Weekly Zero-Day Vulnerability Coverage Bulletin

(31st December – 6th January)

Summary:

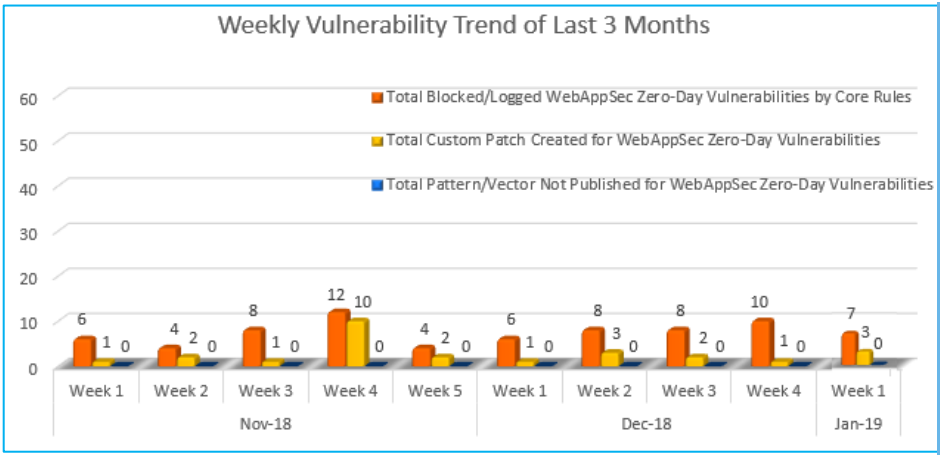
Total **10 Zero-Day Vulnerabilities** were discovered in **5 Categories** previous week

1	2	1	3	3
Cross Site Scripting	Local File Inclusion	Directory Traversal	SQL Injection	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	7
Zero-Day Vulnerabilities Protected through Custom Rules	3*
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

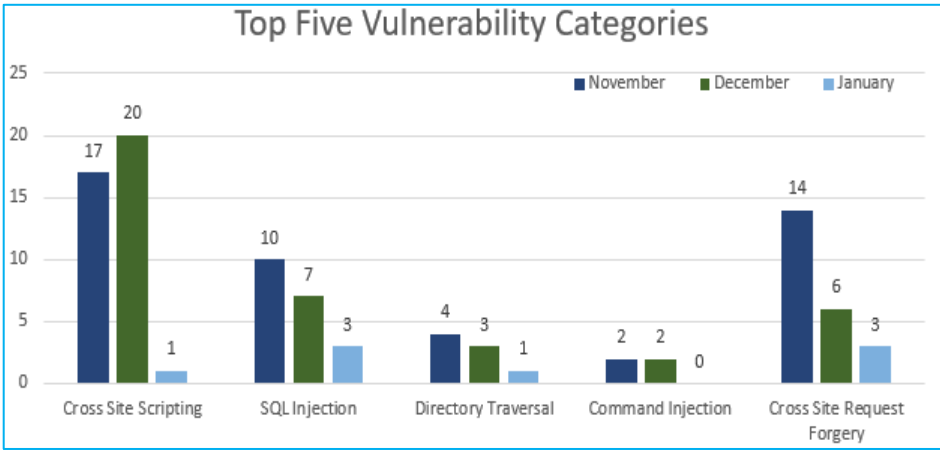
Vulnerability Trend:



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

74% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

26% 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-2018-20611	imcat 4.4 Cookie binfo.php cross site scripting	A vulnerability was found in imcat 4.4. It has been classified as problematic. This affects code of the file *root/tools/adbug/binfo.php?cookie* of the component *Cookie Handler*. The manipulation with an unknown input 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-2018-19998	Dolibarr 8.0.2 user/card.php employee sql injection	A vulnerability, which was classified as critical, was found in Dolibarr 8.0.2. This affects a function of the file *user/card.php*. The manipulation of the argument employee 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 inject and/or alter existing SQL statements which would influence the database exchange. The weakness was published in 01/03/2019.	Protected by Default Rules.
		CVE-2018-19994	Dolibarr 8.0.2 product/card.php desiredstock sql injection	A vulnerability classified as critical was found in Dolibarr 8.0.2. This issue affects some functionality of the file *product/card.php*. The manipulation of the argument desiredstock as part of a *Parameter*	Protected by Default Rules.

