	Symantec Reporter CLI up to 10.1.5.5/10.2.1.7 command injection	A vulnerability, which was classified as critical, was found in Symantec Reporter CLI up to 10.1.5.5/10.2.1.7 (Reporting Software). This	Protected by Default Rules.

		affects a function. 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 presented 01/24/2019. The advisory is shared at support.symantec.com. This vulnerability is uniquely identified as CVE-2018-12237 since 06/12/2018. A single authentication is necessary.