Weekly Zero-Day Vulnerability Coverage Bulletin

(19th November – 25th November)

Summary:

Total **22 Zero-Day Vulnerabilities** were discovered in **7 Categories** this week

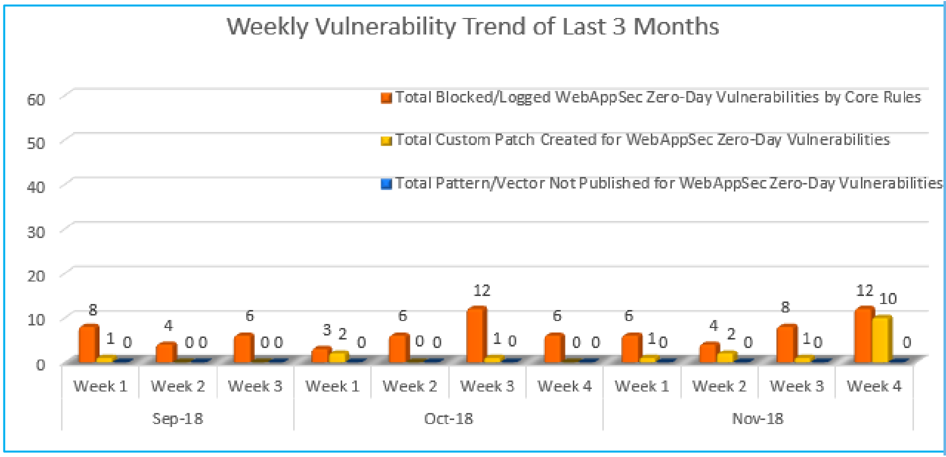
4	**5**	**2**	**1**	**1**	**8**	**1**
Cross Site Scripting	SQL Injection	Malicious File Upload	Directory Traversal	BOT Attack	Cross Site Request Forgery	Command Injection

Zero-Day Vulnerabilities Protected through Core Rules	12
Zero-Day Vulnerabilities Protected through Custom Rules	10*
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

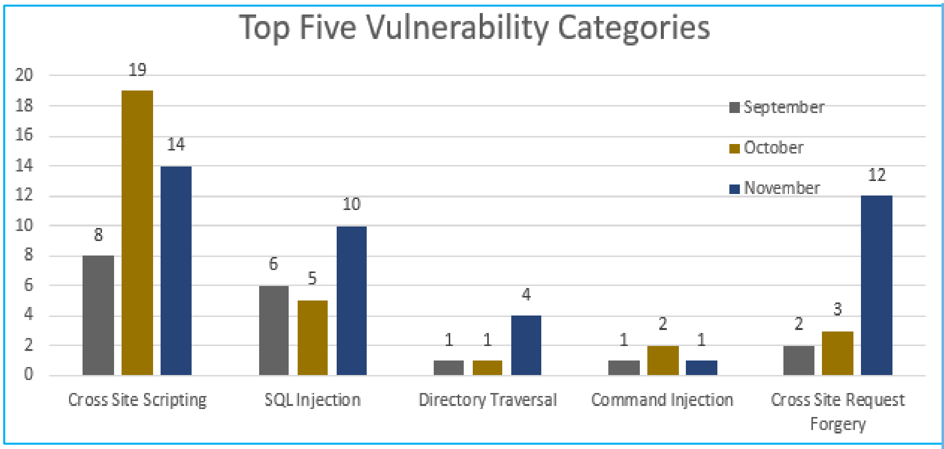
Vulnerability Trend:



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

80% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

20% 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 August compared to other months and categories.

Medium no. of SQL Injection 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-2018-19352	Jupyter Notebook up to 5.7.1 Directory Name notebooklist.js cross site scripting	A vulnerability classified as problematic was found in Jupyter Notebook up to 5.7.1. This vulnerability affects an unknown function of the file *notebook/static/tree/js/ notebooklist.js* of the component *Directory Name Handler*. 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 web site. This would alter the appearance.	Protected by Default Rules.
		CVE-2018-19351	Jupyter Notebook up to 5.7.0 nbconvert Response handlers.py cross site scripting	A vulnerability classified as problematic is found in Jupyter Notebook up to 5.7.0. This affects an unknown function of the file *notebook/nbconvert/handlers.py* of the component *nbconvert Response 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 web site. This would alter the appearance.	Protected by Default Rules.
		CVE-2018-19340	Guriddo Form PHP 5.3 default.php Parameter cross site scripting	A vulnerability was found in Guriddo Form PHP 5.3. It has been classified as problematic. This affects an unknown function of the file *demos/jqform/defaultnodb/default.php*. The manipulation of the argument OrderID/ShipName/ShipAddress/ShipCity/ShipPostalCode /ShipCountry/Freight/details as part of a *Parameter* leads to a	Protected by Default Rules.

