Monthly Zero-Day Vulnerability Coverage Bulletin

November 2021

Total Zero-Day Vulnerabilities Found: 27

Command Injection	CSRF	Local File Inclusion	SQL Injection	Cross-Site Scripting	XML External Entity
1	2	6	4	11	3

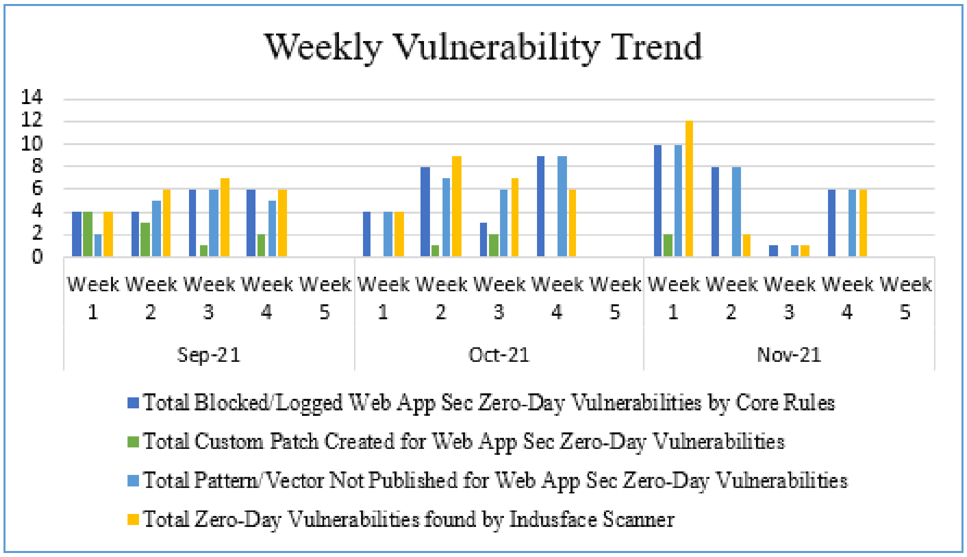
Zero-Day vulnerabilities protected through core rules	25
Zero-Day vulnerabilities protected through custom rules	2 *
Zero-Day vulnerabilities for which protection cannot be determined	0 **
Zero-Day vulnerabilities found by Indusface WAS	25

* To enable custom rules, please contact support@indusface.com

** Since the attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected.

Vulnerability Trend:

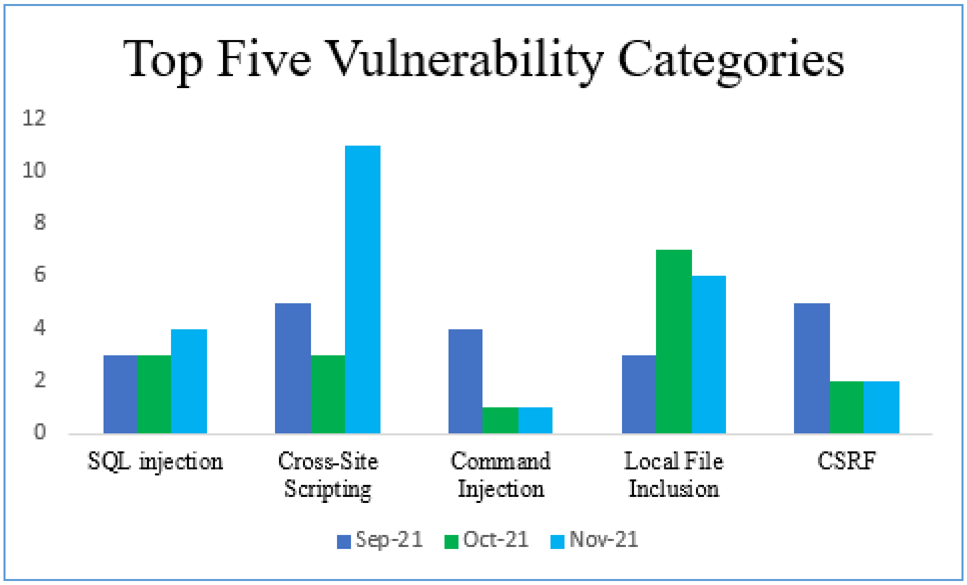
The weekly trend displays the total number of vulnerabilities discovered to the type of protection provided for the last quarter.



