Weekly Zero-Day Vulnerability Coverage Bulletin

May 20

Summary:

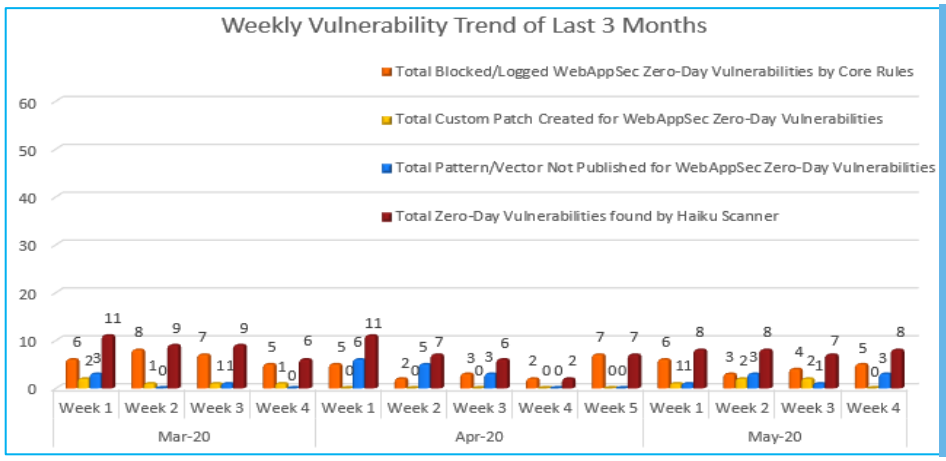
Total **29 Zero-Day Vulnerabilities** were discovered in **7 Categories** this month

8	2	5	5	2	4	3
Cross Site Scripting	SQL Injection	Command Injection	CSRF	Remote Code Execution	Directory Traversal	Open Redirect

Zero-Day Vulnerabilities Protected through Core Rules	19
Zero-Day Vulnerabilities Protected through Custom Rules	6*
Zero-Day Vulnerabilities for which protection cannot be determined	4**
Zero-Day Vulnerabilities found by Indusface WAS	25

* 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:

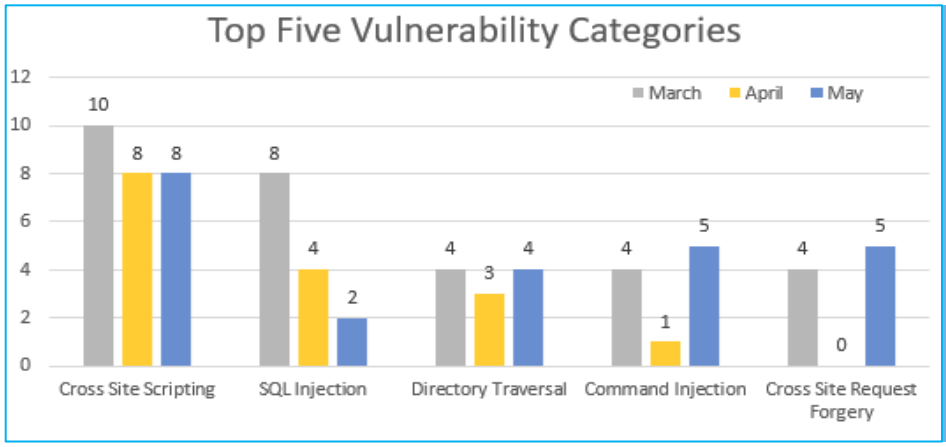


Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

71% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

20% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

87% 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 Scripting 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-2020-5575	Movable Type cross site scripting	A vulnerability classified as problematic was found in piechart-panel up to 1.4.x on Grafana. Affected by this vulnerability is an unknown function. Upgrading to version 1.5.0 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2017-7391	magmi 0.7.22 ajax_gettime.php prefix cross site scripting	A vulnerability classified as problematic has been found in magmi 0.7.22. This affects an unknown code block of the file magmi-git-master/magmi/web/ajax_gettime.php. The manipulation of the argument prefix with an unknown input 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 web site. This would alter the appearance and would make it possible to initiate further attacks against site visitors. The bug was discovered on 03/31/2017. The weakness was presented on 04/01/2017 by Venustech with Adlab of Venustech (GitHub Repository). The advisory is shared at github.com. This vulnerability is uniquely identified as CVE-2017-7391 since 03/31/2017. It is possible to initiate the attack remotely. No form of authentication is needed for exploitation.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		NA	Large-scale attack tries to steal configuration	The goal of the attack was to use old exploits to download or export wp-config.php files from unpatched websites, extract	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.

	files from WordPress sites	database credentials, and then use the usernames and passwords to take over databases. During the first campaign, the threat actor used a batch of XSS (cross-site scripting) vulnerabilities and attempted to insert new admin users and backdoors on targeted sites. The first campaign was also similarly massive in scale, as the group's XSS attacks outweighed all the XSS attacks carried out by other groups combined.		
CVE-2020-8034	Gollem up to 3.0.12 dir Reflected cross site scripting	A vulnerability classified as problematic has been found in Movable Type the affected version unknown). This affects some unknown functionality. 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-2020-13240	Dolibarr 11.0.4 DMS/ECM cross site scripting	A vulnerability was found in Gollem up to 3.0.12and classified as problematic. This issue affects an unknown part. Upgrading to version 3.0.13 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
CVE-2019-20803	Gila CMS up to 1.11.5 postcategory id cross site scripting	A vulnerability was found in Dolibarr 11.0.4 (Enterprise Resource Planning Software) and classified as problematic. This issue affects an unknown functionality of the component DMS/ECM. 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-2020-13429	piechart-panel up to 1.4.x on Grafana Values cross site scripting	A vulnerability, which was classified as problematic, was found in Gila CMS up to 1.11.5 Content Management System). This affects an unknown code of	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.

				the file admin/content/postcategory. Upgrading to version 1.11.6 eliminates this vulnerability.		
		CVE-2020-13660	CMS Made Simple up to 2.2.14 File Picker Profile Name cross site scripting	A vulnerability classified as problematic was found piechart-panel up to 1.4.x on Grafana. Affected by this vulnerability is an unknown function. Upgrading to version 1.5.0 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
2.	SQL Injection	CVE-2020-6010	LearnPress Plugin 3.2.6.7 on WordPress sql injection	A vulnerability classified as critical has been found in LearnPress Plugin 3.2.6.7 on WordPress (WordPress Plugin). Affected is some unknown functionality. 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.
		CVE-2020-6009	LearnDash Plugin 3.1.6 on WordPress sql injection	A vulnerability was found in LearnDash Plugin 3.1.6 on WordPress (WordPress Plugin). It has been declared as critical. This vulnerability affects an unknown code. 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-2020-5332	RSA Archer up to 6.7 P2 command injection	A vulnerability classified as critical was found in RSA Archer up to 6.7 P2 (Risk Management System). Affected by this vulnerability is an unknown functionality. Applying the patch 6.7 P3 can eliminate this problem.	Protected by Default Rules.	Detected by scanner as Command Injection attack.
		CVE -2020-12675	Alert Logic Threat Research Team Identifies New Vulnerability: CVE-2020-12675 in MapPress	A vulnerability classified as critical has been found in mappress-google-maps-for-wordpress Plugin up to 2.54.5 on WordPress (WordPress Plugin). Affected is an unknown code of the component	Protected by Default Rules.	Detected by scanner as Command Injection attack.

