INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

February 2024

The total **zero-day vulnerabilities** count for February month: 174

Command Injection	CSRF	Local File Inclusion	SQLi	Malicious File Upload	XML External Entity	Host Header Injection	Cross-site Scripting
25	14	14	42	13	1	1	64

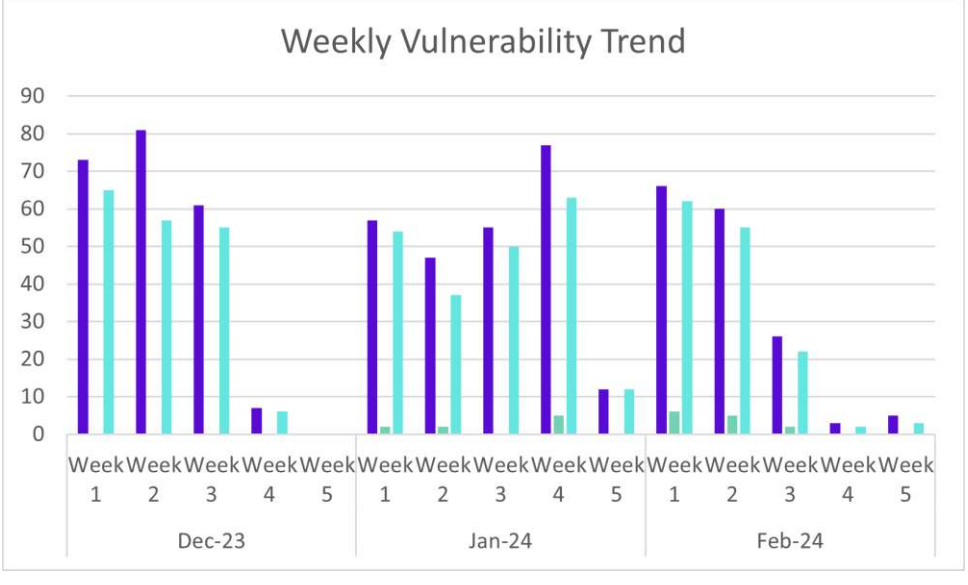
Zero-day vulnerabilities protected through core rules	160
Zero-day vulnerabilities protected through custom rules	13
Zero-day vulnerabilities protected through SaaS rules	1
Zero-day vulnerabilities for which protection cannot be done	0
Zero-day vulnerabilities found by Indusface WAS	144

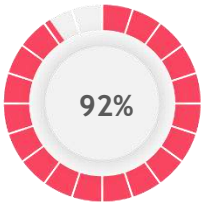
- To enable custom rules, please contact support@indusface.com
- Since the attack vectors are unknown, Indusface cannot determine whether these vulnerabilities are protected.
- Get detailed insights on zero-day vulnerabilities.

Vulnerability Trend:

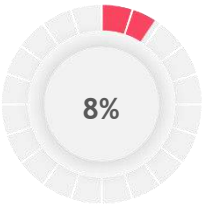
The weekly trend displays the total number of vulnerabilities discovered and the type of protection provided for the last quarter.

Weekly Vulnerability Trend





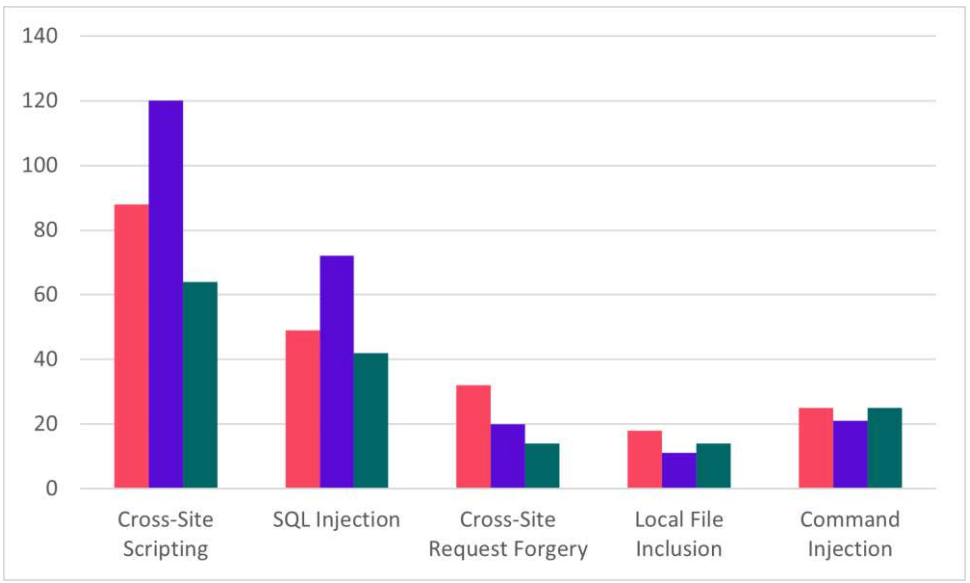
of the zero-day vulnerabilities were protected by the core rules in the last month



of the zero-day vulnerabilities were protected by the custom rules in the last month

of the zero-day vulnerabilities were reported by Indusface Scanner in the last month

