Weekly Zero-Day Vulnerability Coverage Bulletin

(17th December – 23rd December)

Summary:

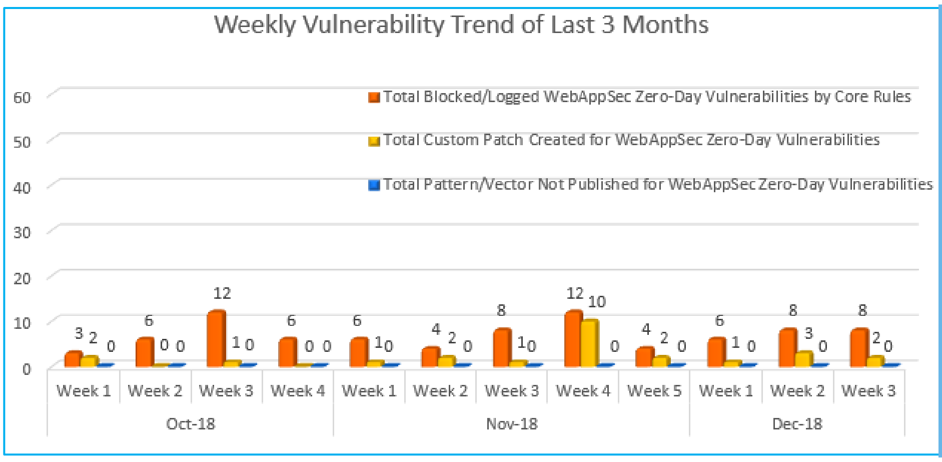
Total **10 Zero-Day Vulnerabilities** were discovered in **4 Categories** this week

4 Cross Site Scripting	**2** SQL Injection	**2** Directory Traversal	**2** Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	8
Zero-Day Vulnerabilities Protected through Custom Rules	2*
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

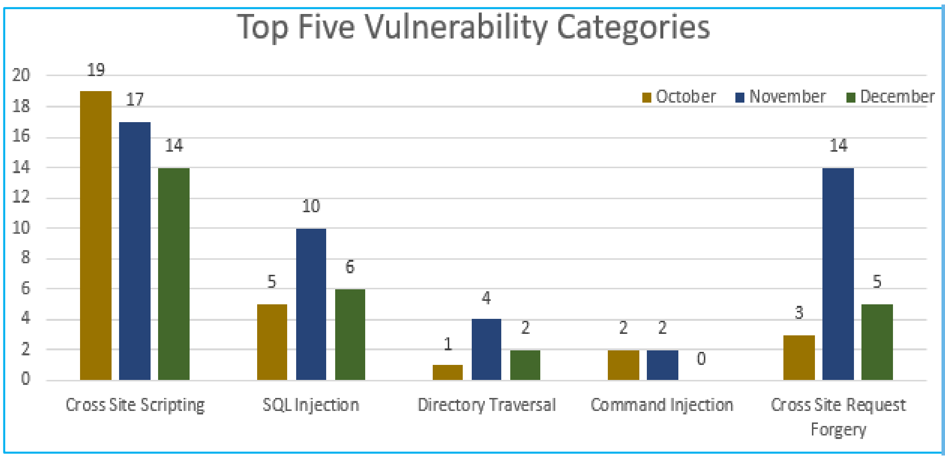
Vulnerability Trend:



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

77% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

23% 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-2018-20153	WordPress up to 5.0.0 Comment cross site scripting	A vulnerability classified as problematic has been found in WordPress up to 5.0.0. Affected is an unknown function of the component *Comment 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. This would alter the appearance and would make it possible to initiate.	Protected by Default Rules.
		CVE-2018-20150	WordPress up to 5.0.0 Plugin cross site scripting	A vulnerability was found in WordPress up to 5.0.0. It has been classified as problematic. This affects an unknown function of the component *Plugin*. 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. This would alter the appearance and make it possible to initiate.	Protected by Default Rules.
		CVE-2018-20172	Nagios XI up to 5.5.7 magpie_slashbox.php rss_url cross site scripting	A vulnerability, which was classified as problematic, has been found in Nagios XI up to 5.5.7. Affected by this issue is an unknown function of the file *rss_dashlet/magpierss/scripts/magpie_slashbox.php*. The manipulation of the argument rss_url 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 website.	Protected by Default Rules.