	Plugin for WordPress	Capability Check. The manipulation with an unknown input leads to a privilege escalation vulnerability (Code Execution). CWE is classifying the issue as CWE-434. This is going to have an impact on confidentiality, integrity, and availability. The weakness was published on 05/29/2020. This vulnerability is traded as CVE-2020-12675 since 05/06/2020. The exploitability is told to be easy. It is possible to launch the attack remotely. The successful exploitation requires a single authentication. There are neither technical details nor an exploit publicly available.		
CVE-2020-3280	Cisco Unified Contact Center Express Java Remote Management Interface Serialized Java Object privilege escalation	A vulnerability was found in Cisco Unified Contact Center Express version unknown). It has been classified as critical. Affected is an unknown code of the component Java Remote Management Interface. Upgrading eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Command Injection attack.
CVE-2020-12675	mappress-google-maps-for-wordpress Plugin up to 2.54.5 on WordPress Capability Check Remote Code Execution	A vulnerability classified as critical has been found in mappress-google-maps-for-wordpress Plugin up to 2.54.5 on WordPress WordPress Plugin). Affected is an unknown code of the component Capability Check. Upgrading to version 2.54.6 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Command Injection attack.
CVE-2020-3956	VMware Cloud Director up to 9.1.0.3/9.5.0.5/ 9.7. 0.4/10.0.0.1 Remote Code Execution	A vulnerability classified as critical was found in VMware Cloud Director up to 9.1.0.3/9.5.0.5/9.7.0.4/10.0. 0.1 (Cloud Software). This vulnerability affects some unknown processing. The manipulation with an unknown input leads to a privilege escalation	Protected by Default Rules.	Detected by scanner as Command Injection attack.

				vulnerability (Code Execution). The CWE definition for the vulnerability is CWE-269. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was released on 05/20/2020. This vulnerability was named CVE-2020-3956 since 12/30/2019. The successful exploitation needs a single authentication. There are neither technical details nor any exploit publicly available.		
4.	Remote Code Execution	CVE-2020-0796	Microsoft Windows 10 1903/10 1909/Server 1903/Server 1909 SMBv3 Server Message Block Code Execution memory corruption	A vulnerability, which was classified as very critical, was found in Microsoft Windows 10 1903/10 1909/Server 1903/Server 1909 (Operating System). Affected is an unknown part of the component SMBv3. The manipulation as part of a Server Message Block leads to a memory corruption vulnerability (Code Execution). CWE is classifying the issue as CWE-20. This is going to have an impact on confidentiality, integrity, and availability. CVE summarizes: A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability'. The weakness was disclosed on 03/12/2020 as confirmed security update guide (Website). The advisory is shared for download at portal.msrc.microsoft.com. The public release has been coordinated in cooperation with the vendor. This vulnerability is traded as CVE-2020-0796 since 11/04/2019. It is possible to	Protected by Custom Rules.	Detected by scanner as Remote Code Execution attack.

				launch the attack remotely. The exploitation does not require any form of authentication. Technical details are unknown, but a private exploit is available.		
		CVE-2020-4448	IBM WebSphere Application Server 7.0/8.0/8.5/9.0 Network Deployment Serialized Object Code Execution memory corruption	A vulnerability was found in IBM WebSphere Application Server 7.0/8.0/8.5/9.0 (Application Server Software) and classified as critical. Affected by this issue is an unknown part of the component Network Deployment. The manipulation as part of a Serialized Object leads to a memory corruption vulnerability (Code Execution). Using CWE to declare the problem leads to CWE-94. Impacted is confidentiality, integrity, and availability. The weakness was released on 06/05/2020. The advisory is shared for download at exchange.xforce.ibmcloud.com. This vulnerability is handled as CVE-2020-4448 since 12/30/2019. The attack may be launched remotely. No form of authentication is required for exploitation. There are neither technical details nor any exploit publicly available.	NA	Detected by scanner as Remote Code Execution attack.
5.	Open Redirect	CVE-2020-13486	Knock Knock Plugin up to 1.2.7 on Craft CMS Open Redirect	A vulnerability was found in Knock Knock Plugin up to 1.2.7 on Craft CMS and classified as critical. Affected by this issue is some unknown processing. Upgrading to version 1.2.8 eliminates this vulnerability.	NA	Detected by scanner as Open Redirect attack.
		CVE-2020-5337	RSA Archer up to 6.7 Open Redirect	A vulnerability was found in RSA Archer up to 6.7 (Risk Management System). It has been classified as critical. Affected is some unknown processing. Applying the patch 6.7 P1 can eliminate this problem.	NA	Detected by scanner as Open Redirect attack.