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-0921	D-Link DIR-816 A2 1.10CNB04 Web Interface setDeviceSettings statuscheckpppoeuser os command injection	A vulnerability has been found in D-Link DIR-816 A2 1.10CNB04 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /goform/setDeviceSettings of the component Web Interface. The manipulation of the argument statuscheckpppoeuser leads to os command injection. This vulnerability is known as CVE-2024-0921. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-22545	TRENDnet TEW-824DRU 1.04b01 sub_420AE0 command injection	A vulnerability was found in TRENDnet TEW-824DRU 1.04b01. It has been rated as critical. This issue affects the function sub_420AE0. The manipulation leads to command injection. The identification of this vulnerability is CVE-2024-22545. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-0986	Issabel PBX 4.0.0 Asterisk-Cli index.php Command os command injection	A vulnerability was found in Issabel PBX 4.0.0. It has been rated as critical. This issue affects some unknown processing of the file /index.phpmenuasterisk_cli of the component Asterisk-Cli. The manipulation of the argument Command leads to os command injection. The identification of this vulnerability is CVE-2024-0986. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2023-49038	Buffalo LS210D 1.78-0.03 Ping Utility os command injection	A vulnerability was found in Buffalo LS210D 1.78-0.03. It has been classified as critical. This affects an unknown part of the component Ping Utility. The manipulation leads to os command injection. This vulnerability is uniquely identified as CVE-2023-49038. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-24325	Totolink A3300R 17.0.0cu.557_B20221024 setParentalRules enable command injection	A vulnerability which was classified as critical has been found in Totolink A3300R 17.0.0cu.557_B20221024. Affected by this issue is the function setParentalRules. The manipulation of the argument enable leads to command injection. This vulnerability is handled as CVE-2024-24325. Access to the local network is required for this attack to succeed. There is no exploit available.	Patched by core rule	Y
CVE-2024-24326	Totolink A3300R 17.1cu.643_B20200521 setStaticDhcpRules arpEnable command injection	A vulnerability which was classified as critical was found in Totolink A3300R 17.1cu.643_B20200521. This affects the function	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		setStaticDhcpRules. The manipulation of the argument arpEnable leads to command injection. This vulnerability is uniquely identified as CVE-2024-24326. The attack needs to be approached within the local network. There is no exploit available.		
CVE-2024-24327	Totolink A3300R 17.0.0cu.557_B20221024 setIpv6Cfg pppoePass command injection	A vulnerability has been found in Totolink A3300R 17.0.0cu.557_B20221024 and classified as critical. This vulnerability affects the function setIpv6Cfg. The manipulation of the argument pppoePass leads to command injection. This vulnerability was named CVE-2024-24327. The attack can only be done within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-24328	Totolink A3300R 17.0.0cu.557_B20221024 setMacFilterRules enable command injection	A vulnerability was found in Totolink A3300R 17.0.0cu.557_B20221024 and classified as critical. This issue affects the function setMacFilterRules. The manipulation of the argument enable leads to command injection. The identification of this vulnerability is CVE-2024-24328. The attack can only be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-24329	Totolink A3300R 17.0.0cu.557_B20221024 setPortForwardRules enable command injection	A vulnerability was found in Totolink A3300R 17.0.0cu.557_B20221024. It has been classified as critical. Affected is the function setPortForwardRules. The manipulation of the argument enable leads to command injection. This vulnerability is traded as CVE-2024-24329. The attack needs to be done within the local network. There is no	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit available.		
CVE-2024-24331	Totolink A3300R 17.0.0cu.557_B20221024 setWiFiScheduleCfg enable command injection	A vulnerability was found in Totolink A3300R 17.0.0cu.557_B20221024. It has been declared as critical. Affected by this vulnerability is the function setWiFiScheduleCfg. The manipulation of the argument enable leads to command injection. This vulnerability is known as CVE-2024-24331. The attack needs to be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-24332	Totolink A3300R 17.0.0cu.557_B20221024 setUrlFilterRules url command injection	A vulnerability was found in Totolink A3300R 17.0.0cu.557_B20221024. It has been rated as critical. Affected by this issue is the function setUrlFilterRules. The manipulation of the argument url leads to command injection. This vulnerability is handled as CVE-2024-24332. Access to the local network is required for this attack. There is no exploit available.	Patched by core rule	Y
CVE-2024-24333	Totolink A3300R 17.0.0cu.557_B20221024 setWiFiAclRules desc command injection	A vulnerability classified as critical has been found in Totolink A3300R 17.0.0cu.557_B20221024. This affects the function setWiFiAclRules. The manipulation of the argument desc leads to command injection. This vulnerability is uniquely identified as CVE-2024-24333. Access to the local network is required for this attack to succeed. There is no exploit available.	Patched by core rule	Y
CVE-2024-24330	Totolink A3300R 17.1cu.643_B20200521 setRemoteCfg enable command injection	A vulnerability classified as critical was found in Totolink A3300R 17.1cu.643_B20200521. Affected by this vulnerability is the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		function setRemoteCfg. The manipulation of the argument enable leads to command injection. This vulnerability is known as CVE-2024-24330. The attack can be launched remotely. There is no exploit available.		
CVE-2024-21488	tomas network prior 0.7.0 mac_address_for os command injection	A vulnerability has been found in tomas network and classified as critical. This vulnerability affects the function mac_address_for. The manipulation leads to os command injection. This vulnerability was named CVE-2024-21488. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-22107	GTB Central Console 15.17.1-30814.NG SystemSettingsController.php command injection	A vulnerability which was classified as critical was found in GTB Central Console 15.17.1-30814.NG. This affects an unknown part of the file /opt/webapp/src/AppBundle/Controller/React/SystemSettingsController.php. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2024-22107. The attack can only be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2023-46359	Hardy Barth cPH2 eCharge Ladestation up to 1.87.0 Connectivity Check os command injection	A vulnerability has been found in Hardy Barth cPH2 eCharge Ladestation up to 1.87.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the component Connectivity Check. The manipulation leads to os command injection. This vulnerability is known as CVE-2023-46359. The attack can	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		be launched remotely. There is no exploit available.		
CVE-2023-36498	TP-LINK ER7206 Omada Gigabit VPN Router 1.3.0 Build 20230322 Rel.70591 PPTP Client os command injection (TALOS-2023-1853)	A vulnerability which was classified as critical was found in TP-LINK ER7206 Omada Gigabit VPN Router 1.3.0 Build 20230322 Rel.70591. Affected is an unknown function of the component PPTP Client. The manipulation leads to os command injection. This vulnerability is traded as CVE-2023-36498. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-47617	TP-Link ER7206 Omada Gigabit VPN Router 1.3.0 Build 20230322 Rel.70591 Web Group Member os command injection (TALOS-2023-1858)	A vulnerability was found in TP-Link ER7206 Omada Gigabit VPN Router 1.3.0 Build 20230322 Rel.70591. It has been rated as critical. This issue affects some unknown processing of the component Web Group Member Handler. The manipulation leads to os command injection. The identification of this vulnerability is CVE-2023-47617. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-43482	TP-LINK ER7206 Omada Gigabit VPN Router 1.3.0 Build 20230322 Rel.70591 Guest Resource os command injection (TALOS-2023-1850)	A vulnerability which was classified as critical has been found in TP-LINK ER7206 Omada Gigabit VPN Router 1.3.0 Build 20230322 Rel.70591. This issue affects some unknown processing of the component Guest Resource. The manipulation leads to os command injection. The identification of this vulnerability is CVE-2023-43482. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-46683	TP-Link ER7206 Omada Gigabit VPN Router 1.3.0 Build 20230322 Rel.70591 Wireguard VPN os command injection (TALOS-2023-1857)	A vulnerability was found in TP-Link ER7206 Omada Gigabit VPN Router 1.3.0 Build 20230322 Rel.70591 and classified as critical. Affected by this issue is some unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		functionality of the component Wireguard VPN. The manipulation leads to os command injection. This vulnerability is handled as CVE-2023-46683. The attack may be launched remotely. There is no exploit available.		
CVE-2023-42664	TP-Link ER7206 Omada Gigabit VPN Router 1.3.0 Build 20230322 Rel.70591 PPTP Global Configuration os command injection (TALOS-2023-1856)	A vulnerability has been found in TP-Link ER7206 Omada Gigabit VPN Router 1.3.0 Build 20230322 Rel.70591 and classified as critical. Affected by this vulnerability is an unknown functionality of the component PPTP Global Configuration. The manipulation leads to os command injection. This vulnerability is known as CVE-2023-42664. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-47167	TP-Link ER7206 Omada Gigabit VPN Router 1.3.0 Build 20230322 Rel.70591 GRE Policy os command injection (TALOS-2023-1855)	A vulnerability was found in TP-Link ER7206 Omada Gigabit VPN Router 1.3.0 Build 20230322 Rel.70591. It has been classified as critical. This affects an unknown part of the component GRE Policy Handler. The manipulation leads to os command injection. This vulnerability is uniquely identified as CVE-2023-47167. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-47209	TP-Link ER7206 Omada Gigabit VPN Router 1.3.0 Build 20230322 Rel.70591 IPsec Policy os command injection (TALOS-2023-1854)	A vulnerability was found in TP-Link ER7206 Omada Gigabit VPN Router 1.3.0 Build 20230322 Rel.70591. It has been declared as critical. This vulnerability affects unknown code of the component IPsec Policy. The manipulation leads to os command injection. This vulnerability was named CVE-2023-47209. The attack can be initiated remotely.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		There is no exploit available.		
CVE-2023-47618	TP-Link ER7206 Omada Gigabit VPN Router 1.3.0 Build 20230322 Rel.70591 Web Filtering os command injection (TALOS-2023-1859)	A vulnerability classified as critical has been found in TP-Link ER7206 Omada Gigabit VPN Router 1.3.0 Build 20230322 Rel.70591. Affected is an unknown function of the component Web Filtering. The manipulation leads to os command injection. This vulnerability is traded as CVE-2023-47618. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-23749	KiTTY up to 0.76.1.13 filename command injection (ID 177031)	A vulnerability was found in KiTTY up to 0.76.1.13. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation of the argument filename leads to command injection. This vulnerability is known as CVE-2024-23749. The attack needs to be initiated within the local network. There is no exploit available.	Patched by core rule	Y

