# Weekly Zero-Day Vulnerability Coverage Bulletin

*(8th October – 14th October)*

Summary:

Total **6 Zero-Day Vulnerabilities** were discovered in **2 Categories** previous week

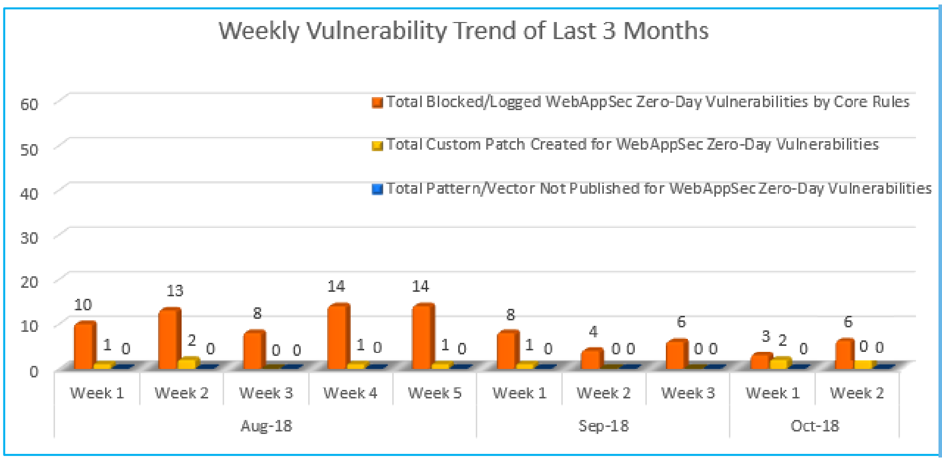
| | |
|---|---|
| **4**<br>Cross Site Scripting | **2**<br>SQL Injection |

| | |
|---|---|
| Zero-Day Vulnerabilities Protected through Core Rules | 6 |
| Zero-Day Vulnerabilities Protected through Custom Rules | 0* |
| 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

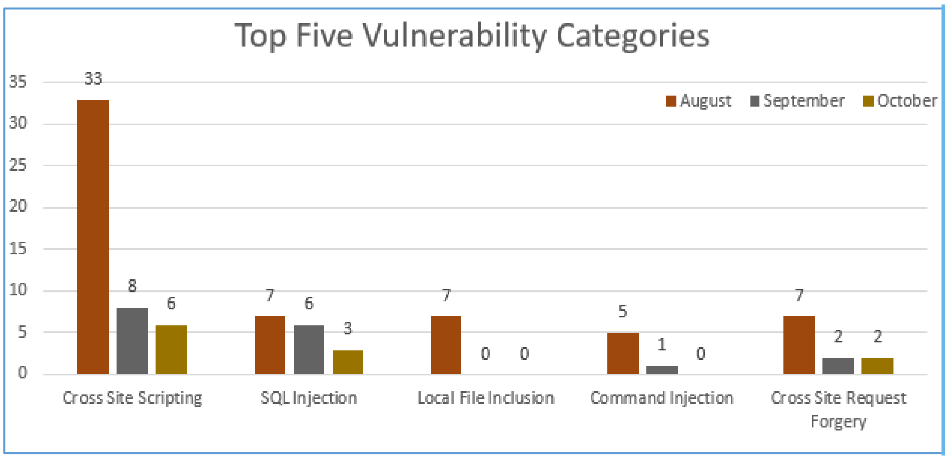
## Vulnerability Trend:



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 Cross Site Scripting vulnerabilities were discovered in July compared to other months and categories so far.

Medium no. of SQL, LFI and CSRF attacks are found.

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-2018-15903 | Discuss Module 1.2.1 on Claromentis Stored cross site scripting | A vulnerability was found in Discuss Module 1.2.1 on Claromentis. It has been classified as problematic. This affects an unknown function. The manipulation with an unknown input leads to a cross site scripting vulnerability (Stored). 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-2018-2470 | SAP NetWeaver Application Server for ABAP up to 7.53 cross site scripting | A vulnerability was found in SAP NetWeaver Application Server for ABAP up to 7.53. It has been declared as problematic. Affected by this vulnerability is an unknown function. 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 and | Protected by Default Rules. |
| | | CVE-2018-17784 | SugarCRM Community Edition 6.5.26 YUI/FlashCanvas cross site scripting | A vulnerability classified as problematic was found in SugarCRM Community Edition 6.5.26. This vulnerability affects an unknown function of the component *YUI/FlashCanvas*. 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 | Protected by Default Rules. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | appearance and would make it possible to initiate | |
| | | CVE-2018-16210 | WAGO 750-881 up to 01.09.19(13) SNMP Configuration webserv/cplcfg/snmp.ssi SNMP_LOC_SNMP_CONT cross site scripting | A vulnerability, which was classified as problematic, has been found in WAGO 750-881 up to 01.09.19(13). Affected by this issue is an unknown function of the file *webserv/cplcfg/snmp.ssi* of the component *SNMP Configuration*. The manipulation of the argument SNMP_LOC_SNMP_CONT 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 web site. This would | Protected by Default Rules. |
| 2. | SQL Injection | CVE-2018-18075 | Wikidforum 2.20 rpc.php parent_post_id/num_records sql injection | A vulnerability classified as critical has been found in Wikidforum 2.20. Affected is an unknown function of the file *rpc.php*. The manipulation of the argument parent_post_id/num_records 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 shared 10/09/2018 as *EDB-ID | Protected by Default Rules. |
| | | CVE-2018-18242 | youke365 1.1.5 admin/login.html Username sql injection | A vulnerability classified as critical has been found in youke365 1.1.5. Affected is an unknown function of the file *admin/login.html*. The manipulation as part of a *Username* 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 | Protected by Default Rules. |

database exchange. The weakness was disclosed 10/11/2018. This vulnerability is traded as CVE-2018-18242