93% of the zero-day vulnerabilities were protected by the **core rules** in the last quarter

7% of the zero-day vulnerabilities were protected by the **custom rules** in the last quarter

93% of the zero-day vulnerabilities were reported by **Indusface Scanner** in the last quarter



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 round-the-clock protection for customer sites.

Vulnerability Details:

S. No	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
1	Local File Inclusion	CVE-2021-3907	Cloudflare OctoRPKI Cache Folder path traversal	A vulnerability, which was classified as critical, has been found inCloudflare OctoRPKI . This issue affects some unknown processing of the component. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the Local File Inclusion attack.
		CVE-2021-43493	ServerManagement pathname traversal	A vulnerability was found in ServerManagement and classified as problematic. Affected by this issue 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 core rules.	Detected by the scanner as the Local File Inclusion attack.
		CVE-2021-43494	OpenCV-REST-API pathname traversal	A vulnerability, which was classified as problematic, has been found in OpenCV-REST-API. This issue affects an unknown function. There is no information about	Protected by core rules.	Detected by the scanner as the Local File Inclusion attack.

			possible countermeasures known. It may be suggested to replace the affected object with an alternative product.		
	CVE-2021-43496	Clustering pathname traversal	A vulnerability, which was classified as problematic, was found in Clustering. Affected is an 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 core rules.	Detected by the scanner as the Local File Inclusion attack.
	CVE-2021-43492	AlquistManager pathname traversal	A vulnerability has been found in AlquistManager and classified as problematic. Affected by this vulnerability 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 core rules.	Detected by the scanner as the Local File Inclusion attack.
	CVE-2021-42727	Adobe RoboHelp Server up to 2020.0.1 Tomcat path traversal	A vulnerability, which was classified as critical, has been found in Adobe RoboHelp Server up to 2020.0.1. Affected by this issue is some unknown functionality of the component.	Protected by core rules.	Detected by the scanner as the Local File Inclusion attack.

				Upgrading eliminates this vulnerability.		
2	Command Injection	CVE-2021-42321	Microsoft Exchange Server 2016 CU22/2019 CU11 Privilege Escalation	A vulnerability has been found in Microsoft Exchange Server 2016 CU22/2019 CU11 and classified as critical. Applying a patch aneliminate this problem. A possible mitigation has been published immediately after the disclosure of the vulnerability.	Protected by core rules.	Detected by the scanner as the Command Injection attack.
3	Cross-Site Request Forgery	CVE-2021-24572	Accept Donations with PayPal Plugin up to 1.3.0 on WordPress Donation Button cross-site request forgery	A vulnerability, which was classified as problematic, was found in Accept Donations with PayPal. This affects some unknown processing of the component. Upgrading to version 1.3.1 eliminates this vulnerability.	Protected by custom rules.	NA
		CVE-2020-36504	WP-Pro-Quiz Plugin up to 0.37 on WordPress Delete cross-site request forgery	A vulnerability classified as problematic was found in WordPress. Affected by this vulnerability is an unknown code of the component. 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	SQL Injection	CVE-2020-28702	PybbsCMS 5.2.1 TopicMapper.xml SQL Injection	A vulnerability, which was classified as critical, has been found in PybbsCMS 5.2.1. Affected by this issue is some unknown processing of the file. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2021-31849	McAfee Data Loss Prevention ePO Extension prior 11.7.100 SQL Injection	A vulnerability, which was classified as critical, has been found in McAfee Data Loss Prevention ePO Extension. This issue affects an unknown functionality. Upgrading to version 11.7.100 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2021-36299	Dell EMC iDRAC9 prior 4.40.29.00/5.00.00.00 SQL Injection	A vulnerability classified as critical was found in Dell EMC iDRAC9. Affected by this vulnerability is an unknown function. Upgrading to version 4.40.29.00 or 5.00.00.00 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2021-36300	Dell EMC iDRAC9 prior 5.00.00.00 SQL Injection	A vulnerability, which was classified as critical, has been found in Dell EMC iDRAC9. Affected by this issue is an unknown functionality. Upgrading to version 5.00.00.00	Protected by core rules.	Detected by the scanner as the SQL Injection attack.