				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.	
		NA	Second WordPress hacking campaign underway, this one targeting AMP for WP plugin	The Wordfence team has identified an XSS (cross-site scripting) campaign that is actively exploiting this security flaw. In the post below, we describe this sophisticated attack campaign in detail. It is critical that site owners using AMP for WP update to the most recent version of this plugin as soon as possible. At the time of writing, the newest version of AMP for WP is version 0.9.97.20.	Protected by Default Rules.
2.	SQL Injection	CVE-2018-19349	SeaCMS 6.64 admin_makehtml.php topic sql injection	A vulnerability was found in SeaCMS 6.64. It has been classified as critical. Affected is an unknown function of the file *admin_makehtml.php*. The manipulation of the argument topic 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 released 11/17/2018.	Protected by Default Rules.
		CVE-2018-19331	S-Cms 1.5 search.php keyword sql injection	A vulnerability, which was classified as critical, was found in S-Cms 1.5. Affected is an unknown function of the file *search.php*. The manipulation of the argument keyword 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	Protected by Default Rules.

		SQL statements which would influence the database exchange. The weakne ss was shared 11/17/2018.	
CVE-2018-18806	School Equipment Monitoring System 1.0 Login Screen include/user.vb sql injection	A vulnerability was found in School Equipment Monitoring System 1.0. It has been rated as critical. Affected by this issue is an unknown function of the file *include/user.vb* of the component *Login Screen*. The manipulation with an unknown input lead 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	Protected by Default Rules.
CVE-2018-18805	PointOfSales 1.0 Login Screen LoginForm1.vb sql injection	A vulnerability was found in PointOfSales 1.0. It has been declared as critical. Affected by this vulnerability is an unknown function of the file *LoginForm1.vb* of the component *Login Screen*. 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	Protected by Default Rules.
CVE-2018-18804	Bakeshop Inventory System 1.0 Login Screen publicfunction.vb sql injection	A vulnerability was found in Bakeshop Inventory System 1.0. It has been classified as critical. Affected is an unknown function of the file *include/publicfunction.vb* of the component *Login Screen*. The manipulati on 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.	Protected by Default Rules.

				An attacker might be able inject and/or alter existing SQL statements which would influence the database exchange.	
3.	Malicious File Upload	CVE-2016-1000031	Apache Struts Patches Remote Code Execution Vulnerability in FileUpload Library (CVE-2016-1000031)	A vulnerability, which was classified as critical, has been found in Apache Commons FileUpload (affected version not known). Affected by this issue is an unknown function. The manipulation with an unknown input leads to a privilege escalation vulnerability. Using CWE to declare the problem leads to CWE-284. Impacted is confidentiality, integrity, and availability.	Protected by Custom Rules.
		CVE-2018-15961	Adobe ColdFusion Flaw exploited in attacks in the wild	A vulnerability classified as critical has been found in Adobe ColdFusion up to 11 Update 14/2016 Update 6/2018. Affected is an unknown function. The manipulation with an unknown input leads to a privilege escalation vulnerability (File Upload). CWE is classifying the issue as CWE-434. This is going to have an impact on confidentiality, integrity, and availability.	Protected by Custom Rules.
4.	Directory Traversal	CVE-2018-19328	LAOBANCMS 2.0 install/mysql_hy.php riqi directory traversal	A vulnerability classified as critical was found in LAOBANCMS 2.0. This vulnerability affects an unknown function of the file *install/mysql_hy.php*. The manipulation of the argument riqi with the input value ../ leads to a directory traversal vulnerability. The CWE definition for the vulnerability is CWE-22. As an impact it is known to affect confidentiality, integrity, and availability. CVE summarizes:LAOBANCMS	Protected by Default Rules.

