Weekly Zero-Day Vulnerability Coverage Bulletin

March 2020

Summary:

Total **33 Zero-Day Vulnerabilities** were discovered in **8 Categories** this month

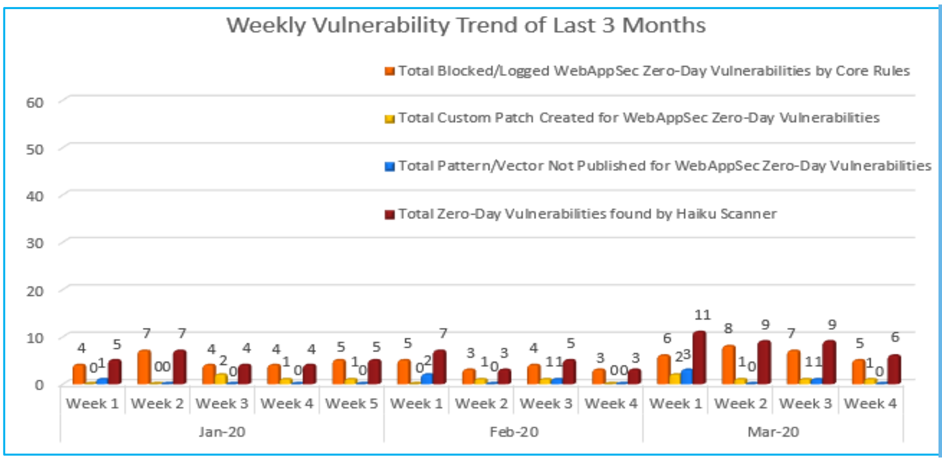
10 Cross Site Scripting	**8** SQL Injection	**1** DDOS Attack	**1** XML External Entities	**4** Directory Traversal	**1** Open Redirect	**4** Command Injection	**4** Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	26
Zero-Day Vulnerabilities Protected through Custom Rules	6*
Zero-Day Vulnerabilities for which protection cannot be determined	1**
Zero-Day Vulnerabilities found by Indusface WAS	28

* 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:

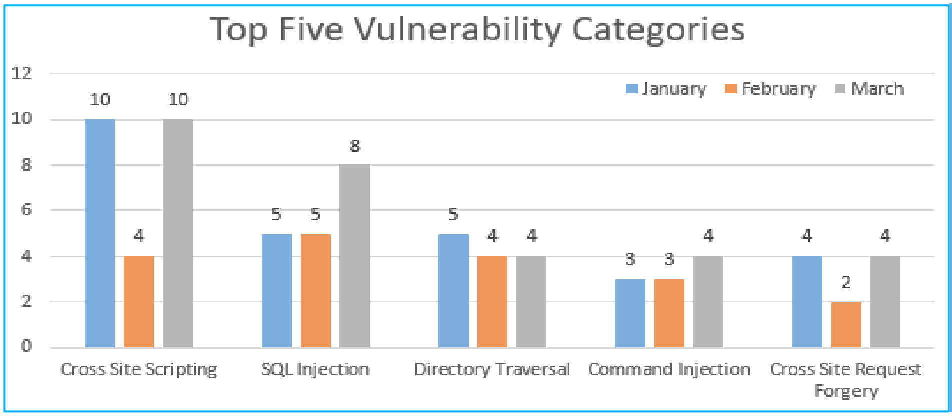


Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.

70% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

26% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

77% 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 January & March.

Minimum CSRF attacks are discovered in February compared to other 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	Indusface WAS Coverage
1.	Cross Site Scripting	CVE-2020-8127	reveal.js up to 3.9.1 postMessage cross site scripting	A vulnerability classified as problematic was found in reveal.js up to 3.9.1 (JavaScript Library). Affected by this vulnerability is some unknown processing. 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-2018-19599	Monstra CMS 1.6 SVG Document cross site scripting	A vulnerability was found in Monstra CMS 1.6 (Content Management System). It has been classified as problematic. Affected is an unknown code block of the file admin/index.php?id=filesmanager&amp;path=uploads/. 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-2018-17572	InfluxDB 0.9.5 Write Data Module Reflected cross site scripting	A vulnerability was found in InfluxDB 0.9.5 and classified as problematic. This issue affects an unknown code of the component Write Data Module. 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.
		NA	MunkiReport up to 5.3.0 /report/broken_client cross site scripting	A vulnerability classified as problematic has been found in MunkiReport up to 5.3.0 (Reporting Software). This affects an	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.