		CVE-2018-20171	Nagios XI up to 5.5.7 magpie_simple.php url cross site scripting	A vulnerability classified as problematic was found in Nagios XI up to 5.5.7. Affected by this vulnerability is an unknown function of the file *rss_dashlet/magpierss/scripts/magpie_simple.php* . The manipulation of the argument url as part of a *Parameter* 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.
2.	SQL Injection	CVE-2018-18923	Abisoft Ticketly up to 1.0 action/addproject.php name/category_id/description Parameter sql injection	A vulnerability, which was classified as critical, was found in Abisoft Ticketly up to 1.0. This affects the function name/category_id/description of the file *action/addproject.php*. The manipulation 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 12/13/2018 as *EDB-ID.	Protected by Default Rules.
		CVE-2018-20329	Chamilo LMS 1.11.8 CoursesAndSessionsCatalog.class.php Database sql injection	A vulnerability has been found in Chamilo LMS 1.11.8 and classified as critical. This vulnerability affects a functionality in the library *main/inc/lib/CoursesAndSessionsCatalog.class.php *. The manipulation as part of a *Database* 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	Protected by Default Rules.

				weakness was disclosed in 12/21/2018.	
3.	Directory Traversal	CVE-2017-18354	Rendertron 1.0.0 Protocol Local File Inclusion	A vulnerability, which was classified as problematic, has been found in Rendertron 1.0.0. This issue affects an unknown function of the component *Protocol Handler*. The manipulation with an unknown input leads to an information disclosure vulnerability (Local File Inclusion). Using CWE to declare the problem leads to CWE-200. Impacted is confidentiality. The weakness was shared 12/17/2018. The identification of this vulnerability is CVE-2017-18354 since 12/17/2018. The attack may be initiated remotely. Neither technical details nor the exploit is publicly available.	Protected by Default Rules.
		CVE-2018-19003	GE Mark VIe directory traversal [CVE-2018-19003]	A vulnerability was found in GE Mark VIe, EX2100e, EX2100e_Reg, LS2100e, EX2100e_Reg and LS2100e. It has been rated as problematic. An unknown function is affected by this issue. The manipulation with an unknown input leads to a directory traversal vulnerability. Using CWE to declare the problem leads to CWE-22. Confidentiality is impacted. CVE summarizes: GE Mark VIe, EX2100e, EX2100e_Reg, and LS2100e Versions 03.03.28C to 05.02.04C, EX2100e All versions prior to v04.09.00C, EX2100e_Reg All versions prior to v04.09.00C, and LS2100e All versions.	Protected by Default Rules.

4.	Cross Site Request Forgery	CVE-2018-18921	PHP Server Monitor up to 3.3.1 cross site request forgery [CVE-2018-18921]	A vulnerability was found in PHP Server Monitor up to 3.3.1. It has been rated as problematic. An unknown function is affected by this issue. The manipulation with an unknown input leads to a cross site request forgery vulnerability. Using CWE to declare the problem leads to CWE-352. Integrity is impacted. An attacker might be able to force legitimate users to initiate unwanted actions within the web application. The weakness was disclosed 12/18/2018 (GitHub Repository).	Protected by Custom Rules.
		CVE-2018-20188	Fuel CMS 1.4.3 users/create/ cross site request forgery	A vulnerability was found in Fuel CMS 1.4.3. It has been classified as problematic. Affected is an unknown function of the file *users/create/*. 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 released 12/17/2018. This vulnerability is traded as CVE-2018-20188.	Protected by Custom Rules.