Weekly Zero-Day Vulnerability Coverage Bulletin

(14th January – 20th January)

Summary:

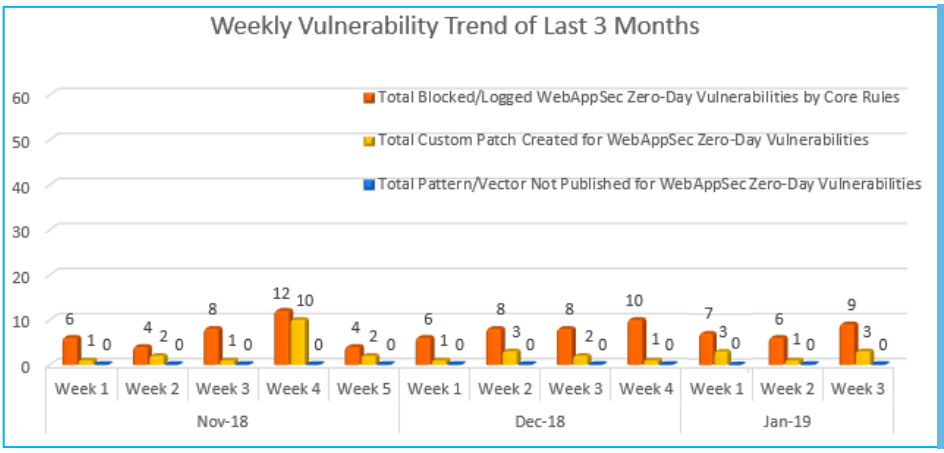
Total **12 Zero-Day Vulnerabilities** were discovered in **5 Categories** in this week

4	4	1	2	1
Cross Site Scripting	SQL Injection	Command Injection	Cross Site Request Forgery	Denial of Service

Zero-Day Vulnerabilities Protected through Core Rules	9
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

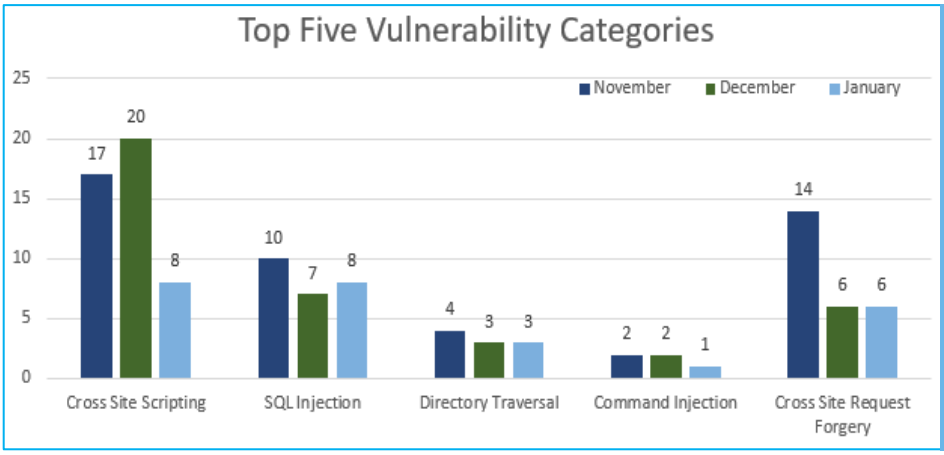
Vulnerability Trend:



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

75% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

25% 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-2018-1967	IBM Security Identity Manager 6.0.0 Web UI cross site scripting	A vulnerability classified as problematic was found in IBM Security Identity Manager 6.0.0. Affected by this vulnerability is the functionality of the component *Web UI*. 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-2018-20703	CubeCart 6.2.2 /{ADMIN-FILE}/ Query String cross site scripting	A vulnerability, which was classified as problematic, was found in CubeCart 6.2.2. Affected is a function of the file */{ADMIN-FILE}/*. The manipulation as part of a *Query String* leads to a cross site scripting vulnerability (Reflected). 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 web site. This would alter the appearance and would make it possible to initiate.	Protected by Default Rules.
		CVE-2018-20729	NeDi up to 1.7Cp2 mh.php reg cross site scripting	A vulnerability was found in NeDi up to 1.7Cp2 and classified as problematic. This issue affects a part of the file *mh.php*. The manipulation of the argument reg 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.	Protected by Default Rules.

		CVE-2019-0646	Microsoft Team Foundation Server 2018 Update 3.2 cross site scripting	A vulnerability, which was classified as problematic, was found in Microsoft Team Foundation Server 2018 Update 3.2. Affected is a function. 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 web site. This would alter the appearance and would make it possible to initiate further attacks.	Protected by Default Rules.
2.	SQL Injection	CVE-2019-6259	idreamsoft iCMS 7.0.13 article.admincp.php data_id sql injection	A vulnerability, which was classified as critical, was found in idreamsoft iCMS 7.0.13. This affects a function of the file *app/article/article.admincp.php*. The manipulation of the argument data_id 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 presented in 01/14/2019.	Protected by Default Rules.
		CVE-2019-6296	Cleanto 5.0 export_ajax.php id sql injection	A vulnerability classified as critical has been found in Cleanto 5.0. This affects an unknown function in the library *assets/lib/export_ajax.php*. The manipulation of the argument id as part of a *Parameter* leads to a sql injection vulnerability. CWE is classifying the issue as	Protected by Default Rules.

		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 shared in 01/15/2019.	
CVE-2019-6295	Cleanto 5.0 service_method_ajax.php service_id sql injection	A vulnerability was found in Cleanto 5.0. It has been rated as critical. Affected by this issue is some processing in the library *assets/lib/service_method_ajax.php*. The manipulation of the argument service_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 presented in 01/15/2019.	Protected by Default Rules.
CVE-2018-20730	NeDi up to 1.7Cp2 query.php sql injection	A vulnerability was found in NeDi up to 1.7Cp2. It has been classified as critical. Affected is code of the file *query.php*. The manipulation with an unknown input lead 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	Protected by Default Rules.

				which would influence the database exchange. The weakness was published in 01/17/2019.	
3.	Cross Site Request Forgery	CVE-2019-6249	HuCart 5.7.4 index.php cross site request forgery	A vulnerability has been found in HuCart 5.7.4 and classified as problematic. Affected by this vulnerability is a functionality of the file */adminsys/index.php?load=admins&act=edit_info&act_type=add*. 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 force legitimate users to initiate unwanted actions within the web application. The weakness was published in 01/13/2019.	Protected by Custom Rules.
		CVE-2018-16887	Satellite up to 3.9.0 katello cross site request forgery	A vulnerability was found in Satellite up to 3.9.0. It has been declared as problematic. Affected by this vulnerability is a code block of the component *katello*. 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 force legitimate users to initiate unwanted actions within the web application. The weakness was shared in 01/13/2019.	Protected by Custom Rules.

4.	Command Injection	NA	ThinkPHP - Remote Code Execution	A vulnerability in the framework's invoke Function method to execute malicious code on the underlying server. The vulnerability is remotely exploitable, as most vulnerabilities in web-based apps tend to be and can allow an attacker to gain control over the server.	Protected by Custom Rules.
5.	Denial of Service	NA	Sieren: A new DoS bot	Zscaler ThreatLabZ recently discovered a new DoS family bot named Sieren. A denial-of-service (DoS) attack is a cyber-attack in which cybercriminals disrupt the service of a host connected to the internet, either temporarily or indefinitely, to its intended users.	Protected by Default Rules.