		unknown function of the file /report/broken_client. Upgradi ng to version 5.3.0.3923 eliminates this vulnerability.		
CVE-2020-4084	HCL Connections 5.5/6.0/6.5 Web UI cross site scripting	A vulnerability has been found in HCL Connections 5.5/6.0/6.5 and classified as problematic. Affected by this vulnerability is an unknown code block of the component Web UI. 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-2020-10434	Chadha PHPKB Standard Multi-Language 9 admin/header.php cross site scripting	A vulnerability classified as problematic was found in Chadha PHPKB Standard Multi-Language 9. This vulnerability affects some unknown processing of the file admin/header.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 Cross Site Scripting attack.
CVE-2020-10242	Joomla CMS up to 3.9.15 Protostar/Beez3 cross site scripting	A vulnerability was found in Joomla CMS up to 3.9.15 (Content Management System). It has been classified as problematic. This affects an unknown code of the component Protostar/Beez3. Upgrading to version 3.9.16 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
CVE-2019-14512	LimeSurvey 3.17.7+190627 Boxes box.php cross site scripting	A vulnerability, which was classified as problematic, was found in LimeSurvey 3.17.7+190627 (Survey Software). Affected is an unknown function of the file application/extensions/PanelBoxWidget/views/box.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.

				php of the component Boxes Handler. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.		
		CVE-2020-7482	Schneider Electric Andover Continuum Web Server cross site scripting	A vulnerability was found in Schneider Electric Andover Continuum affected version not known). It has been rated as problematic. Affected by this issue is an unknown function of the component Web Server. 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-2020-5552	mailform 1.04 cross site scripting	A vulnerability was found in mailform 1.04 and classified as problematic. Affected by this issue is 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 Cross Site Scripting attack.
2.	SQL Injection	CVE-2020-9465	EyesOfNetwork up to 5.3-2 eonweb Web Interface user_id sql injection	A vulnerability classified as critical has been found in EyesOfNetwork up to 5.3-2. This affects an unknown function of the component eonweb Web Interface. Upgrading to version 5.3-3 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
		CVE-2018-16357	PbootCMS api.php/Cms/search order sql injection	A vulnerability, which was classified as critical, was found in PbootCMS (the affected version unknown). This affects some unknown functionality of the file api.ph p/Cms/search. There is no information about possible	Protected by Default Rules.	Detected by scanner as SQL Injection attack.

		countermeasures known. It may be suggested to replace the affected object with an alternative product .		
CVE-2018-16356	PbootCMS api.php/List/index order sql injection	A vulnerability, which was classified as critical, has been found in PbootCMS affected version not known). Affected by this issue is an unknown functionality of the file api.php/List/index. 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-2020-10190	MunkiReport up to 5.2.x tablequery.php sql injection	A vulnerability was found in MunkiReport up to 5.2.x (Reporting Software). It has been declared as critical. Affected by this vulnerability is an unknown code block of the file app/models/tablequery.php. Upgrading to version 5.3.0 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
CVE-2020-8783	SuiteCRM up to 7.10.22/7.11.10 sql injection	A vulnerability was found in SuiteCRM up to 7.10.22/7.11.10. It has been declared as critical. Affected by this vulnerability is an unknown code. Upgrading to version 7.10.23 or 7.11.11 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
CVE-2020-8784	SuiteCRM up to 7.10.22/7.11.10 sql injection	A vulnerability was found in SuiteCRM up to 7.10.22/7.11.10. It has been rated as critical. Affected by this issue is an unknown code block. Upgrading to version 7.10.23 or 7.11.11 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.

		CVE-2020-103 65	LogicalDOC up to 8.3.2 Parameter sql injection	A vulnerability was found in LogicalDOC up to 8.3.2. It has been rated as critical. This issue affects some unknown processing. Upgrading to version 8.3.3 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
		CVE-2020-10817	custom-searchable-data-entry-system up to 1.7.1 on WordPress sql injection	A vulnerability classified as critical has been found in custom-searchable-data-entry-system up to 1.7.1on WordPress (WordPress Plugin). This affects an unknown function. The problem might be mitigated by replacing the product with as an alternative.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
3.	Cross Site Request Forgery	CVE-2020-7988	phpipam 1.4 result.php cross site request forgery	A vulnerability was found in phpipam 1.4. It has been declared as problematic. This vulnerability affects an unknown part of the file tools/pass-change/result.php. 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-2020-10057	GeniXCMS 1.1.7 Incomplete Fix cross site request forgery	A vulnerability was found in GeniXCMS 1.1.7 (Content Management System). It has been rated as problematic. Affected by this issue is an unknown code block of the component Incomplete Fix. 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-2019-16107	phpBB 3.2.7 Token Attachment cross site request forgery	A vulnerability, which was classified as problematic, was found in phpBB 3.2.7 (Forum Software). Affected is an unknown code of the component	Protected by Custom Rules.	NA

