Weekly Zero-Day Vulnerability Coverage Bulletin

(12th November – 18th November)

Summary:

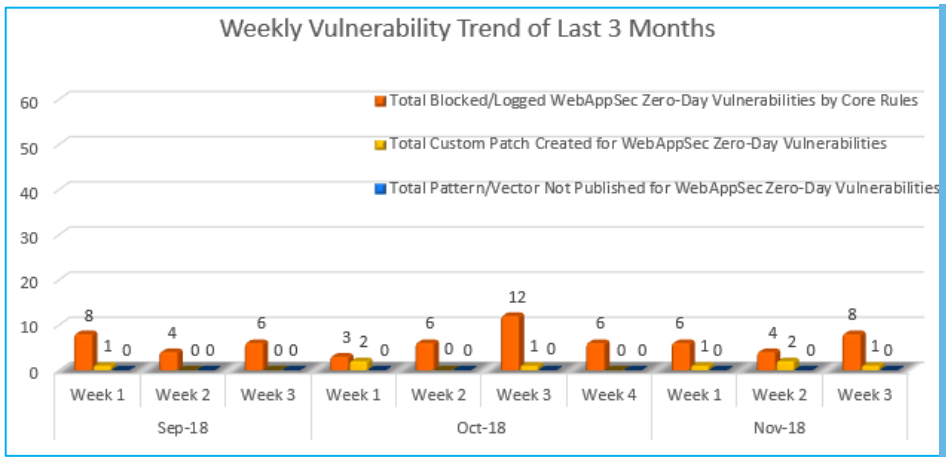
Total **9 Zero-Day Vulnerabilities** were discovered in **4 Categories** this week

5	2	1	1
Cross Site Scripting	SQL 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

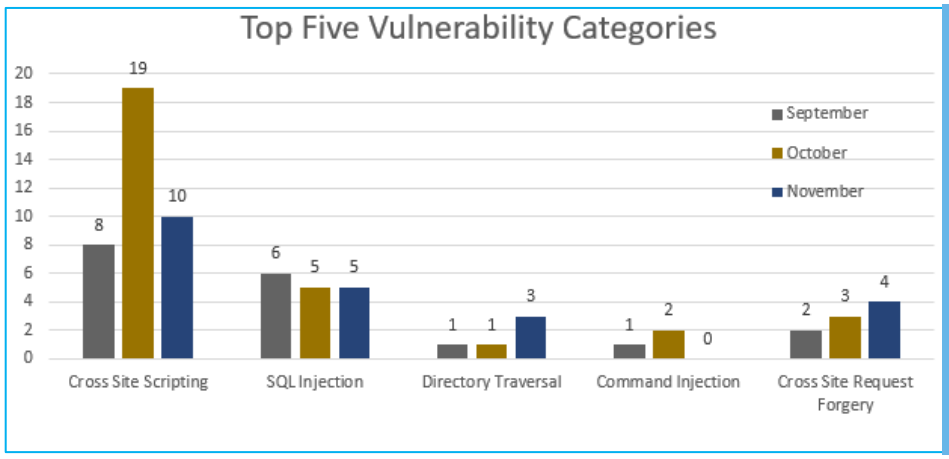
Vulnerability Trend:



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

88% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

12% 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 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-2018-19195	XiaoCms 20141229 show_product.html cross site scripting	A vulnerability, which was classified as problematic, was found in XiaoCms 20141229. Affected is an unknown function of the file *template\default\show_product.html*. 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 further attacks.	Protected by Default Rules.
		CVE-2018-19227	LAOBANCMS 2.0 admin/liuyan.php neirong[] cross site scripting	A vulnerability was found in LAOBANCMS 2.0. It has been rated as problematic. Affected by this issue is an unknown function of the file *admin/liuyan.php*. The manipulation of the argument neirong[] 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 and would make it	Protected by Default Rules.
		CVE-2018-19223	LAOBANCMS 2.0 admin/type.php cross site scripting	A vulnerability has been found in LAOBANCMS 2.0 and classified as problematic. This vulnerability affects an unknown function of the file *admin/type.php?id=1*. 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	Protected by Default Rules.

				script code into the web site. This would alter the appearance and would make it possible to initiate.	
		CVE-2018-8608	Microsoft Dynamics 365 8 Web Request cross site scripting	A vulnerability was found in Microsoft Dynamics 365 8. It has been classified as problematic. Affected is an unknown function. The manipulation as part of a *Web 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 web site. This would alter the appearance and would make it possible to initiate further	Protected by Default Rules.
		CVE-2018-19301	tp4a Teleport 3.1.0 Login Page Username cross site scripting	A vulnerability classified as problematic has been found in tp4a Teleport 3.1.0. Affected is an unknown function of the component *Login Page*. The manipulation as part of a *Username* 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.	Protected by Default Rules.
2.	SQL Injection	CVE-2018-19221	LAOBANCMS 2.0 admin/login.php guanliyuan sql injection	A vulnerability, which was classified as critical, has been found in LAOBANCMS 2.0. Affected by this issue is an unknown function of the file *admin/login.php*. The manipulation of the argument guanliyuan 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	Protected by Default Rules.

				database exchange. The weakness was released in 11/12/2018.	
		CVE-2018-16850	PostgreSQL up to 10.5/11.0 pg_upgrade/pg_dump sql injection	A vulnerability classified as critical was found in PostgreSQL up to 10.5/11.0. This vulnerability affects the function pg_upgrade/pg_dump. The manipulation with an unknown input lead 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 released 11/13/2018 as bug report (Bugzilla). The advisory is available.	Protected by Default Rules.
3.	Directory Traversal	CVE-2018-19197	XiaoCms 20141229 database.php directory traversal	A vulnerability was found in XiaoCms 20141229 and classified as critical. Affected by this issue is an unknown function of the file *admin\controller\database.php*. The manipulation with an unknown input leads to a directory traversal vulnerability. Using CWE to declare the problem leads to CWE-22. Impacted is integrity, and availability. CVE summarizes:An issue was discovered in XiaoCms 20141229. admin\controller\database.php allows arbitrary directory deletion via admin/index.php?c=database&a=import&paths[]=../ directory traversal.The weakness was disclosed 11/12/2018. This vulnerability is handled as CVE-2018-19197 since 11/11/2018. Technical details	Protected by Default Rules.

4.	Cross Site Request Forgery	CVE-2018-19225	LAOBANCMS 2.0 admin/mima.php cross site request forgery	A vulnerability was found in LAOBANCMS 2.0. It has been classified as problematic. Affected is an unknown function of the file *admin/mima.php*. 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 published in 11/12/2018. This vulnerability is traded as CVE-2018-19225.	Protected by Custom Rules.