Weekly Zero-Day Vulnerability Coverage Bulletin

June 20

Summary:

Total **20 Zero-Day Vulnerabilities** were discovered in **6 Categories** this month

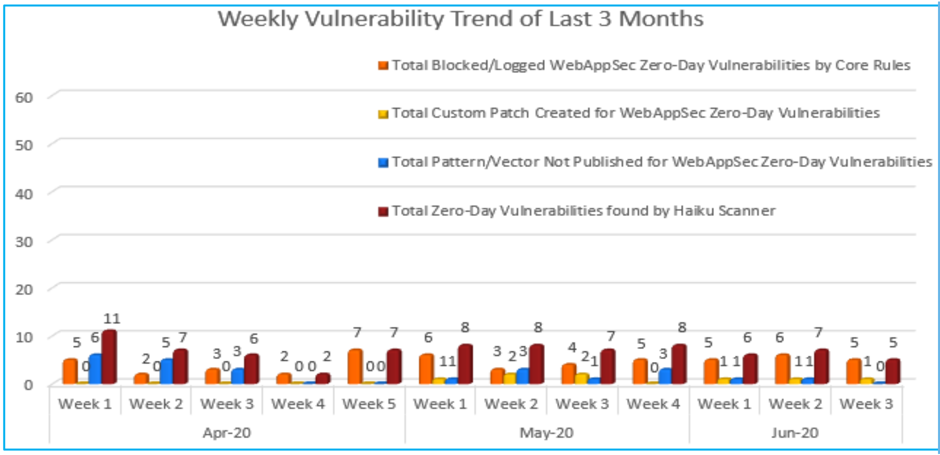
10	2	3	1	1	3
Cross Site Scripting	Directory Traversal	Command Injection	SQL Injection	Open Redirect	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	16
Zero-Day Vulnerabilities Protected through Custom Rules	3*
Zero-Day Vulnerabilities for which protection cannot be determined	1**
Zero-Day Vulnerabilities found by Indusface WAS	18

* 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:

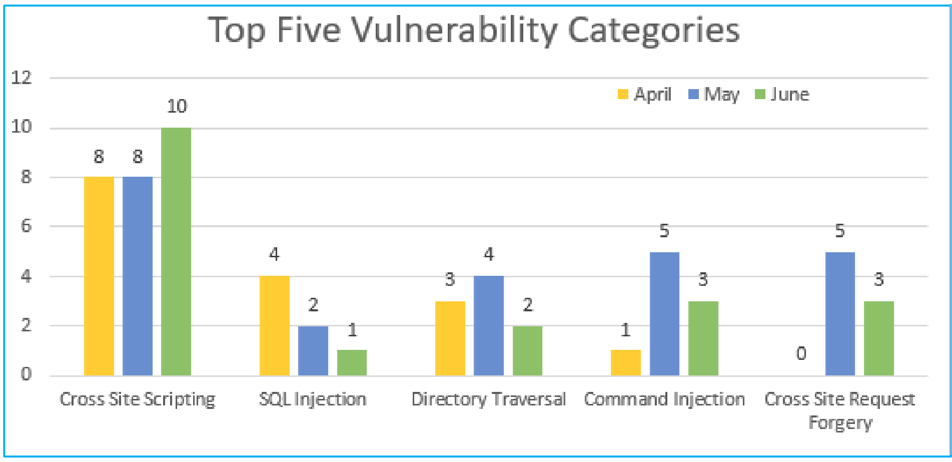


Weekly Trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.

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

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

86% 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 June compared to other months.

Zero Cross Site Request Forgery attack is found 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-2020-4023	Atlassian FishEye/Crucible up to 4.8.1 Review committerFilter cross site scripting	A vulnerability classified as problematic has been found in Atlassian FishEye and Crucible up to 4.8.1 Programming Tool Software). This affects an unknown function of the component Review Handler. Upgrading to version 4.8.2 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2020-13758	Bitrix24 up to 20.0.950 Web Application Firewall post_filter.php cross site scripting	A vulnerability was found in Bitrix24 up to 20.0.950. It has been rated as problematic. This issue affects an unknown code of the file modules/security/classes/general.post_filter.php/post_filter.phpof the component Web Application Firewall. 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-2020-13762	Joomla CMS up to 3.9.18 com_modules cross site scripting	A vulnerability, which was classified as problematic, has been found in Joomla CMS up to 3.9.18 (Content Management System). This issue affects an unknown part of the component com_modules. Upgrading to version 3.9.19 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2020-4041	Bolt CMS up to 3.7.0 File Upload File Name Stored cross site scripting	A vulnerability has been found in Bolt CMS up to 3.7.0 (Content Management System) and classified as problematic. This vulnerability affects an unknown code block of the component File	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.