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-6946	Autotitle Plugin up to 1.0.3 on WordPress Setting cross-site request forgery	A vulnerability has been found in Autotitle Plugin up to 1.0.3 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-6946. The attack can be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2023-6391	Custom User CSS Plugin up to 0.2 on WordPress Setting cross-site request forgery	A vulnerability was found in Custom User CSS Plugin up to 0.2 on WordPress. It has been rated as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-6391. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2023-51813	Free Open-Source Inventory Management System 1.0 index.php staff_list cross-site request forgery	A vulnerability which was classified as problematic was found in Free Open-Source Inventory Management System 1.0. This affects an unknown part of the file index.php. The manipulation of the argument staff_list leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-51813. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-22939	FlyCMS 1.0 category_edit cross-site request forgery	A vulnerability which was classified as problematic has been found in FlyCMS 1.0. This issue affects some unknown processing of the file system/article/category_edit. The manipulation leads to cross-site	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		request forgery. The identification of this vulnerability is CVE-2024-22939. The attack may be initiated remotely. There is no exploit available.		
CVE-2024-24470	flusity CMS 2.33 update_post.php cross-site request forgery	A vulnerability classified as problematic has been found in flusity CMS 2.33. This affects an unknown part of the file update_post.php. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2024-24470. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-24524	flusity CMS 2.33 add_menu.php cross-site request forgery	A vulnerability was found in flusity CMS 2.33. It has been declared as problematic. This vulnerability affects unknown code of the file add_menu.php. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2024-24524. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-24469	flusity CMS 2.33 delete_post.php cross-site request forgery	A vulnerability was found in flusity CMS 2.33. It has been declared as problematic. This vulnerability affects unknown code of the file delete_post.php. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2024-24469. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-24468	flusity CMS 2.33 add_customblock.php cross-site request forgery	A vulnerability was found in flusity CMS 2.33. It has been rated as problematic. This issue affects some unknown processing of the file add_customblock.php. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		2024-24468. The attack may be initiated remotely. There is no exploit available.		
CVE-2024-24593	Allegro AI ClearML prior 1.14.2 Html cross-site request forgery	A vulnerability was found in Allegro AI ClearML. It has been classified as problematic. This affects an unknown part of the component Html Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2024-24593. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	N
CVE-2023-47020	NCR Terminal Handler up to 1.5.1 WSDL cross-site request forgery	A vulnerability classified as problematic was found in NCR Terminal Handler up to 1.5.1. This vulnerability affects unknown code of the component WSDL. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-47020. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-24820	Icinga icingaweb2-module-director cross-site request forgery (GHSA-3mwp-5p5v-j6q3)	A vulnerability was found in Icinga icingaweb2-module-director and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-24820. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	N
CVE-2024-25417	flusity CMS 2.33 add_translation.php cross-site request forgery	A vulnerability was found in flusity CMS 2.33. It has been declared as problematic. Affected by this vulnerability is an unknown functionality	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the file /core/tools/add_translation.php. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2024-25417. The attack can be launched remotely. There is no exploit available.		
CVE-2024-25418	flusity CMS 2.33 delete_menu.php cross-site request forgery	A vulnerability was found in flusity CMS 2.33. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /core/tools/delete_menu.php. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2024-25418. The attack may be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-25419	flusity CMS 2.33 update_menu.php cross-site request forgery	A vulnerability classified as problematic has been found in flusity CMS 2.33. This affects an unknown part of the file /core/tools/update_menu.php. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2024-25419. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	N

