# Weekly Zero-Day Vulnerability Coverage Bulletin

*(18th June – 24th June)*

## Summary:

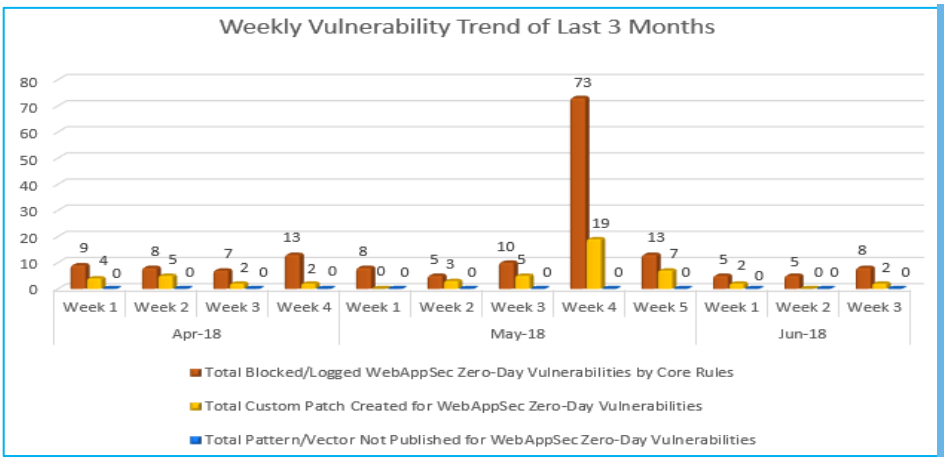
Total **10 Zero-Day Vulnerabilities** were discovered in **6 Categories** previous week

| 2 | 2 | 2 | 1 | 2 | 1 |
|---|---|---|---|---|---|
| Cross Site Scripting | SQL Injection | Local File Inclusion | HTTP Policy Violence | Cross Site Request Forgery | Command Injection |

| | |
|---|---|
| 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:

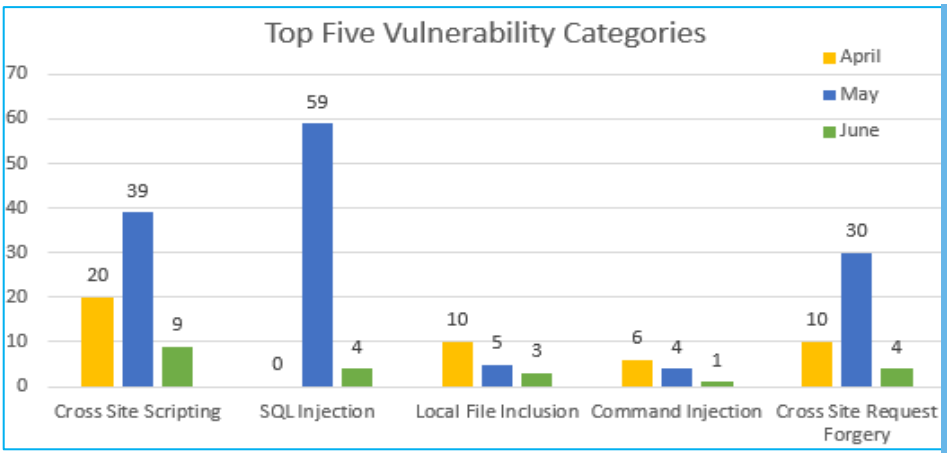



Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

May 4th Week has multiple vulnerabilities blocked by Core Rules.

**75%** Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

**25%** Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months




From the graph, we infer that multiple SQL Injection vulnerabilities were discovered in May compared to other months and categories.

Medium no. of Cross Site Scripting attacks were found in May compared to June.

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-2018-9036 | CheckSec Canopy up to 3.0.6 Login Page Disclaimer Stored cross site scripting | A vulnerability was found in CheckSec Canopy up to 3.0.6 and classified as problematic. This issue affects an unknown function of the component *Login Page Disclaimer*. The manipulation with an unknown input leads to a cross site scripting vulnerability (Stored). 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 an attack. | Protected by Default Rules. |
| | | CVE-2018-12581 | phpMyAdmin up to 4.8.1 Designer js/designer/move.js cross site scripting | A vulnerability was found in phpMyAdmin up to 4.8.1. It has been classified as problematic. This affects an unknown function of the file *js/designer/move.js* of the component *Designer*. 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 and would make it possible to initiate an attack. | Protected by Default Rules. |
| 2. | SQL Injection | CVE-2018-1132 | OpenDaylight SDNInterfaceapp Component Database sql injection | A vulnerability was found in OpenDaylight SDNInterfaceapp (the affected version is unknown). It has been rated as critical. Affected by this issue is an unknown function of the component *Component Database*. The manipulation with an unknown input lead | Protected by Default Rules. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | to 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. | |
| | | CVE-2018-12630 | Newmark NMCMS 2.1 /catalog sect_id sql injection | A vulnerability classified as critical was found in Newmark NMCMS 2.1. Affected by this vulnerability is an unknown function of the file */catalog*. The manipulation of the argument sect_id as part of a *Parameter* leads to 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. | Protected by Default Rules. |
| 3. | Local File Inclusion | EDB-ID: 148226 | Redatam Web Server Directory Traversal | Redatam Web Server prior to version 7 suffer from a directory traversal vulnerability. | Protected by Default Rules. |
| | | CVE-2018-12631 | Redatam7 text LFN directory traversal | A vulnerability, which was classified as problematic, has been found in Redatam7 (the affected version is unknown). Affected by this issue is an unknown function of the file */redbin/rpwebutilities.exe/text*. The manipulation of the argument LFN with the input value ../ leads to a directory traversal vulnerability. Using CWE to declare the problem leads to CWE-22. Impacted is confidentiality. The weakness was disclosed 06/21/2018 as *EDB-ID 44905* as uncorroborated exploit (Exploit-DB). The advisory is shared for download at exploit-db.com. | Protected by Default Rules. |

| | | | | | |
|---|---|---|---|---|---|
| 4. | HTTP Policy Violence | EDB-ID: 148221 | Tapplock Smart Lock Insecure Direct Object Reference | Tapplock Smart Lock suffers from multiple insecure direct object reference vulnerabilities. | Protected by Default Rules. |
| 5. | Command Injection | CVE-2018-11652 | Nikto 2.1.6 CSV Injection | Nikto version 2.1.6 suffers from a csv injection vulnerability. | Protected by Default Rules. |
| 6. | Cross Site Request Forgery | EDB-ID: 148223 | Joomla Jomres 9.11.2 Cross Site Request Forgery | Joomla Jomres component version 9.11.2 suffers from a cross site request forgery vulnerability. | Protected by Custom Rules. |
| | | EDB-ID: 148229 | RabbitMQ Web Management Cross Site Request Forgery | RabbitMQ Web Management versions prior to 3.7.6 suffer from a cross site request forgery vulnerability. | Protected by Custom Rules. |