Weekly Zero-Day Vulnerability Coverage Bulletin

(8th April – 14th April)

Summary:

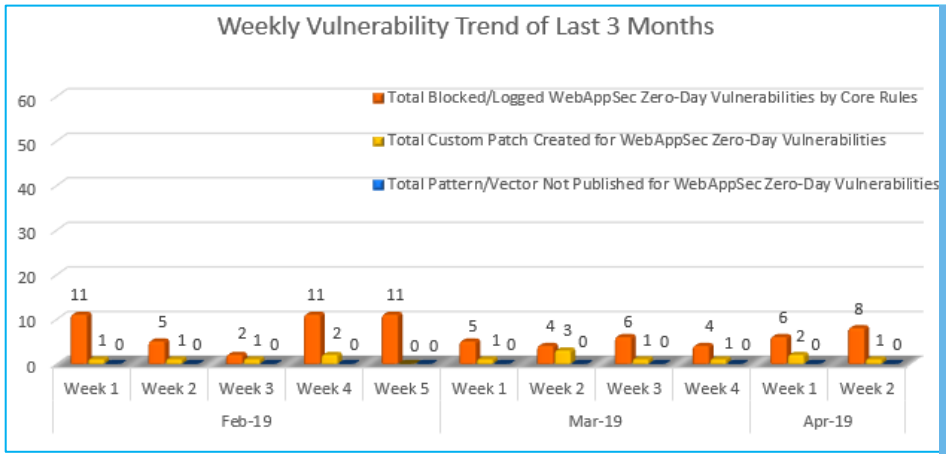
Total **9 Zero-Day Vulnerabilities** were discovered in **5 Categories** previous week

3	1	2	1	2
Cross Site Scripting	SQL Injection	Directory Traversal	Cross Site Request Forgery	Command Injection

Zero-Day Vulnerabilities Protected through Core Rules	8
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

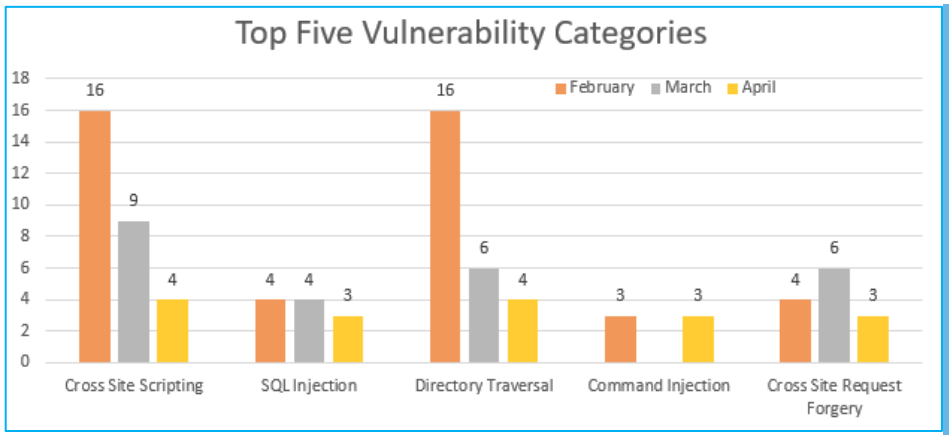
Vulnerability Trend:



Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a quarter.

82% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

18% 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 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	CVE-2019-9844	Khan Academy simple-markdown up to 0.4.3 URI cross site scripting	A vulnerability was found in Khan Academy simple-markdown up to 0.4.3. It has been declared as problematic. Affected by this vulnerability is a code block of the component *URI 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.	Protected by Default Rules.
		CVE-2019-11004	Materialize up to 1.0.0 Toast cross site scripting	A vulnerability was found in Materialize up to 1.0.0. It has been declared as problematic. Affected by this vulnerability is a code block of the component *Toast*. The manipulation with an unknown input 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.	Protected by Default Rules.
		NA	Yuzo Related Posts Zero-Day Vulnerability Exploited in the Wild	The Yuzo Related Posts plugin, which is installed on over 60,000 websites, was removed from the WordPress.org plugin directory on March 30, 2019 after an unpatched vulnerability was publicly, and irresponsibly, disclosed by a security researcher that same day. The vulnerability, which allows stored cross-site	Protected by Default Rules.