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-23822	sni Thruk up to 3.11 File Upload path traversal (GHSA-4mrh-mx7x-rqjx)	A vulnerability which was classified as critical has been found in sni Thruk up to 3.11. This issue affects some unknown processing of the component File Upload. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2024-23822. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-24565	CrateDB 5.3.9/5.4.8/5.5.4/5.6.1 COPY FROM path traversal (GHSA-475g-vj6c-xf96)	A vulnerability was found in CrateDB 5.3.9/5.4.8/5.5.4/5.6.1. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component COPY FROM Handler. The manipulation leads to path traversal. This vulnerability is known as CVE-2024-24565. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-22523	Qiyu iFair up to 23.8_ad0 uploadimage path traversal	A vulnerability classified as critical was found in Qiyu iFair up to 23.8_ad0. This vulnerability affects the function uploadimage. The manipulation leads to path traversal.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability was named CVE-2024-22523. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-23334	aio-libs aiohttp up to 3.9.1 Symbolic Links path traversal (GHSA-5h86-8mv2-jq9f)	A vulnerability classified as problematic has been found in aio-libs aiohttp up to 3.9.1. Affected is an unknown function of the component Symbolic Links Handler. The manipulation leads to path traversal. This vulnerability is traded as CVE-2024-23334. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-24569	pixee java-security-toolkit up to 1.1.1 path traversal (GHSA-qh4g-4m4w-jgv2)	A vulnerability was found in pixee java-security-toolkit up to 1.1.1. It has been classified as critical. Affected is an unknown function. The manipulation leads to path traversal. This vulnerability is traded as CVE-2024-24569. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-24756	Crafatar up to 2.1.4 Skin lib/public/ path traversal (GHSA-5cxq-25mp-q5f2)	A vulnerability has been found in Crafatar up to 2.1.4 and classified as critical. This vulnerability affects unknown code in the library lib/public/ of the component Skin	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Handler. The manipulation leads to path traversal. This vulnerability was named CVE-2024-24756. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-24161	MRCMS 3.0 /admin/file/edit.do path path traversal	A vulnerability which was classified as critical was found in MRCMS 3.0. Affected is an unknown function of the file /admin/file/edit.do. The manipulation of the argument path leads to path traversal. This vulnerability is traded as CVE-2024-24161. Access to the local network is required for this attack. There is no exploit available.	Patched by core rule	Y
CVE-2024-22779	Kihron ServerRPExposer up to 1.0.2 ServerResourcePackProviderMixin.java loadServerPack path traversal	A vulnerability was found in Kihron ServerRPExposer up to 1.0.2. It has been declared as critical. This vulnerability affects the function loadServerPack of the file ServerResourcePackProviderMixin.java. The manipulation leads to path traversal. This vulnerability was named CVE-2024-22779. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-24482	Aprktool up to 2.9.2 on Windows path traversal (GHSA-vgwr-4w3p-xmjv)	A vulnerability which was classified as critical has been found in Aprktool up to 2.9.2 on Windows. This issue affects some unknown processing. The manipulation leads to path traversal: &039;../filedir&039;. The identification of this vulnerability is CVE-2024-24482. The attack needs to be initiated within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2023-52138	mate-desktop engrampa path traversal (GHSA-c98h-v39w-3r7v)	A vulnerability classified as critical has been found in mate-desktop engrampa. This affects an unknown part. The manipulation leads to path traversal: &039;/../filedir&039;. This vulnerability is uniquely identified as CVE-2023-52138. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y
CVE-2024-24398	Stimulsoft Dashboard.JS prior 2024.1.2 Save fileName path traversal	A vulnerability was found in Stimulsoft Dashboard.JS and classified as critical. This issue affects the function Save. The manipulation of the argument fileName leads to path traversal. The identification of this vulnerability is CVE-2024-24398. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-24591	Allegro AI ClearML 1.4.0 path traversal	A vulnerability was found in Allegro AI ClearML 1.4.0. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2024-24591. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-0964	gradio API Request path traversal	A vulnerability was found in gradio. It has been classified as critical. This affects an unknown part of the component API Request Handler. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2024-0964. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y
CVE-2024-1708	ConnectWise ScreenConnect up to 23.9.7 path traversal	A vulnerability was found in ConnectWise ScreenConnect up to 23.9.7. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to path	Patched by core rule	no coverage need to check product specific

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		traversal. The identification of this vulnerability is CVE-2024-1708. The attack may be initiated remotely. There is no exploit available.		

