Weekly Zero-Day Vulnerability Coverage Bulletin

(25th March – 31st March)

Summary:

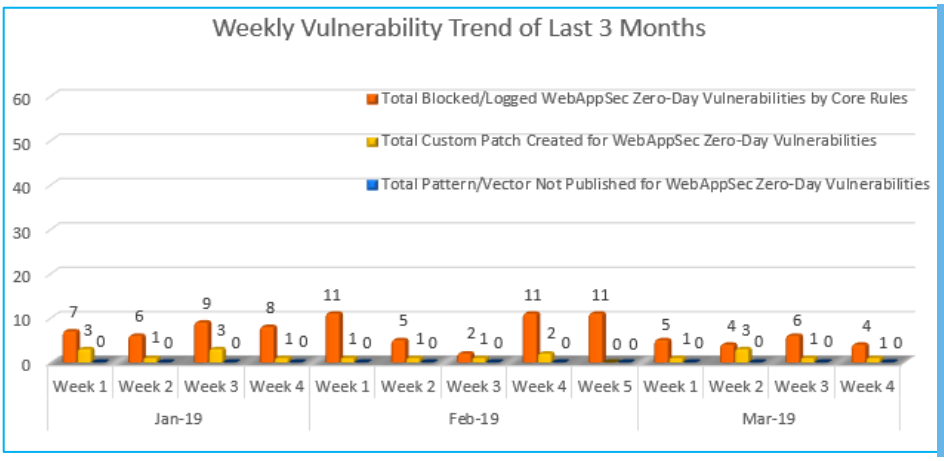
Total **5 Zero-Day Vulnerabilities** were discovered in **3 Categories** this week

3	1	1
Cross Site Scripting	Cross Site Request Forgery	Directory Traversal

Zero-Day Vulnerabilities Protected through Core Rules	4
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

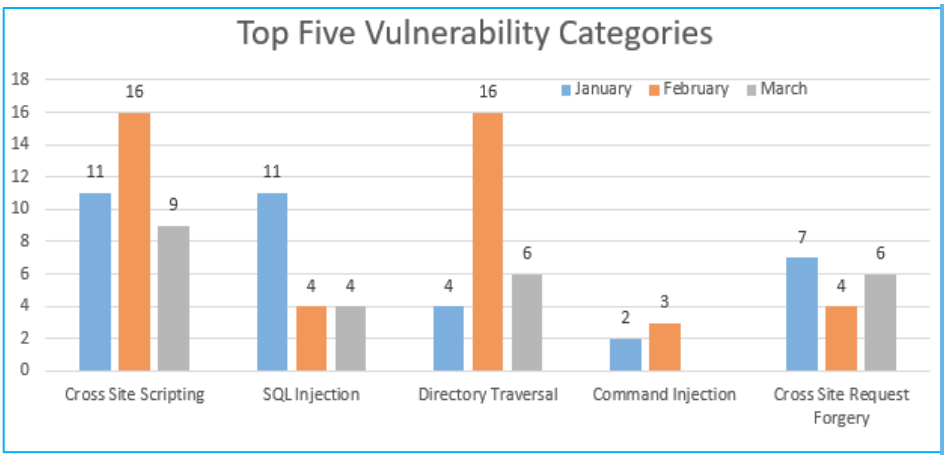
Vulnerability Trend:



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

84% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

16% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



From the graph, we infer that maximum Cross Site Scripting and Directory Traversal vulnerabilities were discovered in February compared to other months and categories so far.

Medium no. of SQL Injection and CSRF 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	NA	Unpatched Zero-Day Vulnerability in Social Warfare Plugin Exploited in the Wild	Vulnerable versions of the Social Warfare plugin are currently installed on more than 70,000 websites. The plugin was temporarily removed from the WordPress plugin store and was later added again after the zero-day flaw has been addressed. This flaw could allow remote unauthenticated attackers to execute JavaScript code stored in the database of WordPress websites that use vulnerable versions of the Social Warfare plugin.	Protected by Default Rules.
		SA-CORE-2019-004	Drupal core - Moderately critical - Cross Site Scripting - SA-CORE-2019-004	Under certain circumstances the File module/subsystem allows a malicious user to upload a file that can trigger a cross-site scripting (XSS) vulnerability.	Protected by Default Rules.
		CVE-2019-7646	CentOS Web Panel up to 0.9.8.763 Package Name add_package Persistent cross site scripting	A vulnerability was found in CentOS Web Panel up to 0.9.8.763. It has been classified as problematic. This affects code of the component *Package Name Handler*. The manipulation of the argument add_package as part of a *Parameter* 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 web site. This would alter	Protected by Default Rules.
2.	Directory Traversal	NA	Arbitrary Directory Deletion in WP-Fastest-Cache	In this detailed article, the researcher who found this issue mentions that it may affect close to 10,000 sites. Since $_SERVER['HTTP_REFERER'] may be controlled by the user, nothing prevents them from sending "http://vulnerable-site.com/../../../" in the Refer field to make the	Protected by Default Rules.

				whole website unreachable for anyone.	
3.	Cross Site Request Forgery	NA	WordPress 5.1.1 Patches Remote Code Execution Vulnerability	To exploit the vulnerability, an attacker would have to trick the site administrator to visit a domain to trigger a cross-site request forgery (CSRF) exploit in the background. The exploit leverages a series of logic flaws and sanitization errors to execute code and take over the target site, Simon Scannell of RIPS Technologies explains.	Protected by Custom Rules.