				2.0 allows install/mysql_hy.php?riqi=../ Directory Traversal.The weakness was disclosed 11/17/2018. This vulnerability was named CVE-2018-19328 since 11/17/2018.	
5.	BOT Attack	NA	Mirai: Not Just for IoT Anymore	Botmasters have taken the lessons from developing Internet of Things (IoT) malware and shifted their focus to targeting commodity Linux servers. Like many IoT devices, unpatched Linux servers linger on the network, and are being abused at scale by attackers sending exploits to every vulnerable server they can find. ASERT has been monitoring exploit attempts for the Hadoop YARN vulnerability in our honeypot network and found a familiar, but surprising payload – Mirai. These versions of Mirai behave much like the original but are tailored to run on Linux servers and not underpowered IoT devices. While ASERT has previously published observations of Windows Mirai, this is the first time we've seen non-IoT Mirai in the wild.	Protected by Default Rules.
6.	Command Injection	CVE-2018-18858	LiquidVPN Client up to 1.37 XPC Service tun_path/tap_path OS Command Injection privilege escalation	A vulnerability, which was classified as critical, has been found in LiquidVPN Client up to 1.37. This issue affects an unknown function of the component *XPC Service*. The manipulation of the argument tun_path/tap_path with an unknown input leads to a privilege escalation vulnerability (OS Command Injection). Using CWE to declare the problem leads to CWE-77.	Protected by Default Rules.

				This impacted confidentiality, integrity, and availability. The weakness was disclosed 11/20/2018 as *EDB-ID 45782* as uncorroborated exploit (Exploit-DB). The advisory is shared at exploit-db.com.	
7.	Cross Site Request Forgery	CVE-2018-19332	S-Cms v1.5 ajax.php cross site request forgery	A vulnerability has been found in S-Cms v1.5 and classified as problematic. Affected by this vulnerability is an unknown function of the file *admin/ajax.php?type=member&action=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 11/17/2018.	Protected by Custom Rules.
		CVE-2018-19327	JTBC(PHP) 3.0.1.7 manage.php cross site request forgery	A vulnerability classified as problematic has been found in JTBC(PHP) 3.0.1.7. This affects an unknown function of the file *aboutus/manage.php?type=action&action=add*. 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 11/17/2018. This	Protected by Custom Rules.

		vulnerability is uniquely identified as CVE-2018-19327 since 11/17/2018.	
CVE-20 18-19319	SRCMS 3.0.0 admin.php cross site request forgery	A vulnerability was found in SRCMS 3.0.0 and classified as problematic. Affected by this issue is an unknown function of the file *admin.php?m=Admin&c =gifts&a=update*. 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 force legitimate users to initiate unwanted actions within the web application. The weakness was presented 11/16/2018. This vulnerability is handled as CVE-2018-19319 since 11/16/2018.	Protected by Custom Rules.
CVE-2018-19318	SRCMS 3.0.0 admin.php cross site request forgery	A vulnerability has been found in SRCMS 3.0.0 and classified as problematic. Affected by this vulnerability is an unknown function of the file *admin.php?m=Admin&c =manager&a=update*. 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 disclosed 11/16/2018.	Protected by Custom Rules.

CVE-2018-1 9335	Google Monorail prior 2018-06-07 cross site request forgery [CVE-2018-19335]	A vulnerability was found in Google Monorail. It has been classified as problematic. Affected is an unknown function. 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 shared 11/20/2018. This vulnerability is traded as CVE-2018-19335 since 11/17/2018.	Protected by Custom Rules.
CVE-2018-19334	Google Monorail prior 2018-05-04 cross site request forgery [CVE-2018-19334]	A vulnerability was found in Google Monorail and classified as problematic. This issue affects an unknown function. 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 force legitimate users to initiate unwanted actions within the web application. The weakness was presented 11/20/2018. The identification of this vulnerability is CVE-2018-19334 since 11/17/2018. The attack may be initiated remotely.	Protected by Custom Rules.
CVE-2018 -10099	Google Monorail prior 2018-04-04 cross site request forgery [CVE-2018-10099]	A vulnerability classified as problematic was found in Google Monorail. Affected by this vulnerability is an unknown function. The manipulation with an unknown input leads to a cross site request forgery	Protected by Custom Rules.

		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 11/20/2018. This vulnerability is known as CVE-2018-10099 since 04/13/2018.	
NA	MSA-18-0020: Moodle Login CSRF vulnerability in login form	A vulnerability was found in Moodle up to 3.1.14/3.3.8/3.4.5/3.5.2 and classified as problematic. Affected by this issue is an unknown function. 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 force legitimate users to initiate unwanted actions within the web application.	Protected by Custom Rules.