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-22550	ShopSite 14.0 SVG File /alsdemo/ss/mediam.cgi unrestricted upload (ID 176312)	A vulnerability has been found in ShopSite 14.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /alsdemo/ss/mediam.cgi of the component SVG File Handler. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2024-22550. The attack needs to be initiated within the local network. There is no exploit available.	Patched by custom rule	N
CVE-2024-0939	Beijing Baichuo Smart S210 Management Platform up to 20240117 /Tool/uploadfile.php file_upload unrestricted upload	A vulnerability has been found in Beijing Baichuo Smart S210 Management Platform up to 20240117 and classified as critical. This vulnerability affects unknown code of the file /Tool/uploadfile.php. The manipulation of the argument file_upload leads to unrestricted upload. This vulnerability was named CVE-2024-0939. The attack can be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by custom rule	N
CVE-2024-1008	SourceCodester Employee Management System 1.0 Profile Page edit-photo.php unrestricted upload	A vulnerability was found in SourceCodester Employee Management System 1.0. It has been	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		declared as critical. Affected by this vulnerability is an unknown functionality of the file edit-photo.php of the component Profile Page. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2024-1008. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2023-31505	Schlix CMS 2.2.8-1 unrestricted upload	A vulnerability classified as critical was found in Schlix CMS 2.2.8-1. Affected by this vulnerability is an unknown functionality. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2023-31505. The attack can be launched remotely. There is no exploit available.	Patched by custom rule	N
CVE-2023-31505	Schlix CMS 2.2.8-1 unrestricted upload	A vulnerability classified as critical was found in Schlix CMS 2.2.8-1. Affected by this vulnerability is an unknown functionality. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2023-31505. The attack can be launched remotely. There is no exploit available.	Patched by custom rule	N
CVE-2024-24059	springboot-manager 1.6 unrestricted upload	A vulnerability classified as problematic has been found in springboot-manager 1.6. Affected is an unknown function. The manipulation leads to unrestricted	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		upload. This vulnerability is traded as CVE-2024-24059. The attack can only be initiated within the local network. There is no exploit available.		
CVE-2021-4436	3DPrint Lite Plugin up to 1.9.1.4 on WordPress p3dlite_handle_upload unrestricted upload	A vulnerability which was classified as problematic has been found in 3DPrint Lite Plugin up to 1.9.1.4 on WordPress. Affected by this issue is the function p3dlite_handle_upload. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2021-4436. The attack can only be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Patched by custom rule	N
CVE-2024-22567	MCMS 5.3.5 HTTP POST Request /ms/file/upload.do unrestricted upload	A vulnerability classified as problematic was found in MCMS 5.3.5. This vulnerability affects unknown code of the file /ms/file/upload.do of the component HTTP POST Request Handler. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2024-22567. The attack needs to be done within the local network. There is no exploit available.	Patched by custom rule	N
CVE-2024-1253	Beijing Baichuo Smart S40 Management Platform up to 20240126 Import	A vulnerability which was classified as critical has been found in Beijing Baichuo Smart S40	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	/useratte/web.php file_upload unrestricted upload	Management Platform up to 20240126. Affected by this issue is some unknown functionality of the file /useratte/web.php of the component Import Handler. The manipulation of the argument file_upload leads to unrestricted upload. This vulnerability is handled as CVE-2024-1253. The attack may be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-24350	Software Publico e-Sic Livre up to 2.0 unrestricted upload	A vulnerability classified as critical was found in Software Publico e-Sic Livre up to 2.0. Affected by this vulnerability is an unknown functionality. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2024-24350. The attack can be launched remotely. There is no exploit available.	Patched by custom rule	N
CVE-2024-24202	ZenTao Community Edition/Biz/Max TXT File /upgrade/control.php unrestricted upload	A vulnerability has been found in ZenTao Community Edition Biz and Max and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /upgrade/control.php of the component TXT File Handler. The manipulation leads to	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unrestricted upload. This vulnerability is known as CVE-2024-24202. Access to the local network is required for this attack to succeed. There is no exploit available.		
CVE-2024-24498	Employee Management System 1.0 edit-photo.php unrestricted upload	A vulnerability was found in Employee Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file edit-photo.php. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2024-24498. The attack may be launched remotely. There is no exploit available.	Patched by custom rule	N
CVE-2024-24393	Pichome 1.1.01 POST Request index.php unrestricted upload (Issue 24)	A vulnerability which was classified as critical has been found in Pichome 1.1.01. This issue affects some unknown processing of the file index.php of the component POST Request Handler. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2024-24393. The attack may be initiated remotely. There is no exploit available.	Patched by custom rule	N