				Token Handler. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.		
		CVE-2020-6585	Nagios Log Server 2.1.3 cross site request forgery	A vulnerability was found in Nagios Log Server 2.1.3 (Log Management Software) and classified as problematic. Affected by this issue is 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 Custom Rules.	NA
4.	Command Injection	CVE-2019-5155	WAGO PFC200 03.00.39(12)/03.01.07(13)/03.02.02(14) System Command command injection	A vulnerability classified as critical was found in WAGO PFC200 03.00.39(12)/03.01.07(13)/03.02.02(14). Affected by this vulnerability is 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 Command Injection attack.
		CVE-2020-7601	gulp-scss-lint up to 1.0.0 src/command.js command injection	A vulnerability was found in gulp-scss-lint up to 1.0.0 and classified as critical. Affected by this issue is an unknown code block of the file src/command.js. 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 Command Injection attack.
		CVE-2020-10808	Vesta Control Panel up to 0.9.8-26 Backup Listing Endpoint schedule/backup Shell Metacharacter	A vulnerability has been found in Vesta Control Panel up to 0.9.8-26 and classified as critical. This vulnerability affects an unknown code block of the file schedule/backup of the component Backup	Protected by Default Rules.	Detected by scanner as Command Injection attack.

			command injection	Listing Endpoint. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.		
		CVE-2020-5556	Shihonkanri Plus GOOUT 1.5.8/2.2.10 OS Command Injection privilege escalation	A vulnerability classified as critical has been found in Shihonkanri Plus GOOUT 1.5.8/2.2.10. Affected is 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 Command Injection attack.
5.	Directory Traversal	CVE-2020-1737	Ansible up to 2.7.17/2.8.9/2.9.6 win_unzip Extract-Zip Archive directory traversal	A vulnerability has been found in Ansible up to 2.7.17/2.8.9/2.9.6 and classified as problematic. This vulnerability affects the function Extract-Zip of the component win_unzip. 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-2019-19296	Siemens SiNVR 3 Central Control Server FTP Service directory traversal	A vulnerability has been found in Siemens SiNVR 3 Central Control Server and SiNVR 3 Video Server the affected version is unknown) and classified as critical. This vulnerability affects an unknown functionality of the component FTP Service. 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.
			Kyocera ECOSYS M5526cdw 2R7_2000.001.701 Web Application	A vulnerability classified as critical was found in Kyocera ECOSYS M5526cdw 2R7_2000.001.701. This	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.

			directory traversal	vulnerability affects some unknown functionality of the component Web Application. There is no information about possible countermeasures known . It may be suggested to replace the affected object with an alternative product.		
		CVE-2019-19486	Centreon up to 19.04.4 Plugin Test minPlayCommand.php directory traversal	A vulnerability, which was classified as critical, has been found in Centreon up to 19.04.4. This issue affects some unknown functionality of the file minPlayCommand.php of the component Plugin Test 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.	DDOS Attack	NA	Memcached Ddos Attack	The bug is caused by a buffer overflow in the memcached code and if an attacker can supply a long enough value as the buggy parameter, the application will crash. On Monday, someone posted the details of the vulnerability and the PoC code to GitHub, which was apparently the first indication that the application's maintainers got about the issue. The bug affects versions 1.6.0 and 1.6.1.	Protected by Custom Rules.	NA
7.	Open redirect	CVE-2019-6696	Fortinet FortiOS up to 6.0.8/6.2.1 URL Open Redirect	The bug is caused by a buffer overflow in the memcached code and if an attacker can supply a long enough value as the buggy parameter, the application will crash. On Monday, someone posted the details of the vulnerability and the POC code to GitHub, which was apparently the first indication that the	NA	Detected by scanner as Open redirect attack.

				application's maintainers got about the issue. The bug affects versions 1.6.0 and 1.6.1.		
8.	XML External Entities	CVE-2020-10991	MuleSoft APIkit up to 1.3.0 RestXmlSchema Validator.java XML External Entity	Two zero-day flaws have been uncovered in Zoom's macOS client version, according to researchers. The web conferencing platform vulnerabilities could give local, unprivileged attackers root privileges, and allow them to access victims' microphone and camera. The first flaw stems from an issue with Zoom's installer and allows unprivileged attackers to gain root privileges. The second zero day flaw gives attackers Zoom's mic and camera access, allowing for a way to record Zoom meetings, or snoop in on victims' personal lives – sans a user access prompt.	Protected by Custom Rules.	Detected by scanner as XML External Entities attack.