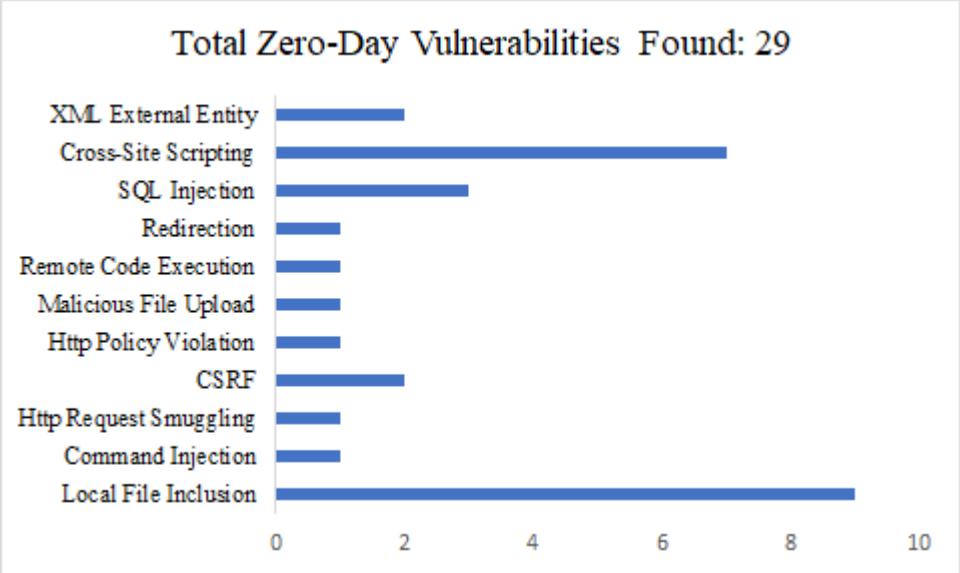
Monthly Zero-Day Vulnerability Coverage Bulletin

October 2021



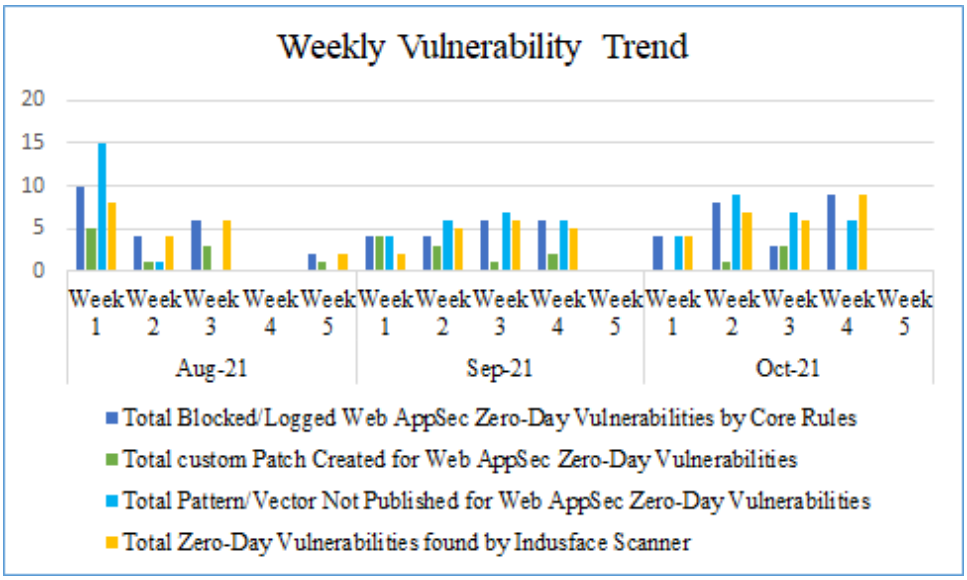
Zero-Day vulnerabilities protected through core rules	24
Zero-Day vulnerabilities protected through custom rules	4 *
Zero-Day vulnerabilities for which protection cannot be determined	1 **
Zero-Day vulnerabilities found by Indusface WAS	26