				scripting (XSS), is now being exploited in the wild. These attacks appear to be linked to the same threat actor who targeted the recent Social Warfare and Easy WP SMTP vulnerabilities.	
2.	SQL Injection	CVE-2019-7139	Magento up to 1.9.4.0/1.14.4.0/ 2.2.7/2.3.0 sql injection [CVE-2019-7139]	A vulnerability has been found in Magento up to 1.9.4.0/1.14.4.0/2.2.7/2.3.0 and classified as critical. Affected by this vulnerability is a functionality. 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 shared 04/10/2019.	Protected by Default Rules.
3.	Directory Traversal	CVE-2019-10632	ZyXEL NAS 326 up to 5.21 File Browser directory traversal	A vulnerability, which was classified as critical, was found in ZyXEL NAS 326 up to 5.21. Affected is a function of the component *File Browser*. The manipulation with an unknown input leads to a directory traversal vulnerability. CWE is classifying the issue as CWE-22. This is going to have an impact on integrity, and availability. The weakness was presented 04/09/2019. This vulnerability is traded as CVE-2019-10632 since 03/29/2019. A single authentication is necessary for exploitation. The technical details are unknown.	Protected by Default Rules.

		CVE-2018-14918	LOYTEC LGATE-902 up to 6.4.1 /webui/file_guest path directory traversal	A vulnerability was found in LOYTEC LGATE-902 up to 6.4.1 and classified as critical. Affected by this issue is a part of the file */webui/file_guest*. The manipulation of the argument path with the input value /var/www/documentation/../../../../../etc/passwd leads to a directory traversal vulnerability. Using CWE to declare the problem leads to CWE-22. Impacted is integrity, and availability. The weakness was released in 04/07/2019 as *Loytec LGATE-902: Multiple Vulnerabilities (XSS, Path traversal and File Deletion) * as confirmed mailinglist post (Full-Disclosure).	Protected by Default Rules.
4.	Cross Site Request Forgery	CVE-2019-11078	MKCMS 5.0 ucenter/userinfo.php cross site request forgery	A vulnerability was found in MKCMS 5.0. It has been rated as problematic. This issue affects some processing of the file *ucenter/userinfo.php*. The manipulation with an unknown input leads to a cross site request forgery vulnerability. Using CWE to declare the problem leads to CWE-352. Impacted is integrity. An attacker might be able force legitimate users to initiate unwanted actions within the web application. The weakness was presented in 04/11/2019. The identification of this vulnerability is CVE-2019-11078 since 04/10/2019.	Protected by Custom Rules.
5.	Command Injection	CVE-2018-17305	UiPath Orchestrator up to 2018.2.4 Remote Code Execution [CVE-2018-17305]	A vulnerability classified as critical has been found in UiPath Orchestrator up to 2018.2.4. Affected is an unknown function. The manipulation with an unknown input leads to a	Protected by Default Rules.

			privilege escalation vulnerability (Code Execution). CWE is classifying the issue as CWE-264. This is going to have an impact on confidentiality, integrity, and availability. The weakness was shared in 04/11/2019. The advisory is shared for download at uipath.com. This vulnerability is traded as CVE-2018-17305 since 09/21/2018. The exploitability is told to be easy.	
	CVE-2018-1335	Exploiting CVE-2018-1335: Command Injection in Apache Tika	This post is a walk-through of steps taken to go from an undisclosed CVE for a command injection vulnerability in the Apache tika-server to a complete exploit. The CVE is https://nvd.nist.gov/vuln/detail/CVE-2018-1335. Since Apache Tika is open source, I was able to take some basic information from the CVE and identify the actual issue by analyzing the Apache Tika code. Although a command injection vulnerability is typically straightforward, as you will see in this post there were some hurdles to overcome to achieve full remote code or command execution. This was due to the way Java handles executing operating system commands andalso some intricacies of the Apache Tika code itself. In the end, it was still possible to get around these blockers using the Windows Script Host (Cscript.exe).	Protected by Default Rules.