				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. The weakness was presented in 01/03/2019.	
		CVE-2018-19415	Plikli CMS 4.0.0 join_group.php id sql injection	A vulnerability, which was classified as critical, has been found in Plikli CMS 4.0.0. This issue affects some functionality of the file *join_group.php*. The manipulation of the argument id as part of a *Parameter* leads to a sql injection vulnerability. Using CWE to declare the problem leads to CWE-89. Confidentiality, integrity, and availability are impacted. An attacker might be able inject and/or alter existing SQL statements which would influence the database exchange. The weakness was published in 01/03/2019 as mailing list post.	Protected by Default Rules.
3.	Cross Site Request Forgery	CVE-2018-20613	TEMMOKU T1.09 Beta admin/user/add cross site request forgery	A vulnerability was found in TEMMOKU T1.09 Beta. It has been rated as problematic. This issue affects some processing of the file *admin/user/add*. The manipulation with an unknown input leads to a cross site request forgery vulnerability. Using CWE to declare the problem leads to CWE-352. An attacker might be able force legitimate users to initiate unwanted actions within the web application. The weakness	Protected by Custom Rules.

				was presented in 12/30/2018. The identification of this vulnerability is CVE-2018-20613 since 12/30/2018.	
		CVE-2018-20577	Orange Livebox 00.96.320S cgi-bin/restore.exe cross site request forgery	A vulnerability, which was classified as problematic, has been found in Orange Livebox 00.96.320S. Affected by this issue is some functionality of the file *cgi-bin/restore.exe*. 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 to force legitimate users to initiate unwanted actions within the web application. The weakness was published 12/28/2018. This vulnerability is handled as CVE-2018-20577 since 12/28/2018.	Protected by Custom Rules.
		CVE-2018-20576	Orange Livebox 00.96.320S cgi-bin/autodialing.exe cross site request forgery	A vulnerability classified as problematic was found in Orange Livebox 00.96.320S. Affected by this vulnerability is the functionality of the file *cgi-bin/autodialing.exe*. 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 integrity. An attacker might be able to force legitimate users to initiate unwanted actions within the web application. The weakness was shared 12/28/2018. This vulnerability is known as CVE-2018-20576.	Protected by Custom Rules.
4.	Directory Traversal	CVE-2018-20610	imcat 4.4 root/run/adm.ph	A vulnerability was found in imcat 4.4 and classified as critical. This issue	Protected by Default Rules.

			p efile directory traversal	affects some functionality of the file *root/run/adm.php*. The manipulation of the argument efile with an unknown input leads to a directory traversal vulnerability. Using CWE to declare the problem leads to CWE-22. Impacted is confidentiality, integrity, and availability. CVE summarizes:imcat 4.4 allows directory traversal via the root/run/adm.php efile parameter. The weakness was published in 12/30/2018. This vulnerability is handled as CVE-2018-20610 since 12/30/2018.	
5.	Local File Inclusion	CVE-2018-17246	Kibana Local File Inclusion Flaw	Kibana versions before 6.4.3 and 5.6.13 contain an arbitrary file inclusion flaw in the Console plugin. An attacker with access to the Kibana Console API could send a request that will attempt to execute java script code. This could possibly lead to an attacker executing arbitrary commands with permissions of the Kibana process on the host system.	Protected by Default Rules.
		CVE-2018-17246	Kibana Local File Inclusion Flaw	Kibana versions before 6.4.3 and 5.6.13 contain an arbitrary file inclusion flaw in the Console plugin. An attacker with access to the Kibana Console API could send a request that will attempt to execute java script code. This could possibly lead to an attacker executing arbitrary commands with permissions of the Kibana process on the host system.	Protected by Default Rules.