* 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:

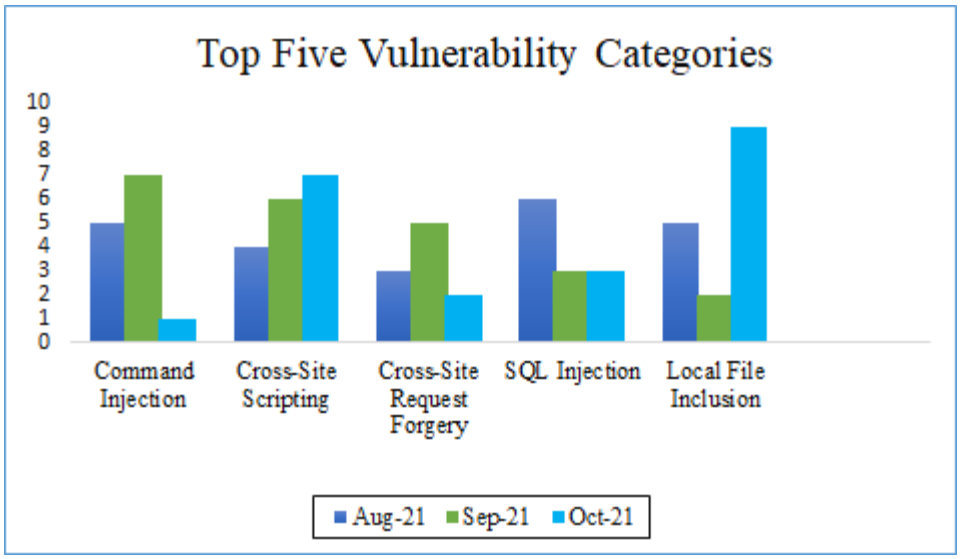
The weekly trend displays the total no. of vulnerabilities discovered to the type of protection provided for the last quarter.



83% of the zero-day vulnerabilities were protected by the **core rules** in the last quarter

14% of the zero-day vulnerabilities were protected by the **custom rules** in the last quarter

90% 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-2021-3710	Apport apport/hookutils.py read_file path traversal	A vulnerability, which was classified as critical, was found in Apport. This affects the function. Upgrading eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Local File Inclusion attack.
		CVE-2021-41103	containerd up to 1.4.10/1.5.6 path traversal	A vulnerability, which was classified as critical, has been found in containerd up to 1.4.10/1.5.6. Affected by this issue is an unknown code. Upgrading to version 1.4.11 or 1.5.7 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Local File Inclusion attack.
		CVE-2021-41773	Apache HTTP Server 2.4.49 Path Normalization path traversal	A vulnerability has been found in Apache HTTP Server 2.4.49 and classified as critical. This vulnerability affects	Protected by core rules.	Detected by the scanner as the Local File Inclusion attack.

			an unknown code of the component. Upgrading to version 2.4.50 eliminates this vulnerability.		
	CVE-2021-41152	OpenOLAT up to 15.5.7/16.0.0 Folder path traversal	A vulnerability classified as critical was found in OpenOLAT up to 15.5.7/16.0.0. This vulnerability affects some unknown processing of the component. Upgrading to version 15.5.8 or 16.0.1 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Local File Inclusion attack.
	CVE-2021-41150	tough Library up to 0.11.x Repository path traversal	A vulnerability was found in tough Library up to 0.11.x. It has been classified as critical. Affected is some unknown functionality of the component. Upgrading to version 0.12.0 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Local File Inclusion attack.
	CVE-2021-22013	vCenter Server file path traversal vulnerability	The vCenter Server contains a file path traversal vulnerability leading to information disclosure in the appliance management API. A malicious actor with network access to port 443 on vCenter Server may exploit this issue to gain access to sensitive information.	Protected by core rules.	Detected by the scanner as the Local File Inclusion attack.
	CVE-2021-38346	Authenticated File Upload and Path Traversal	The Brizy Page Builder plugin <= 2.3.11 for WordPress allowed authenticated users to upload executable files to a location of their choice using the	Protected by core rules.	Detected by the scanner as the Local File Inclusion attack.