		CVE-2020-1059	Microsoft Edge Open Redirect	A vulnerability was found in Microsoft Edge (Web Browser) (version unknown). It has been classified as critical. Affected is some unknown functionality. Applying a patch can eliminate this problem. A possible mitigation has been published immediately after the disclosure of the vulnerability.	NA	Detected by scanner as Open Redirect attack.
6.	Directory Traversal	CVE-2020-7652	snyk-broker up to 4.79.x directory traversal	A vulnerability has been found in snyk-broker up to 4.79.x and classified as problematic. This vulnerability affects an unknown code block. Upgrading to version 4.80.0 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.
		CVE-2020-6008	LifterLMS Plugin 3.37.15 on WordPress Code Execution directory traversal	A vulnerability, which was classified as critical, was found in LifterLMS Plugin 3.37.15 on WordPress (WordPress Plugin). This affects an unknown function. 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.
		CVE-2020-9484	CSA | SingCERT | Critical Vulnerability in Apache Tomcat	A vulnerability classified as critical has been found in Apache Tomcat up to 7.0.103/8.5.54/9.0.34/10.0.0-M4 (Application Server Software). Affected is an unknown function. The manipulation with an unknown input lead to a privilege escalation vulnerability (Deserialization). CWE is classifying the issue as CWE-502. This is going to have an impact on confidentiality, integrity, and availability. The weakness was shared on 05/20/2020. This vulnerability is traded as CVE-2020-9484 since 03/01/2020. There are	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.

				neither technical details nor an exploit publicly available.		
		CVE-2020-1631	Juniper Junos HTTP Service command injection directory traversal	A vulnerability was found in Juniper Junos (Router Operating System) (affected version unknown). It has been declared as critical. Affected by this vulnerability is some unknown processing of the component HTTP Service. Upgrading eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.
7.	Cross Site Request Forgery	CVE-2020-12626	RoundCube Webmail up to 1.4.3 cross site request forgery	A vulnerability classified as problematic has been found in RoundCube Webmail up to 1.4.3 (Mail Client Software). Affected is some unknown processing. Upgrading to version 1.4.4 eliminates this vulnerability.	Protected by Custom Rules.	Detected by scanner as Cross Site Request Forgery attack.
		CVE-2020-5576	Movable Type cross site request forgery	A vulnerability classified as problematic was found in Movable Type (the affected version is unknown). This vulnerability affects an unknown part. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Custom Rules.	NA
		CVE-2019-20390	Subrion CMS 4.2.1 read.json cross site request forgery	A vulnerability classified as problematic was found in Subrion CMS 4.2.1 (Content Management System). This vulnerability affects an unknown code block of the file panel/uploads/read.json?cmd=rm. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Custom Rules.	NA
		NA	Two security flaws in the PageLayer WordPress plugin can be exploited to potentially wipe the contents or	PageLayer is a WordPress page builder plugin, it is very easy to use and has over 200,000 active installations according to numbers available on its WordPress plugins repository entry. One	Protected by Custom Rules.	NA

	take over WordPress sites.	vulnerability could allow an authenticated user with subscriber-level and above permissions to update and modify post. The second vulnerability could allow attackers to forge a request on behalf of a site's administrator to change the plugin settings allowing to inject malicious JavaScript.		
CVE-2020-13412	Aviatrix Controller prior 5.4.1204 Web Interface cross site request forgery	A vulnerability classified as problematic was found in Aviatrix Controller. This vulnerability affects an unknown code block of the component Web Interface. Upgrading to version 5.4.1204 eliminates this vulnerability.	Protected by Custom Rules.	NA