Weekly Zero-Day Vulnerability Coverage Bulletin

April 20

Summary:

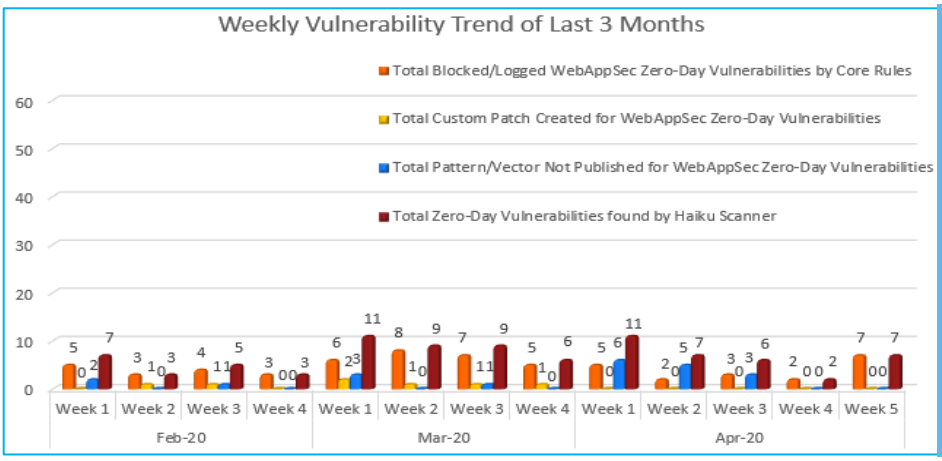
Total **25 Zero-Day Vulnerabilities** were discovered in **11 Categories** this month

8	4	1	1	2	1	2	1	1	3	1
Cross Site Scripting	SQL Injection	Deserialization	Open Redirect	Privilege Escalation	Server Side Request Forgery	Directory Traversal	Botnet attack	Local File Inclusion	Remote Code Execution	Command Injection

Zero-Day Vulnerabilities Protected through Core Rules	17
Zero-Day Vulnerabilities Protected through Custom Rules	6*
Zero-Day Vulnerabilities for which protection cannot be determined	2**
Zero-Day Vulnerabilities found by Indusface WAS	21

* 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:

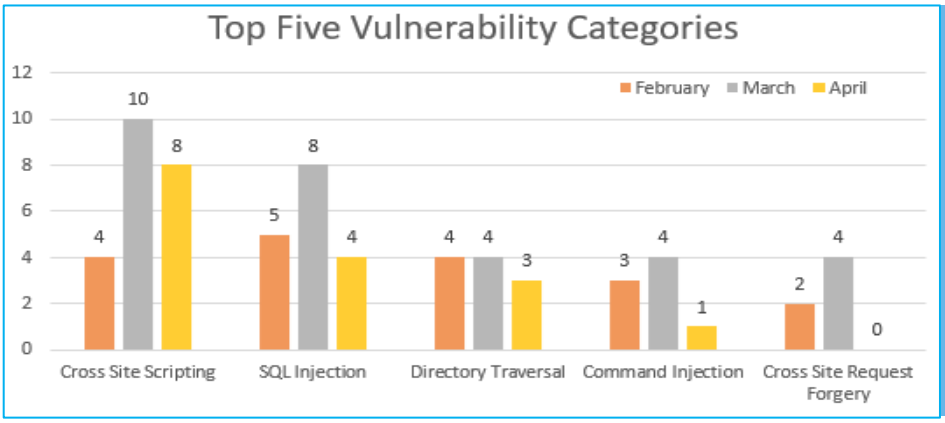


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

72% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

22% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

83% Of Zero-Day Vulnerabilities were reported by Haiku Scanner in last quarter



From the graph, we infer that maximum Cross Site Scripting vulnerabilities are discovered in March compared to other months.

Zero no. of Cross Site Request Forgery attacks are discovered in April.

