Weekly Zero-Day Vulnerability Coverage Bulletin

(24th December – 30th December)

Summary:

Total **11 Zero-Day Vulnerabilities** were discovered in **5 Categories** this week

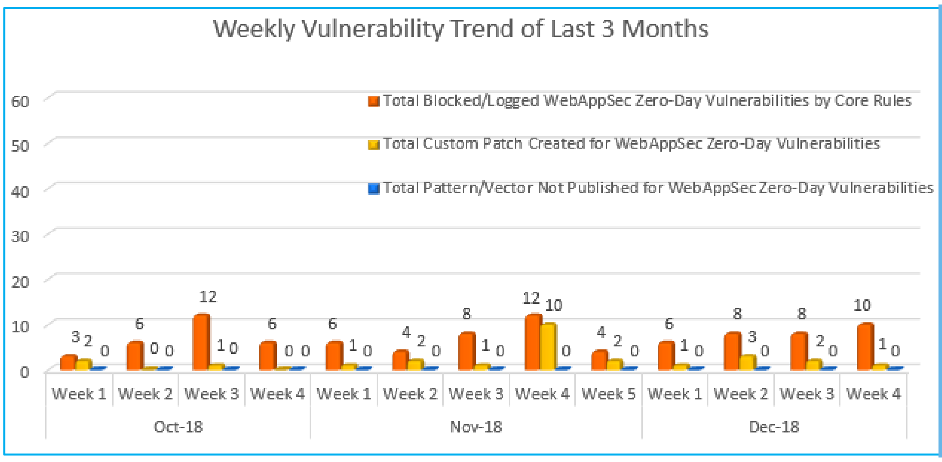
6	1	1	2	1
Cross Site Scripting	SQL Injection	Directory Traversal	Command Injection	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	10
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

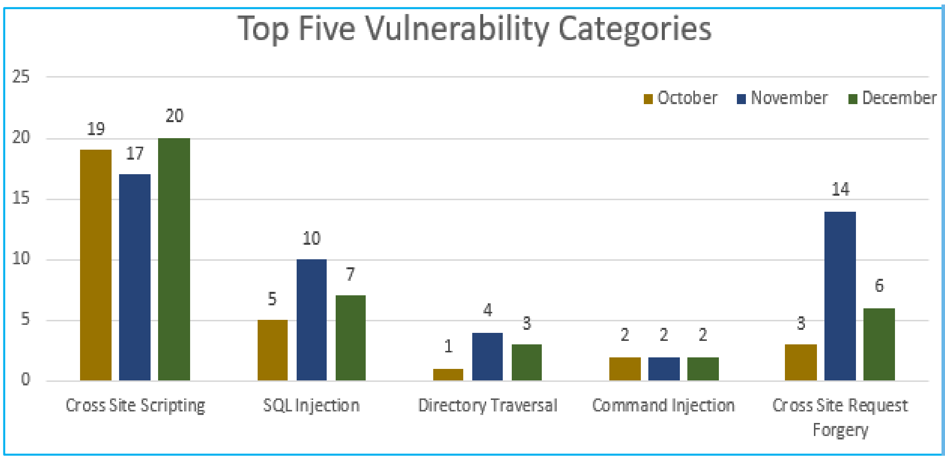
Vulnerability Trend:



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

79% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

21% 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-2018-20370	SZ NetChat up to 7.8 Options Module MyName cross site scripting	A vulnerability, which was classified as problematic, was found in SZ NetChat up to 7.8. Affected is a function of the component *Options Module*. The manipulation of the argument MyName 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.	Protected by Default Rules.
		CVE-2018-20369	Barracuda Message Archiver 2018 Add_Update Module ldap_load_entry.cgi ldap_user cross site scripting	A vulnerability, which was classified as problematic, has been found in Barracuda Message Archiver 2018. This issue affects some functionality of the file *cgi-mod/ldap_load_entry.cgi* of the component *Add_Update Module*. The manipulation of the argument ldap_user as part of a *Parameter* 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.	Protected by Default Rules.
		CVE-2018-20368	Master Slider Plugin 3.2.7/3.5.1 on WordPress wp-admin/admin-ajax.php Name cross site scripting	A vulnerability classified as problematic was found in Master Slider Plugin 3.2.7/3.5.1 on WordPress. This vulnerability affects the functionality of the file *wp-admin/admin-ajax.php*. The manipulation of the argument Name 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	Protected by Default Rules.