		Upload. Upgrading to version 3.7.1 eliminates this vulnerability.		
CVE-2020-13892	SportsPress Plugin up to 2.7.1 on WordPress cross site scripting	A vulnerability classified as problematic has been found in SportsPress Plugin up to 2.7.1 on WordPress (WordPress Plugin). Affected is some unknown functionality. Upgrading to version 2.7.2 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
CVE-2020-14012	osTicket 1.14.2 scp/categories.php cross site scripting	A vulnerability, which was classified as problematic, was found in osTicket 1.14.2 (Ticket Tracking Software). Affected is an unknown code block of the file scp/categories.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-2020-9426	OX Guard up to 2.10.3 cross site scripting	A vulnerability has been found in OX Guard up to 2.10.3 and classified as problematic. Affected by this vulnerability is 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 Default Rules.	Detected by scanner as Cross Site Scripting attack.
CVE-2019-19112	wpForo Plugin 1.6.5 on WordPress dashboard.php wpf-dw-td-value cross site scripting	A vulnerability, which was classified as problematic, was found in wpForo Plugin 1.6.5 on WordPress (WordPress Plugin). Affected is the function wpf-dw-td-value of the file dashboard.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-2019-19111	wpForo Plugin 1.6.5 on WordPress admin.php langid cross site scripting	A vulnerability, which was classified as problematic, has been found in wpForo Plugin 1.6.5 on WordPress (WordPress Plugin). This issue affects some unknown processing of the file wp-admin/admin.php?page= wpforo-phrases. 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-2019-19110	wpForo Plugin 1.6.5 on WordPress admin.php cross site scripting	A vulnerability classified as problematic was found in wpForo Plugin 1.6.5 on WordPress (WordPress Plugin). This vulnerability affects an unknown code block of the file wp-admin/admin.php?page= wpforo-phrases. 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-2020-13996	J2Store Plugin up to 3.3.12 on Joomla sql injection	A vulnerability was found in J2Store Plugin up to 3.3.12 on Joomla (Joomla Component). It has been declared as critical. Affected by this vulnerability is some unknown functionality. Upgrading to version 3.3.13 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as SQL Injection attack.
		CVE-2020-10549	rConfig up to 3.9.4 snippets.inc.php sql injection	A vulnerability classified as critical has been found in rConfig up to 3.9.4. Affected is an unknown function of the file snippets.inc.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.	Cross Site Request Forgery	CVE-2020-13760	Joomla CMS up to 3.9.18 com_postinstall cross site request forgery	A vulnerability classified as problematic has been found in Joomla CMS up to 3.9.18 (Content Management System). This affects an unknown functionality of the component com_postinstall. Upgrading to version 3.9.19 eliminates this vulnerability.	Protected by Custom Rules.	Detected by scanner as Cross Site Request Forgery attack.
		CVE-2020-9042	Couchbase Server 6.0 REST API API Request cross site request forgery	A vulnerability was found in Couchbase Server 6.0. It has been classified as problematic. This affects some unknown functionality of the component REST API. 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-2019-19109	wpForo Plugin 1.6.5 on WordPress admin.php cross site request forgery	A vulnerability classified as problematic has been found in wpForo Plugin 1.6.5 on WordPress (WordPress Plugin). This affects an unknown code of the file wp-admin/admin.php?page= wpforo-usergroups. 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-2020-7672	mosc up to 1.0.0 eval properties Code Execution	A vulnerability, which was classified as critical, was found in mosc up to 1.0.0. Affected is the function eval. 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-2020-7674	access-policy up to 3.1.0 eval Code Execution	A vulnerability was found in access-policy up to 3.1.0 and classified as critical. Affected by this issue is the function eval. 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-2020-12851	Pydio Cells 2.0.4 Web Application directory traversal	A vulnerability, which was classified as critical, was found in Pydio Cells 2.0.4. Affected is an unknown part 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.	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.
		CVE-2020-4053	Helm up to 3.2.3 Plugin Installation TAR Archive directory traversal	A vulnerability was found in Helm up to 3.2.3. It has been rated as critical. This issue affects an unknown code of the component Plugin Installation Handler. Upgrading to version 3.2.4 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.
6.	Open Redirect	CVE-2020-4048	WordPress up to 5.4.1 wp_validate_redirect() Open Redirect	A vulnerability was found in WordPress (Content Management System). It has been declared as problematic. This vulnerability affects the function wp_validate_redirect. Upgrading to version 3.7.34, 3.8.34, 3.9.32, 4.0.31, 4.1.31, 4.2.28, 4.3.24, 4.4.23, 4.5.22, 4.6.19, 4.7.18, 4.8.14, 4.9.15, 5.0.10, 5.1.6, 5.2.7, 5.3.4 or 5.4.2 eliminates this vulnerability.	NA	Detected by scanner as Open Redirect attack.