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	Indusface WAS Coverage
1.	Cross Site Scripting	CVE-2020-1949	Sling CMS up to 0.15.x Administrative Console Reflected cross site scripting	A vulnerability classified as problematic has been found in Sling CMS up to 0.15.x (Content Management System). This affects an unknown code of the component Administrative Console. Upgrading to version 0.16.0 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2020-2175	FitNesse Plugin up to 1.31 on Jenkins Report Stored cross site scripting	A vulnerability was found in FitNesse Plugin up to 1.31 on Jenkins (Jenkins Plugin). It has been classified as problematic. Affected is some unknown processing of the component Report Handler. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		2019-17230	OneTone Vulnerability Leads to JavaScript Cookie Hijacking	Due to missing capability checks and security nonces, an unauthenticated attacker can use the theme options import feature to inject JavaScript code into all pages and posts of the website.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		NA	Cross Site Scripting vulnerability in datepicker plugin	The Contact Form 7 Datepicker plugin allows users to add a datepicker to forms generated by Contact Form 7. The plugin also allows the users to modify settings for these datepickers. “In order to process these settings, it registered an AJAX action calling a function that failed to include a capability check or a nonce check. As such, it was possible for a logged-in attacker with minimal permissions, such as a subscriber, to send a crafted	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.

		request containing malicious JavaScript which would be stored in the plugin's settings." continues the analysis. "The next time an authorized user created or modified a contact form, the stored JavaScript would be executed in their browser, which could be used to steal an administrator's session or even create malicious administrative users."		
CVE-2020-7642	lazysizes up to 5.2.0 video-embed Plugin Attribute cross site scripting	A vulnerability was found in lazysizes up to 5.2.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component video-embed Plugin. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
CVE-2020-12071	Anchor 0.12.7 Content cross site scripting	A vulnerability classified as problematic was found in Anchor 0.12.7. This vulnerability affects an unknown function of the component Content Handler. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
CVE-2019-20789	Croogo up to 3.0.6 admin/menus/ menus title cross site scripting	A vulnerability was found in Croogo up to 3.0.6 and classified as problematic. This issue affects some unknown functionality of the file admin/menus/menus. Upgrading to version 3.0.7 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
CVE-2020-12077	Critical Vulnerabilities Patched in MapPress Maps Plugin	A vulnerability was found in mappress-google-maps-for-wordpress Plugin up to 2.53.8 on WordPress (WordPress Plugin). It has been classified as critical. This affects an unknown	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.

				code block of the component Ajax Handler. The manipulation with an unknown input leads to a privilege escalation vulnerability. CWE is classifying the issue as CWE-269. This is going to have an impact on confidentiality, integrity, and availability. The weakness was disclosed on 04/23/2020. This vulnerability is uniquely identified as CVE-2020-12077 since 04/23/2020. Neither technical details nor an exploit is publicly available.		
2.	SQL Injection	CVE-2020-10617	Advantech WebAccess/NMS up to 3.0.1 sql injection [CVE-2020-10617]	A vulnerability classified as critical was found in Advantech WebAccess and NMS up to 3.0.1 (SCADA Software). This vulnerability affects an unknown code. Upgrading to version 3.0.2 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
		NA	Duplicated Vulnerabilities in WordPress Plugins	The original code was very simple. Comprising little more than 100 lines of code and well commented, it had one major issue: A SQL injection into a serialized table. A few years later, this vulnerable code snippet was then converted to three plugins: Duplicate Page and WP Post Page Clone in 2016, and Duplicate Page and Post in 2017. All of these plugins contained the vulnerability from the original post which ironically was updated to fix the vulnerability in mid-2016, barely a week after the first plugin copied it and before the two others were even released.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
		CVE-2020-12429	Online Course Registration 2.0 change-password.php sql injection	A vulnerability was found in Online Course Registration 2.0. It has been classified as critical. Affected is an unknown code of the file admin/change-password.php. There is no	Protected by Default Rules.	Detected by scanner as SQL Injection attack.

