# Weekly Zero-Day Vulnerability Coverage Bulletin

*(27th May – 2nd June)*

Summary:

Total **7 Zero-Day Vulnerabilities** were discovered in **2 Categories** this week

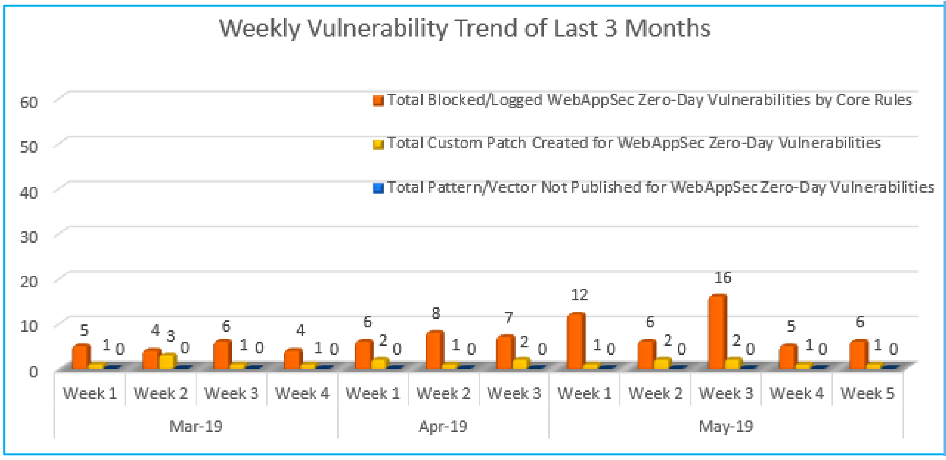
| | |
|---|---|
| **6**<br>Cross Site Scripting | **1**<br>Cross Site Request Forgery |

| | |
|---|---|
| Zero-Day Vulnerabilities Protected through Core Rules | 6 |
| 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

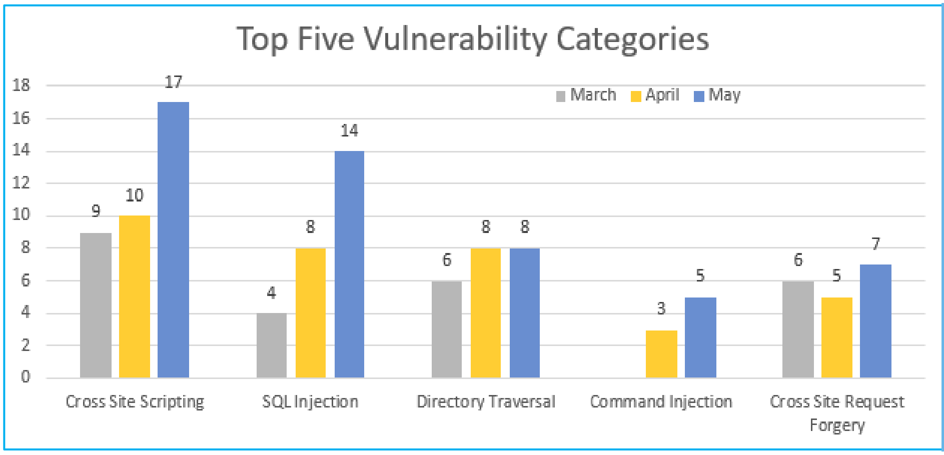
## Vulnerability Trend:



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

**83%** Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

**17%** 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 and SQL Injection vulnerabilities are discovered in May compared to other months.

No Command Injection vulnerabilities are found in March

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-2019-12362 | EmpireCMS 7.5.0 e/member/doaction.php Referer Header cross site scripting | A vulnerability was found in EmpireCMS 7.5.0. It has been rated as problematic. This issue affects some processing of the file *e/member/doaction.php*. The manipulation as part of a *Referer Header* 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 further attacks. | Protected by Default Rules. |
| | | CVE-2019-12345 | Kiboko Hostel Plugin up to 1.1.3 on WordPress cross site scripting | A vulnerability was found in Kiboko Hostel Plugin up to 1.1.3 on WordPress (Plugin Software) and classified as problematic. Affected by this issue is a part. 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 further attacks. | Protected by Default Rules. |
| | | CVE-2019-11226 | CMS Made Simple up to 2.2.10 m1_title Persistent cross site scripting [Disputed] | A vulnerability, which was classified as problematic, was found in CMS Made Simple up to 2.2.10 (Content Management System). Affected is a function. The manipulation of the argument m1_title with an unknown input leads to a cross site scripting vulnerability (Persistent). 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-2019-0221 | Apache Tomcat up to | A vulnerability was found in Apache Tomcat up to | |

| | | | | | |
|---|---|---|---|---|---|
| | | | 7.0.93/8.5.39/9.0.0.17 SSI printenv Command cross site scripting | 7.0.93/8.5.39/9.0.0.17 (Application Server Software). It has been declared as problematic. This vulnerability affects a code block of the component *SSI printenv Command 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 website. | |
| | | CVE-2019-12461 | Web Port 1.19.1 /log type cross site scripting | A vulnerability classified as problematic was found in Web Port 1.19.1. Affected by this vulnerability is the functionality of the file */log*. The manipulation of the argument type as part of a *Parameter* leads to a cross site scripting vulnerability. The CWE definition for the vulnerability is CWE-79. As an impact it is known to affect integrity. An attacker might be able to inject arbitrary html and script code into the website. This would alter the appearance. | |
| | | CVE-2019-12460 | Web Port 1.19.1 /access/setup type cross site scripting | A vulnerability classified as problematic has been found in Web Port 1.19.1. Affected is an unknown function of the file */access/setup*. The manipulation of the argument type as part of a *Parameter* leads to a cross site scripting vulnerability. CWE is classifying the issue as CWE-79. 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. | Protected by Default Rules. |
| 2. | Cross Site Request Forgery | CVE-2019-12361 | EmpireCMS 7.5.0 e/member/doaction.php from cross site request forgery | A vulnerability was found in EmpireCMS 7.5.0. It has been declared as problematic. This vulnerability affects a code block of the file | Protected by Custom Rules. |

| | | |
|---|---|---|
| | | *e/member/doaction.php*. The manipulation of the argument from as part of a *Parameter* 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 released in 05/27/2019. |