# Weekly Zero-Day Vulnerability Coverage Bulletin

*(25th June – 1st July)*

## Summary:

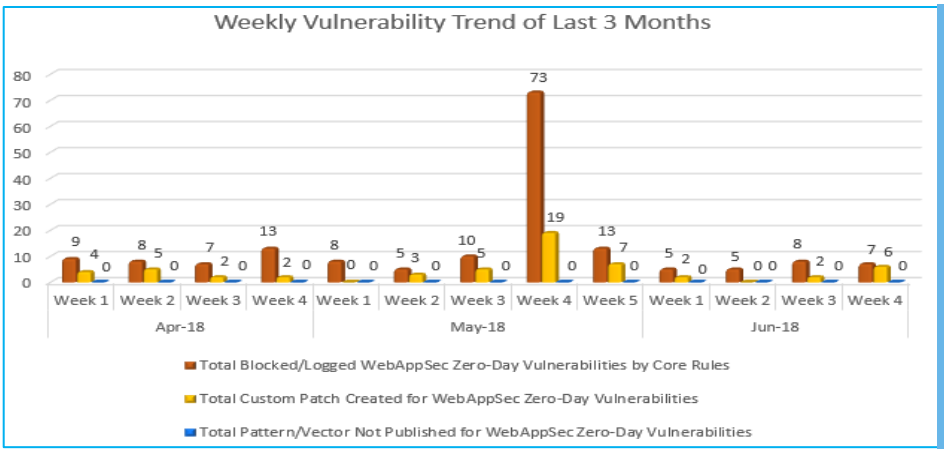
Total **13 Zero-Day Vulnerabilities** were discovered in **5 Categories** previous week

| 3 | 2 | 1 | 5 | 2 |
|---|---|---|---|---|
| Cross Site Scripting | SQL Injection | Arbitrary File Upload | Cross Site Request Forgery | Command Injection |

| | |
|---|---|
| Zero-Day Vulnerabilities Protected through Core Rules | 7 |
| Zero-Day Vulnerabilities Protected through Custom Rules | 6* |
| 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:

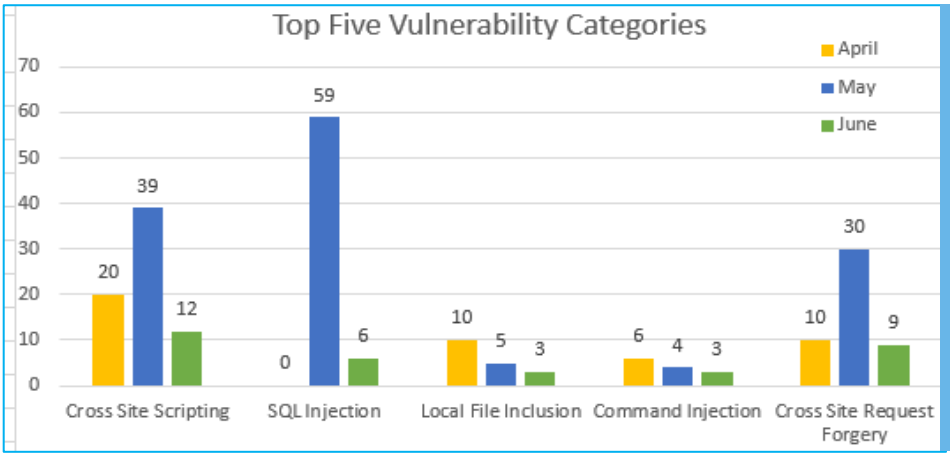



Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

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

**74%** Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

**26%** 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 was 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-2018-7681 | Micro Focus Business Manager up to 11.3 Favourites Cross Site Scripting | A vulnerability was found in Micro Focus Business Manager up to 11.3. It has been classified as problematic. Affected is an unknown function of the component *Favourites 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. | Protected by Default Rules. |
| | | CVE-2018-1507 | IBM DOORS Next Generation 6.0.5 Web UI cross site scripting | A vulnerability, which was classified as problematic, has been found in IBM DOORS Next Generation 6.0.5. This issue affects an unknown function of the component *Web UI*. The manipulation 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 alter the appearance and would make it possible to initiate. | Protected by Default Rules. |
| | | CVE-2018-1000512 | Reflected XSS in Tooltipy (tooltips for WP) | Tootipy contains reflected Cross Site Scripting in the [kttg_glossary] shortcode meaning that admin users' browsers can be hijacked by anybody who sends them a link. The hijacked browser can be made to do almost anything an admin user can normally do. | Protected by Default Rules. |
| 2. | SQL Injection | EDB-ID: 44930 | Travel Agency 1.1 - 'cid' SQL Injection | Vulnerable Source is Line20:if(isset($_GET['action']) && ($_GET['action'] == 'del')){ Line21:$delete = mysql_query("DELETE FROM destination where | Protected by Default Rules. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | destination_id= '".$_GET['cid']."'"); | |
| | | CVE-2018-12984 | Hycus CMS 1.0.4 sql injection [CVE-2018-12984] | A vulnerability was found in Hycus CMS 1.0.4. It has been rated as critical. Affected by this issue is an unknown function. The manipulation with the input value '=' 'OR' 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 database exchange. The weakness was released on 06/29/2018 in *EDB-ID 44954* as uncorroborated exploit (Exploit-DB). | Protected by Default Rules. |
| 3. | Arbitrary File Upload | EDB-ID: 44939 | Intex Router N-150 - Arbitrary File Upload | The firmware allows malicious files to be uploaded without any checking of extensions and allows filed to be uploaded. | Protected by Custom Rules. |
| 4. | Command Injection | CVE-2018-11526 | Wordpress Plugin Comments Import & Export < 2.0.4 - CSV Injection | WordPress Comments Import & Export plugin version 2.0.4 and before are affected by the vulnerability Remote Command Execution using CSV Injection. This allows a public user to inject commands as a part of form fields and when a user with higher privilege exports the form data in CSV opens the file on their machine, the command is executed. | Protected by Default Rules. |
| | | CVE-2018-11525 | Wordpress Plugin Advanced Order Export for WooCommerce < 1.5.4 - CSV Injection | Advanced Order Export for WooCommerce plugin version 1.5.4 and before are affected by the vulnerability. Remote Command Execution using CSV Injection. This allows a public user to inject commands as a part of | Protected by Default Rules. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | form fields and when a user with higher privilege exports the form data in CSV opens the file on their machine, the command is executed. | |
| 5. | Cross Site Request Forgery | EDB-ID: 44938 | Ecessa ShieldLink SL175EHQ < 10.7.4 - Cross-Site Request Forgery (Add Superuser) | The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious website. | Protected by Custom Rules. |
| | | EDB-ID: 44937 | AsusWRT RT-AC750GF - Cross-Site Request Forgery (Change Admin Password) | AsusWRT RT-AC750GF - Cross-Site Request Forgery (Change Admin Password). | Protected by Custom Rules. |
| | | EDB-ID: 44936 | Ecessa WANWorx WVR-30 < 10.7.4 - Cross-Site Request Forgery (Add Superuser) | The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious website. | Protected by Custom Rules. |
| | | EDB-ID: 44933 | Intex Router N-150 - Cross-Site Request Forgery (Add Admin) | The firmware allows malicious request to be executed without verifying source of request. This leads to arbitrary execution with malicious request which will lead to the creation of a privileged user. | Protected by Custom Rules. |
| | | PS-148302 | Ecessa Edge EV150 10.7.4 - Cross-Site Request Forgery (Add Superuser) | The application interface allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious website. | Protected by Custom Rules. |