				information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.		
		CVE-2020-12461	php-fusion 9.03.50 maincore.php sort_order sql injection	A vulnerability was found in php-fusion 9.03.50 (Content Management System) and classified as critical. This issue affects an unknown code block of the file maincore.php. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
3.	Command Injection	CVE-2020-7609	node-rules up to 4.x fromJSON() command injection	A vulnerability has been found in node-rules up to 4.x and classified as critical. This vulnerability affects the function fromJSON(). Upgrading to version 5.0.0 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Command Injection attack.
4.	Remote Code Execution	CVE-2020-4427	RCE Exploit Released for IBM Data Risk Manager, No Patch Available	A vulnerability, which was classified as critical, has been found in IBM Data Risk Manager up to 2.0.6. This issue affects an unknown code block of the component SAML Authentication. The manipulation as part of a HTTP Request leads to a weak authentication vulnerability. Using CWE to declare the problem leads to CWE-287. Impacted is confidentiality, integrity, and availability. The weakness was released on 05/07/2020. The advisory is shared at exchange.xforce.ibmcloud.com. The identification of this vulnerability is CVE-2020-4427 since 12/30/2019. The exploitation is known to be difficult. The attack may be initiated remotely. No form of authentication is needed for a successful exploitation. Neither technical details nor	Protected by Custom Rules.	NA

		an exploit is publicly available.		
CVE-2020-4428	RCE Exploit Released for IBM Data Risk Manager, No Patch Available	A vulnerability, which was classified as critical, was found in IBM Data Risk Manager up to 2.0.6. Affected is some unknown processing. The manipulation as part of a Command leads to a privilege escalation vulnerability. CWE is classifying the issue as CWE-269. This is going to have an impact on confidentiality, integrity, and availability. The weakness was disclosed on 05/07/2020. The advisory is available at exchange.xforce.ibmcloud.com. This vulnerability is traded as CVE-2020-4428 since 12/30/2019. It is possible to launch the attack remotely. A single authentication is required for exploitation. The technical details are unknown, and an exploit is not available.	Protected by Custom Rules.	NA
CVE-2020-4430	RCE Exploit Released for IBM Data Risk Manager, No Patch Available	A vulnerability was found in IBM Data Risk Manager up to 2.0.6 and classified as problematic. Affected by this issue is an unknown functionality. The manipulation as part of a Request leads to a directory traversal vulnerability. Using CWE to declare the problem leads to CWE-22. Impacted is confidentiality. The weakness was shared in 05/07/2020. The advisory is shared for download at exchange.xforce.ibmcloud.com. This vulnerability is handled as CVE-2020-4430 since 12/30/2019. The attack may be launched remotely. A single authentication is needed for exploitation. There are neither technical details nor an exploit publicly available.	Protected by Default Rules.	Detected by scanner as Remote Code Execution attack.

5.	Directory Traversal	CVE-2020-10696	Buildah up to 1.14.4 Container Image directory traversal	A vulnerability was found in Buildah up to 1.14.4. It has been rated as critical. This issue affects some unknown processing of the component Container Image Handler. Upgrading to version 1.14.5 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.
		CVE-2020-12102	Tiny File Manager 2.4.1 Ajax directory traversal	A vulnerability, which was classified as problematic, has been found in Tiny File Manager 2.4.1. Affected by this issue is an unknown function of the component Ajax Handler. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.
6.	Deserialization	CVE-2020-2833	Oracle WebLogic Deserialization Vulnerability Exploited in the Wild	A vulnerability classified as very critical was found in Oracle WebLogic Server 10.3.6.0.0/12.1.3.0.0/12.2.1.3.0/12.2.1.4.0 (Application Server Software). This vulnerability affects an unknown part of the component Core. As an impact it is known to affect confidentiality, integrity, and availability. CVE summarizes: Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/	Protected by Custom Rules.	Detected by scanner as Deserialization attack.

