Weekly Zero-Day Vulnerability Coverage Bulletin

(1st April – 7th April)

Summary:

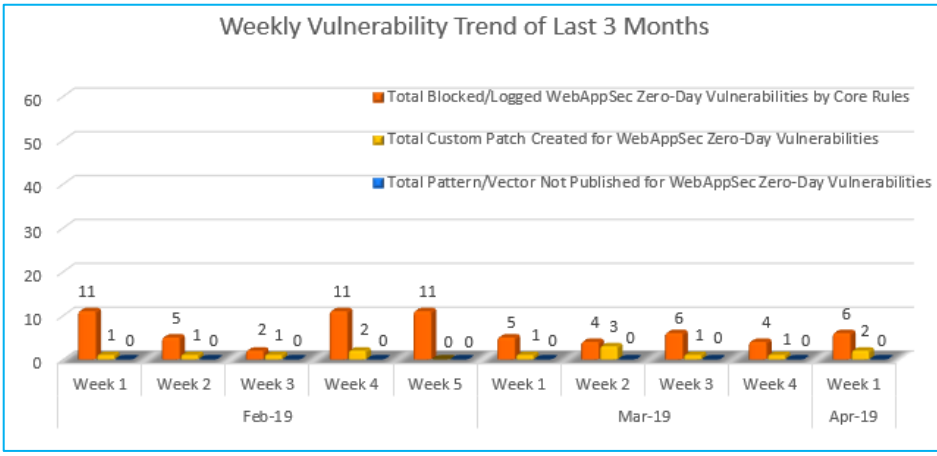
Total **8 Zero-Day Vulnerabilities** were discovered in **5 Categories** this week

1	2	2	1	2
Cross Site Scripting	SQL Injection	Directory Traversal	Command Injection	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	6
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

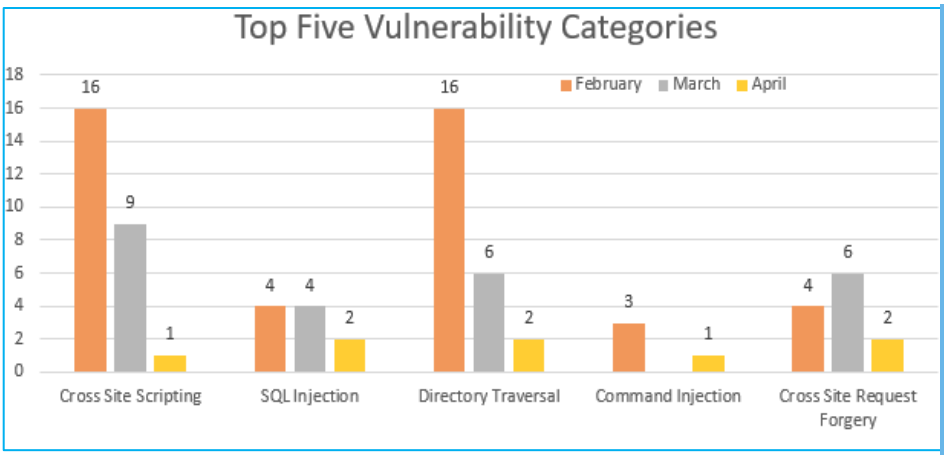
Vulnerability Trend:



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

81% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

19% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



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

Medium no. of SQL Injection & CSRF attacks are found in all 3 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	CVE-2019-5888	OverIT Geocall up to 6.3 cross site scripting	A vulnerability was found in OverIT Geocall up to 6.3. It has been declared as problematic. This vulnerability affects a code block. 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 would make it possible to initiate.	Protected by Default Rules.
2.	SQL Injection	CVE-2019-3792	Pivotal Concourse up to 5.0.0 API sql injection	A vulnerability has been found in Pivotal Concourse up to 5.0.0 and classified as critical. Affected by this vulnerability is a functionality of the component *API*. The manipulation with an unknown input lead to a 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. The weakness was released in 04/01/2019.	Protected by Default Rules.
		CVE-2019-10707	MKCMS 5.0 bplay.php play sql injection	A vulnerability classified as critical has been found in MKCMS 5.0. Affected is an unknown function of the file *bplay.php*. The manipulation of the argument play as part of a	Protected by Default Rules.

				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 to inject and/or alter existing SQL statements which would influence the database exchange. The weakness was disclosed in 04/02/2019.	
3.	Directory Traversal	CVE-2018-13299	Synology Calendar up to 2.2.2 File Upload filename directory traversal	A vulnerability was found in Synology Calendar up to 2.2.2 (Calendar Software). It has been declared as critical. Affected by this vulnerability is a code block of the component *File Upload*. The manipulation of the argument filename as part of a *Parameter* leads to a directory traversal vulnerability. The CWE definition for the vulnerability is CWE-22. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was disclosed 04/01/2019. It is possible to read the advisory.	Protected by Default Rules.
		CVE-2019-10009	South River Technologies Titan FTP Server 2019 Build 3505 /PreviewHandler .ashx path directory traversal	A vulnerability has been found in South River Technologies Titan FTP Server 2019 Build 3505 (File Transfer Software) and classified as critical. This vulnerability affects a functionality of the file */PreviewHandler.ashx*. The manipulation of the argument path with the input value \..\..\..\..\Python27\READ ME.txt leads to a directory traversal vulnerability. The CWE definition for the vulnerability is CWE-22. As an impact it is known to affect confidentiality,	Protected by Default Rules.

				integrity, and availability. The bug was discovered in 03/23/2019. The weakness was published on 03/26/2019 by Kevin.	
4.	Cross Site Request Forgery	CVE-2014-7198	OMERO up to 5.0.5 Web Interface cross site request forgery	A vulnerability was found in OMERO up to 5.0.5. It has been classified as problematic. Affected is code of the component *Web Interface*. The manipulation with an unknown input leads to a cross site request forgery vulnerability. CWE is classifying the issue as CWE-352. This is going to have an impact on integrity. An attacker might be able to force legitimate users to initiate unwanted actions within the web application. The weakness was presented in 04/01/2019. This vulnerability is traded as CVE-2014-7198.	Protected by Custom Rules.
		CVE-2018-1622	IBM 2.2.1 cross site request forgery [CVE-2018-1622]	A vulnerability was found in IBM Security Privileged Identity Manager Virtual Appliance 2.2.1. It has been classified as problematic. Affected is code. The manipulation with an unknown input leads to a cross site request forgery vulnerability. CWE is classifying the issue as CWE-352. This is going to have an impact on integrity. An attacker might be able to force legitimate users to initiate unwanted actions within the web application. The weakness was disclosed in 04/02/2019. The advisory is available at exchange.xforce.ibmcloud .com.	Protected by Custom Rules.
5.	Command Injection	CVE-2019-1010260	ktlint up to 0.29.x Code Execution [CVE-2019-1010260]	A vulnerability was found in ktlint up to 0.29.x. It has been classified as critical. This affects code. The	Protected by Default Rules.

		manipulation with an unknown input leads to a privilege escalation vulnerability (Code Execution). CWE is classifying the issue as CWE-269. This is going to have an impact on confidentiality, integrity, and availability. The weakness was released in 04/02/2019. This vulnerability is uniquely identified as CVE-2019-1010260 since 03/20/2019. The technical details are unknown, and an exploit is not publicly available. Upgrading the version.