			brizy_create_block_ screenshot AJAX action. The file would be named using the id parameter, which could be prepended with "../" to perform directory traversal, and the file contents were populated via the ibsf parameter, which would be base64-decoded and written to the file. While the plugin added a .jpg extension to all uploaded filenames, a double extension attack was still possible, e.g., a file named shell.php would be saved as shell.php.jpg, and would be executable on a number of common configurations.		
	CVE-2021-41773	Apache HTTP Server Path Traversal	A flaw was found in a change made to path normalization in Apache HTTP Server 2.4.49. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives.	Protected by core rules.	Detected by the scanner as the Local File Inclusion attack.
	CVE-2021-42013	Apache HTTP Server Remote Code Execution	An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied",	Protected by core rules.	Detected by the scanner as the Local File Inclusion attack.

				these requests can succeed. If CGI scripts are also enabled for these aliased pathes, this could allow for remote code execution.		
2	Command Injection	CVE-2021-42094	Zammad up to 4.1.0 Custom Package command injection	A vulnerability classified as critical was found in Zammad up to 4.1.0. Affected by this vulnerability is an unknown functionality of the component. Upgrading to version 4.1.1 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Command Injection attack.
3	HTTP Request Smuggling	CVE-2021-22959	Node.js up to 12.22.6/14.18.0 /16.11.0 llhttp request smuggling	A vulnerability has been found inNode.js up to 12.22.6/14.18.0/16. 11.0 and classified as critical. Affected by this vulnerability is an unknown code of the component. Upgrading to version 12.22.7, 14.18.1 or 16.11.1 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the HTTP Request Smuggling attack.
4	Cross-Site Request Forgery	CVE-2020-21386	maccms 10 info.html cross-site request forgery	A vulnerability was found in. It has been classified as problematic. This affects 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 custom rules.	NA
		CVE-2021-42228	KindEditor 4.1.x Google Editor uploadbutton.ht ml cross-site request forgery	A vulnerability was found in. It has been classified as problematic. This affects an unknown part of the file.	Protected by custom rules.	NA

	There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

5	HTTP Policy Violation	CVE-2021-22018	vCenter Server file deletion vulnerability	The vCenter Server contains an arbitrary file deletion vulnerability in a VMware vSphere Life-cycle Manager plug-in. A malicious actor with network access to port 9087 on vCenter Server may exploit this issue to delete non critical files.	Protected by core rules.	Detected by the scanner as the HTTP Policy Violation attack.
6	Malicious File Upload	CVE-2021-41868	OnionShare 2.3.0/2.3.1/2.3.2/2.3.3 Receive unrestricted upload	A vulnerability, which was classified as critical, has been found in OnionShare 2.3.0/2.3.1/2.3.2/2.3.3. Affected by this issue is an unknown function of the component. Upgrading to version 2.4 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Malicious File Upload attack.
7	Remote Code Execution	CVE-2021-38112	AWS WorkSpaces Remote Code Execution	In the Amazon AWS WorkSpaces client 3.0.10 through 3.1.8 on Windows, argument injection in the workspaces:// URI handler can lead to remote code execution because of the Chromium Embedded Framework (CEF) --gpu-launcher argument. This is fixed in 3.1.9.	Protected by core rules.	Detected by the scanner as the Remote Code Execution attack.
8	Redirection	CVE-2021-22963	fastify-static up to 4.2.3 redirect	A vulnerability, which was classified as problematic, was found infastify-static up to 4.2.3. Affected is an unknown function. Upgrading to version 4.2.4 eliminates this vulnerability.	Research in queue	Research in queue