				UI:N/S:U/C:H/I:H/A:H). The weakness was presented in 04/15/2020 as Oracle Critical Patch Update Advisory - April 2020 as confirmed advisory (Website). The advisory is available at oracle.com. This vulnerability was named as CVE-2020-2883. The attack can be initiated remotely. No form of authentication is required for a successful exploitation. The technical details are unknown, and an exploit is not available.		
7.	Privilege Escalation	CVE-2020-11651	SaltStack Salt critical bugs allow data center, cloud server hijacking as root	A vulnerability was found in SaltStack Salt. It has been classified as critical. Affected is the function ClearFuncs. The manipulation with an unknown input leads to a privilege escalation vulnerability. CWE is classifying the issue as CWE-269. This is going to have an impact on confidentiality, integrity, and availability. The weakness was shared on 04/30/2020. The advisory is shared for download at lists.opensuse.org. This vulnerability is traded as CVE-2020-11651 since 04/08/2020. It is possible to launch the attack remotely. There are known technical details, but no exploit is available.	Protected by Custom Rules.	Detected by scanner as Privilege Escalation attack.
		CVE-2020-12720	An Undisclosed Critical Vulnerability Affect vBulletin Forums — Patch Now	A vulnerability classified as critical was found in vBulletin up to 5.5.6/5.6.0/5.6.1 (Forum Software). This vulnerability affects an unknown code of the component Access Control. The manipulation with an unknown input leads to a privilege escalation vulnerability. The CWE definition for the vulnerability is CWE-863. As an impact it is known to	NA	Detected by scanner as Privilege Escalation attack.

				affect confidentiality, integrity, and availability. The weakness was published 05/08/2020. This vulnerability was named as CVE-2020-12720 since 05/07/2020. The exploitation appears to be easy. The attack can be initiated remotely. No form of authentication is required for a successful exploitation. There are neither technical details nor an exploit publicly available.		
8.	Local File Inclusion	CVE-2020-11652	SaltStack Salt critical bugs allow data center, cloud server hijacking as root	A vulnerability was found in SaltStack Salt. It has been classified as critical. Affected is the function ClearFuncs. The manipulation with an unknown input leads to a privilege escalation vulnerability. CWE is classifying the issue as CWE-269. This is going to have an impact on confidentiality, integrity, and availability. The weakness was shared on 04/30/2020. The advisory is shared for download at lists.opensuse.org. This vulnerability is traded as CVE-2020-11651 since 04/08/2020. It is possible to launch the attack remotely. There are known technical details, but no exploit is available.	Protected by Default Rules.	Detected by scanner as Local File Inclusion attack.
9.	Server Side Request Forgery	NA	Multiple SSRF on Vanilla Moodle Installations	The vulnerability resides on image parsing from an arbitrary URL (when an user choose to retrieve an image using the URL, as mentioned before). If you request an HTML page, Moodle will fetch all '<img>' tags inside it and ask you to choose which image you want to download. It extracts the src attribute for all image tags in the page and directly downloads the image,	Protected by Custom Rules.	NA

				without further checks. That means that if we request the image from a server we control, we can request an HTML page with an arbitrary URL inside an image tag and Moodle will perform this arbitrary request for us.		
10.	Botnet attack	NA	Hacker Group Backdoors Thousands of Microsoft SQL Servers Daily	Hackers have forced thousands of vulnerable Microsoft SQL Servers (MSSQL) daily to install crypto miners and Remote Access Trojans (RATs) since May 2018. This attack campaign still actively infects between 2000 and 3000 MSSQL servers daily and it has been nicknamed Vollgar because the cryptomining scripts it deploys on compromised MSSQL will exploit the cryptocurrency Monero (XMR) and Vollar (VDS).Its operators use brute force to rape targeted machines and will then deploy backdoors that remove several malicious modules, including remote access tools (RAT) and crypto miners.	Protected by Custom Rules.	NA
11.	Open Redirect	NA	Thousands of WordPress Sites Hacked to Fuel Scam Campaign - "CP Contact Form with PayPal" and the "Simple Fields" plugins	When exploited, the vulnerabilities allow the attackers to inject JavaScript that loads scripts from admarketlocation[.]com and gotosecond2[.]com directly into the site's theme	NA	Detected by scanner as Open Redirect attack.