				eliminates this vulnerability.		
5	Cross-Site Scripting	CVE-2021-24685	Flat Preloader Plugin up to 1.5.3 on WordPress Setting cross-site scripting	A vulnerability classified as problematic was found in the Flat Preloader Plugin up to 1.5.3. This vulnerability affects some unknown functionality of the component. Upgrading to version 1.5.4 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2015-10001	WP-Stats Plugin prior 2.52 on WordPress cross-site scripting	A vulnerability was found in WP-Stats Plugin. It has been declared as problematic. This vulnerability affects an unknown code block. Upgrading to version 2.52 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-24789	Flat Preloader Plugin up to 1.5.4 on WordPress Frontend cross-site scripting	A vulnerability, which was classified as problematic, has been found in Flat Preloader Plugin up to 1.5.4. Affected by this issue is some unknown functionality of the component. Upgrading to version 1.5.5 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
		CVE-2021-24715	WP Sitemap Page Plugin up to 1.6.x on WordPress Setting cross-site scripting	A vulnerability was found in WP Sitemap Page Plugin up to 1.6.x. It has been classified as problematic. Affected is some unknown functionality of the component. Upgrading to version	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.

		1.7.0 eliminates this vulnerability.		
CVE-2021-24813	Events Made Easy Plugin prior 2.2.24 on WordPress Custom Field cross-site scripting	A vulnerability was found in the Events Made Easy Plugin. It has been classified as problematic. This affects an unknown code of the component. Upgrading to version 2.2.24 eliminates this vulnerability. Applying a patch can eliminate this problem. The best possible mitigation is suggested to be upgrading to the latest version.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2021-41349	Microsoft Exchange Server 2013 CU23/2016 CU22/2019 CU11 information disclosure	A vulnerability was found in Microsoft Exchange Server 2013 CU23/2016 CU22/2019 CU11. It has been declared as problematic. Affected by this vulnerability is an unknown code. Applying a patch can eliminate this problem. A possible mitigation has been published immediately after the disclosure of vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2020-14424	Cacti up to 1.2.17 Template Import cross-site scripting	A vulnerability, which was classified as problematic, has been found in Cacti up to 1.2.17). This issue affects an unknown code block of the component. Upgrading to version 1.2.18 eliminates this vulnerability. Applying a patch can	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.

		eliminate this problem. The best possible mitigation is suggested to be upgrading to the latest version.		
CVE-2021-33850	Microsoft Clarity 0.3 Configuration cross-site scripting	A vulnerability was found in Microsoft Clarity 0.3 and classified as problematic. Affected by this issue is an unknown function of the component. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2021-31852	McAfee Policy Auditor up to 6.5.1 Web-based Interface UID cross-site scripting	A vulnerability was found in Microsoft Clarity 0.3 and classified as problematic. Affected by this issue is an unknown function of the component. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
CVE-2021-31851	McAfee Policy Auditor up to 6.5.1 Web-based Interface profileNodeID cross-site scripting	A vulnerability classified as problematic has been found in McAfee Policy Auditor up to 6.5.1. Affected is an unknown part of the component. Upgrading to version	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.

				6.5.2 eliminates this vulnerability.		
		CVE-2021-36332	Dell EMC CloudLink up to 7.1 cross-site scripting	A vulnerability, which was classified as problematic, has been found in Dell EMC CloudLink up to 7.1. This issue affects an unknown part. Upgrading eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross-Site Scripting attack.
6	XML External Entity	CVE-2020-25911	MODX CMS 2.7.3 modRestService Request XML external entity reference	A vulnerability was found in MODX CMS 2.7.3. It has been rated as critical. This issue affects an unknown code block of the component. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as an XML external entity attack.
		CVE-2021-20839	Antenna House Office Server Document Converter up to 7.1MR7/7.2MR4 XML Document XML external entity reference	A vulnerability was found in Antenna House Office Server Document Converter up to 7.1MR7/7.2MR4. It has been declared as critical. This vulnerability affects an unknown code of the component. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as an XML external entity attack.

	CVE-2020-26705	Easy-XML 0.5.0 XML Content parseXML xml external entity reference	A vulnerability was found in Easy-XML 0.5.0 and classified as critical. Affected by this issue is the function of the component. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by core rules.	Detected by the scanner as XML external entity attack.