				inject arbitrary html and script code into the website. This would alter the appearance.	
		CVE-2018-20418	Craft CMS 3.0.25 cross site scripting [CVE-2018-20418]	A vulnerability was found in Craft CMS 3.0.25 and classified as problematic. Affected by this issue is a part of the file *index.php?p=admin/actions/entries/save-entry*. 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 website. This would alter the appearance and would make it possible to initiate further attacks against site	Protected by Default Rules.
		CVE-2018-8918	Synology Router Manager up to 1.1.7 info.cgi host cross site scripting	A vulnerability was found in Synology Router Manager up to 1.1.7. It has been classified as problematic. This affects code of the file *info.cgi*. The manipulation of the argument host as part of a *Parameter* 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. This would alter the appearance.	Protected by Default Rules.
		CVE-2018-8917	Synology DiskStation Manager up to 6.1.6 info.cgi host cross site scripting	A vulnerability was found in Synology DiskStation Manager up to 6.1.6 and classified as problematic. Affected by this issue is a part of the file *info.cgi*. The manipulation of the argument host as part of a *Parameter* 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.	Protected by Default Rules.
2.	SQL Injection	CVE-2018-7802	EVLink Parking up to v3.2.0-12_v1 Web	A vulnerability classified as critical has been found in EVLink Parking up to	Protected by Default Rules.

			Interface sql injection	v3.2.0-12_v1. This affects an unknown function of the component *Web Interface*. The manipulation with an unknown input lead to 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 12/24/2018.	
		CVE-2018-7835	IIoT Monitor 3.1.38 directory traversal [CVE-2018-7835]	A vulnerability, which was classified as critical, has been found in IIoT Monitor 3.1.38. This issue affects some functionality. The manipulation 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. The summary by CVE is: An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in IIoT Monitor 3.1.38 which could allow access to files available to SYSTEM user.	Protected by Default Rules.
4.	Cross Site Request Forgery	CVE-2018-19182	Engelsystem cross site request forgery [CVE-2018-19182]	A vulnerability, which was classified as problematic, has been found in Engelsystem (unknown version). This issue affects some functionality. 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	Protected by Custom Rules.

				force legitimate users to initiate unwanted actions within the web application. The weakness was released in 12/26/2018 (GitHub Repository). The advisory is shared at github.com.	
5.	Command Injection	CVE-2018-7801	EVLink Parking up to v3.2.0-12_v1 Remote Code Execution [CVE-2018-7801]	A vulnerability was found in EVLink Parking up to v3.2.0-12_v1. It has been rated as critical. Some processing is affected by this issue. The manipulation with an unknown input leads to a privilege escalation vulnerability (Code Execution). Using CWE to declare the problem leads to CWE-269. Impacted is confidentiality, integrity, and availability. The weakness was shared in 12/24/2018. The advisory is shared for download at schneider-electric.com. This vulnerability is handled as CVE-2018-7801 since 03/08/2018. The attack might be launched remotely.	Protected by Default Rules.
		CVE-2018-20463	JSmol2WP Plugin 1.07 on WordPress query SSRF directory traversal	A vulnerability was found in JSmol2WP Plugin 1.07 on WordPress. It has been rated as critical. Some processing is affected by this issue. The manipulation of the argument query as part of a *Query String* leads to a directory traversal vulnerability (SSRF). Using CWE to declare the problem leads to CWE-918. Impacted is confidentiality, integrity, and availability. CVE summarizes: An issue was discovered in JSmol2WP plugin 1.07 for WordPress. There is an arbitrary file read vulnerability via../directory traversal.	Protected by Default Rules.