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-0941	Novel-Plus 4.3.0-RC1 /novel/bookComment/list sort sql injection	A vulnerability was found in Novel-Plus 4.3.0-RC1 and classified as critical. This issue affects some unknown processing of the file /novel/bookComment/list. The manipulation of the argument sort leads to sql injection. The identification of this vulnerability is CVE-2024-0941. The attack needs to be done within the local network. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-0938	Tongda OA 2017 up to 11.9 delete_webmail.php WEBBODY_ID_STR sql injection	A vulnerability which was classified as critical was found in Tongda OA 2017 up to 11.9. This affects an unknown part of the file /general/email/inbox/delete_webmail.php. The manipulation of the argument WEBBODY_ID_STR leads to sql injection. This vulnerability is uniquely identified as CVE-2024-0938. The attack can only be done within the local network. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way. It is recommended to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		upgrade the affected component.		
CVE-2024-1007	SourceCodester Employee Management System 1.0 edit_profile.php txtfullname sql injection	A vulnerability was found in SourceCodester Employee Management System 1.0. It has been classified as critical. Affected is an unknown function of the file edit_profile.php. The manipulation of the argument txtfullname leads to sql injection. This vulnerability is traded as CVE-2024-1007. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-24139	SourceCodester Login System with Email Verification 1.0 user sql injection	A vulnerability was found in SourceCodester Login System with Email Verification 1.0. It has been declared as critical. This vulnerability affects unknown code. The manipulation of the argument user leads to sql injection. This vulnerability was named CVE-2024-24139. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-1009	SourceCodester Employee Management System 1.0 /Admin/login.php txtusername sql injection	A vulnerability was found in SourceCodester Employee Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /Admin/login.php. The manipulation of the argument txtusername leads to sql injection.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is handled as CVE-2024-1009. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-24141	SourceCodester School Task Manager App 1.0 task sql injection	A vulnerability was found in SourceCodester School Task Manager App 1.0. It has been classified as critical. Affected is an unknown function. The manipulation of the argument task leads to sql injection. This vulnerability is traded as CVE-2024-24141. Access to the local network is required for this attack. There is no exploit available.	Patched by core rule	Y
CVE-2024-24140	SourceCodester Daily Habit Tracker App 1.0 tracker sql injection	A vulnerability was found in SourceCodester Daily Habit Tracker App 1.0 and classified as critical. This issue affects some unknown processing. The manipulation of the argument tracker leads to sql injection. The identification of this vulnerability is CVE-2024-24140. The attack needs to be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-1012	Wanhu ezOFFICE 11.1.0 wf_printnum.jsp recordId sql injection	A vulnerability which was classified as critical has been found in Wanhu ezOFFICE 11.1.0. This issue affects some unknown processing of the file defaultroot/platform/bpm/work_flow/operate/wf_printnum.jsp. The manipulation of the argument recordId leads to sql injection.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The identification of this vulnerability is CVE-2024-1012. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-1061	HTML5 Video Player Plugin up to 2.5.24 on WordPress get_view id sql injection	A vulnerability classified as critical has been found in HTML5 Video Player Plugin up to 2.5.24 on WordPress. Affected is the function get_view. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-1061. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-24572	WillyXJ facileManager up to 4.5.0 Parameter admin-logs.php extract $_REQUEST sql injection (GHSA-xw34-8pj6-75gc)	A vulnerability classified as critical was found in WillyXJ facileManager up to 4.5.0. Affected by this vulnerability is the function extract of the file admin-logs.php of the component Parameter Handler. The manipulation of the argument $_REQUEST leads to sql injection. This vulnerability is known as CVE-2024-24572. The attack can be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y
CVE-2022-47072	Sparx Enterprise Architect 16.0.1605 on 32-bit Select Classifier Dialog Box	A vulnerability which was classified as critical was found in Sparx Enterprise Architect	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Find sql injection	16.0.1605 on 32-bit. Affected is an unknown function of the component Select Classifier Dialog Box. The manipulation of the argument Find leads to sql injection. This vulnerability is traded as CVE-2022-47072. The attack can only be initiated within the local network. There is no exploit available.		
CVE-2024-24029	JFinalCMS 5.0.0 /admin/content/data sql injection	A vulnerability which was classified as critical was found in JFinalCMS 5.0.0. This affects an unknown part of the file /admin/content/data. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2024-24029. Access to the local network is required for this attack to succeed. There is no exploit available.	Patched by core rule	Y
CVE-2024-22108	GTB Central Console 15.17.1-30814.NG CCApi.class.php sql injection	A vulnerability has been found in GTB Central Console 15.17.1-30814.NG and classified as critical. This vulnerability affects unknown code in the library /opt/webapp/lib/PureApi/CCApi.class.php. The manipulation leads to sql injection. This vulnerability was named CVE-2024-22108. The attack needs to be done within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-1251	Tongda OA 2017 up to 11.10 delete.php DELETE_STR sql	A vulnerability classified as critical has been found in Tongda	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	OA 2017 up to 11.10. Affected is an unknown function of the file /general/email/outbox/delete.php. The manipulation of the argument DELETE_STR leads to sql injection. This vulnerability is traded as CVE-2024-1251. The attack needs to be done within the local network. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2023-51951	Stock Management System 1.0 manage_bo.php id sql injection (WLX-2023-004)	A vulnerability classified as critical was found in Stock Management System 1.0. This vulnerability affects unknown code of the file manage_bo.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-51951. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-1252	Tongda OA 2017 up to 11.9 delete.php ASK_DUTY_ID sql injection	A vulnerability classified as critical was found in Tongda OA 2017 up to 11.9. Affected by this vulnerability is an unknown functionality of the file /general/attendance/manage/ask_duty/delete.php. The manipulation of the argument ASK_DUTY_ID leads to sql injection. This vulnerability is known as CVE-2024-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		1252. The attack needs to be initiated within the local network. Furthermore there is an exploit available. It is recommended to upgrade the affected component.		
CVE-2024-24112	xmall 1.1 orderDir sql injection (Issue 78)	A vulnerability classified as critical was found in xmall 1.1. Affected by this vulnerability is an unknown functionality. The manipulation of the argument orderDir leads to sql injection. This vulnerability is known as CVE-2024-24112. Access to the local network is required for this attack to succeed. There is no exploit available.	Patched by core rule	Y
CVE-2024-1254	Beijing Baichuo Smart S20 Management Platform up to 20231120 sysmanageajax.php id sql injection	A vulnerability which was classified as critical was found in Beijing Baichuo Smart S20 Management Platform up to 20231120. This affects an unknown part of the file /sysmanage/sysmanageajax.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-1254. It is possible to initiate the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-24001	jshERP 3.3 findallocationDetail sql injection (Issue 99)	A vulnerability was found in jshERP 3.3. It has been classified as critical. Affected is the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		function findallocationDetail. The manipulation leads to sql injection. This vulnerability is traded as CVE-2024-24001. The attack needs to be initiated within the local network. There is no exploit available.		
CVE-2024-24004	jshERP 3.3 findInOutDetail sql injection (Issue 99)	A vulnerability was found in jshERP 3.3. It has been rated as critical. Affected by this issue is the function findInOutDetail. The manipulation leads to sql injection. This vulnerability is handled as CVE-2024-24004. Access to the local network is required for this attack to succeed. There is no exploit available.	Patched by core rule	Y
CVE-2024-24002	jshERP 3.3 getListWithStock sql injection (Issue 99)	A vulnerability was found in jshERP 3.3. It has been declared as critical. Affected by this vulnerability is the function getListWithStock. The manipulation leads to sql injection. This vulnerability is known as CVE-2024-24002. Access to the local network is required for this attack. There is no exploit available.	Patched by core rule	Y