9	SQL Injection	CVE-2021-41647	Kaushik Jadhav Online Food Ordering Web App 1.0 Parameter login.php username sql injection	A vulnerability, which was classified as critical, was found in Subrion CMS 4.2.1. This affects 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 SQL Injection attack.
		CVE-2021-24465	Meow Gallery Plugin up to 4.1.8 on WordPress Shortcode sql injection	A vulnerability classified as critical has been found in Meow Gallery Plugin up to 4.1.8. This affects an unknown part of the component. Upgrading to version 4.1.9 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the SQL Injection attack.
		CVE-2021-41947	Subrion CMS 4.2.1 Visual-Mode sql injection	A vulnerability, which was classified as critical, was found in Subrion CMS 4.2.1. This affects 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 SQL Injection attack.

10	Cross-Site Scripting	CVE-2020-20799	JeeCMS 1.0.1 Parameter commentText cross site scripting	A vulnerability was found in JeeCMS 1.0.1. It has been classified as problematic. This 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 Cross- Site Scripting attack.
		CVE-2021-40922	bugs up to 1.8 Parameter install/index.php last_name cross site scripting	A vulnerability, which was classified as problematic, has been found in bugs up to 1.8. This issue affects an unknown part of the file 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-2021-24654	User Registration Plugin up to 2.0.1 on WordPress user_registration_update_profile_details user_registration_profile_pic_url cross site scripting	A vulnerability classified as problematic was found in User Registration Plugin up to 2.0.1. This vulnerability affects the function. Upgrading to version 2.0.2 eliminates this vulnerability.	Protected by core rules.	Detected by the scanner as the Cross- Site Scripting attack.

	CVE-2021-39329	JobBoardWP Plugin up to 1.0.7 on WordPress class-metabox.php cross site scripting	A vulnerability has been found in JobBoardWP Plugin up to 1.0.7 and classified as problematic. This vulnerability affects an unknown functionality 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 Cross- Site Scripting attack.
	CVE-2021-22016	vCenter Server reflected XSS vulnerability	The vCenter Server contains a reflected cross-site scripting vulnerability due to a lack of input sanitization. An attacker may exploit this issue to execute malicious scripts by tricking a victim into clicking a malicious link.	Protected by core rules.	Detected by the scanner as the Cross- Site Scripting attack.
	CVE-2021-38344	Authenticated Stored Cross-Site Scripting	The Brizy Page Builder plugin <= 2.3.11 for WordPress was vulnerable to stored XSS by lower-privileged users such as a subscribers. It was possible to add malicious JavaScript to a page by modifying the request sent to update the	Protected by core rules.	Detected by the scanner as the Cross- Site Scripting attack.

			page via the brizy_update_item AJAX action and adding JavaScript to the data parameter, which would be executed in the session of any visitor viewing or previewing the post or page.		
	CVE-2021-38356	Reflected Cross-Site Scripting(XSS)	The NextScripts: Social Networks Auto-Poster <= 4.3.20 WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the $_REQUEST['page'] parameter which is echoed out on inc/nxs_class_snap.php by supplying the appropriate value 'nxssnap-post' to load the page in $_GET['page'] along with malicious JavaScript in $_POST['page'].	Protected by core rules.	Detected by the scanner as the Cross- Site Scripting attack.

11	XML External Entity	CVE-2021-20801	Cybozu Remote Service 3.1.8/3.1.9 xml external entity reference	A vulnerability classified as critical has been found in Cybozu Remote Service 3.1.8/3.1.9. 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 custom rules.	NA
		CVE-2020-19954	S-CMS 3.0 /api/notify.php xml external entity reference	A vulnerability was found inS-CMS 3.0. It has been classified as problematic. Affected is an unknown functionality 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 custom rules.	NA