CVE-2024-24003	jshERP 3.3 com.jsh.erp.controller.DepotHeadController findInOutMaterialCount column/order sql injection (Issue 99)	A vulnerability has been found in jshERP 3.3 and classified as critical. Affected by this vulnerability is the function findInOutMaterialCount of the component com.jsh.erp.controller.DepotHeadController. The manipulation of the argument	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		column/order leads to sql injection. This vulnerability is known as CVE-2024-24003. The attack needs to be done within the local network. There is no exploit available.		
CVE-2024-24499	Employee Management System 1.0 edit_profile.php txtfullname/txtphone sql injection	A vulnerability which was classified as critical was found in Employee Management System 1.0. This affects an unknown part of the file edit_profile.php. The manipulation of the argument txtfullname/txtphone leads to sql injection. This vulnerability is uniquely identified as CVE-2024-24499. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-25308	code-projects Simple School Management System 1.0 School/teacher_login.php name sql injection	A vulnerability classified as critical was found in code-projects Simple School Management System 1.0. Affected by this vulnerability is an unknown functionality of the file School/teacher_login.php. The manipulation of the argument name leads to sql injection. This vulnerability is known as CVE-2024-25308. The attack can only be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-25318	code-projects Hotel Management System 1.0 Hotel/admin/print.php pid sql injection	A vulnerability was found in code-projects Hotel Management System 1.0. It has been classified as critical. Affected is an unknown function of the file Hotel/admin/print.php.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The manipulation of the argument pid leads to sql injection. This vulnerability is traded as CVE-2024-25318. The attack needs to be approached within the local network. There is no exploit available.		
CVE-2024-25315	code-projects Hotel Management System 1.0 Hotel/admin/roombook.php rid sql injection	A vulnerability has been found in code-projects Hotel Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file Hotel/admin/roombook.php. The manipulation of the argument rid leads to sql injection. This vulnerability is known as CVE-2024-25315. The attack needs to be approached within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-25304	code-projects Simple School Management System 1.0 School/index.php apass sql injection	A vulnerability was found in code-projects Simple School Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file School/index.php. The manipulation of the argument apass leads to sql injection. The identification of this vulnerability is CVE-2024-25304. The attack needs to be approached within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-24495	Daily Habit Tracker 1.0 GET Request delete-tracker.php sql injection	A vulnerability classified as critical was found in Daily Habit Tracker 1.0. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability affects unknown code of the file delete-tracker.php of the component GET Request Handler. The manipulation leads to sql injection. This vulnerability was named CVE-2024-24495. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-25309	code-projects Simple School Management System 1.0 School/teacher_login.php pass sql injection	A vulnerability which was classified as critical has been found in code-projects Simple School Management System 1.0. Affected by this issue is some unknown functionality of the file School/teacher_login.php. The manipulation of the argument pass leads to sql injection. This vulnerability is handled as CVE-2024-25309. The attack needs to be done within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-25307	code-projects Cinema Seat Reservation System 1.0 booking.php id sql injection	A vulnerability was found in code-projects Cinema Seat Reservation System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /Cinema-Reservation/booking.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2024-25307. The attack can only be done within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-25316	code-projects Hotel	A vulnerability was	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Management System 1.0 usersettingdel.php eid sql injection	found in code-projects Hotel Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file Hotel/admin/usersettingdel.php. The manipulation of the argument eid leads to sql injection. This vulnerability is handled as CVE-2024-25316. The attack can only be done within the local network. There is no exploit available.	core rule	
CVE-2024-24497	Employee Management System 1.0 login.php txtusername/txtpassword sql injection	A vulnerability was found in Employee Management System 1.0 and classified as critical. This issue affects some unknown processing of the file login.php. The manipulation of the argument txtusername/txtpassword leads to sql injection. The identification of this vulnerability is CVE-2024-24497. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-25314	code-projects Hotel Management System 1.0 Hotel/admin/show.php sid sql injection	A vulnerability which was classified as critical was found in code-projects Hotel Management System 1.0. Affected is the function Hotel of the file Hotel/admin/show.php. The manipulation of the argument sid leads to sql injection. This vulnerability is traded as CVE-2024-25314. Access to the local network is required for this attack	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to succeed. There is no exploit available.		
CVE-2024-25302	SourceCodester Event Student Attendance System 1.0 student sql injection	A vulnerability which was classified as critical has been found in SourceCodester Event Student Attendance System 1.0. This issue affects some unknown processing. The manipulation of the argument student leads to sql injection. The identification of this vulnerability is CVE-2024-25302. Access to the local network is required for this attack. There is no exploit available.	Patched by core rule	Y
CVE-2024-25312	code-projects Simple School Management System 1.0 School/sub_delete.php id sql injection	A vulnerability classified as critical has been found in code-projects Simple School Management System 1.0. This affects an unknown part of the file School/sub_delete.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-25312. The attack needs to be done within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-25306	code-projects Simple School Management System 1.0 School/index.php aname sql injection	A vulnerability which was classified as critical was found in code-projects Simple School Management System 1.0. This affects an unknown part of the file School/index.php. The manipulation of the argument aname leads to sql injection. This vulnerability is uniquely identified as CVE-2024-25306. The attack needs to be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		initiated within the local network. There is no exploit available.		
CVE-2024-25310	code-projects Simple School Management System 1.0 School/delete.php id sql injection	A vulnerability was found in code-projects Simple School Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file School/delete.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-25310. The attack can only be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-23763	Gambio up to 4.9.2.0 GET Request modifiers[attribute][] sql injection (usd-2023-0047)	A vulnerability was found in Gambio up to 4.9.2.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component GET Request Handler. The manipulation of the argument modifiers[attribute][] leads to sql injection. This vulnerability is known as CVE-2024-23763. The attack needs to be approached within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-1071	Ultimate Member Plugin 2.1.3/2.8.2 on WordPress sql injection	A vulnerability which was classified as critical was found in Ultimate Member Plugin 2.1.3/2.8.2 on WordPress. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2024-1071. The attack needs to be approached within the local network. There is no exploit available.		
CVE-2024-1878	SourceCodester Employee Management System 1.0 /myprofile.php id sql injection	A vulnerability was found in SourceCodester Employee Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /myprofile.php. The manipulation of the argument id with the input 1%20or%2011 leads to sql injection. This vulnerability is handled as CVE-2024-1878. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	need to target, product specific
CVE-2024-1877	SourceCodester Employee Management System 1.0 /cancel.php id sql injection	A vulnerability was found in SourceCodester Employee Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /cancel.php. The manipulation of the argument id with the input 1%20or%2011 leads to sql injection. This vulnerability is known as CVE-2024-1877. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-1876	SourceCodester Employee Management System 1.0 /psubmit.php pid sql injection	A vulnerability was found in SourceCodester Employee Management System 1.0. It has been classified as critical.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Affected is an unknown function of the file /psubmit.php. The manipulation of the argument pid with the input &039;+or+1%3d1%23 leads to sql injection. This vulnerability is traded as CVE-2024-1876. It is possible to launch the attack remotely. Furthermore there is an exploit available.		

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-22551	WhatACart 2.0.7 /site/default/search cross site scripting (ID 176314)	A vulnerability which was classified as problematic was found in WhatACart 2.0.7. Affected is an unknown function of the file /site/default/search. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-22551. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-0948	NetBox up to 3.7.0 Home Page Configuration /core/config-revisions cross site scripting	A vulnerability which was classified as problematic has been found in NetBox up to 3.7.0. This issue affects some unknown processing of the file /core/config-revisions of the component Home Page Configuration. The manipulation with the input <<h1 onloadalert>>test</h1> leads to cross site scripting. The identification of this vulnerability is CVE-2024-0948. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-0958	CodeAstro Stock Management System 1.0 Add Category /index.php Category Name/Category Description cross site scripting	A vulnerability was found in CodeAstro Stock Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/index.php of the component Add Category Handler. The manipulation of the argument Category Name/Category Description leads to cross site scripting. The identification of this vulnerability is CVE-2024-0958. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2023-48202	Sunlight CMS 8.0.1 File Manager cross site scripting	A vulnerability classified as problematic has been found in Sunlight CMS 8.0.1. Affected is an unknown function of the component File Manager. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-48202. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-48201	Sunlight CMS 8.0.1 Content Text Editor cross site scripting	A vulnerability was found in Sunlight CMS 8.0.1. It has been rated as problematic. This issue affects some unknown processing of the component Content Text Editor. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-48201. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-1018	PbootCMS 3.2.5-20230421 name cross site scripting	A vulnerability classified as problematic has been found in PbootCMS 3.2.5-20230421. Affected is an unknown function of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/admin.phpp/Area/indextabt2. The manipulation of the argument name leads to cross site scripting. This vulnerability is traded as CVE-2024-1018. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2024-1020	Rebuild up to 3.5.5 /filex/proxy-download getStorageFile url cross site scripting	A vulnerability classified as problematic was found in Rebuild up to 3.5.5. Affected by this vulnerability is the function getStorageFile of the file /filex/proxy-download. The manipulation of the argument url leads to cross site scripting. This vulnerability is known as CVE-2024-1020. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-1022	CodeAstro Simple Student Result Management System 5.6 Add Class Page /add_classes.php Class Name cross site scripting	A vulnerability which was classified as problematic was found in CodeAstro Simple Student Result Management System 5.6. This affects an unknown part of the file /add_classes.php of the component Add Class Page. The manipulation of the argument Class Name leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-1022. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-1010	SourceCodester Employee	A vulnerability classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Management System 1.0 edit-profile.php cross site scripting	problematic has been found in SourceCodester Employee Management System 1.0. This affects an unknown part of the file edit-profile.php. The manipulation of the argument fullname/phone/date of birth/address/date of appointment leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-1010. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-24136	SourceCodester Math Game with Leaderboard 1.0 Score Section Your Name cross site scripting	A vulnerability classified as problematic has been found in SourceCodester Math Game with Leaderboard 1.0. This affects an unknown part of the component Score Section. The manipulation of the argument Your Name leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-24136. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-24134	SourceCodester Online Food Menu 1.0 Update Menu Section Menu Name/Description cross site scripting	A vulnerability classified as problematic was found in SourceCodester Online Food Menu 1.0. This vulnerability affects unknown code of the component Update Menu Section. The manipulation of the argument Menu Name/Description leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability was named CVE-2024-24134. The attack can be initiated remotely. There is no exploit available.		
CVE-2023-7225	MapPress Plugin up to 2.88.16 on WordPress Map Setting cross site scripting	A vulnerability has been found in MapPress Plugin up to 2.88.16 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Map Setting Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-7225. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-22559	LightCMS 2.0 Content Management Articles cross site scripting (Issue 34)	A vulnerability was found in LightCMS 2.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Content Management. The manipulation of the argument Articles leads to cross site scripting. This vulnerability is known as CVE-2024-22559. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-5124	Page Builder Plugin up to 1.7.x on WordPress cross site scripting	A vulnerability was found in Page Builder Plugin up to 1.7.x on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is handled as CVE-2023-5124. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-6165	Restrict Usernames Emails Characters Plugin up to 3.1.3 on WordPress Setting cross site scripting	A vulnerability classified as problematic was found in Restrict Usernames Emails Characters Plugin up to 3.1.3 on WordPress. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-6165. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2023-5943	Wp-Adv-Quiz Plugin up to 1.0.2 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic has been found in Wp-Adv-Quiz Plugin up to 1.0.2 on WordPress. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-5943. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-6278	Biteship Plugin up to 2.2.24 on WordPress biteship_error/biteship_message cross site scripting	A vulnerability which was classified as problematic was found in Biteship Plugin up to 2.2.24 on WordPress. Affected is an unknown function. The manipulation of the argument biteship_error/biteship_message leads to cross site scripting. This vulnerability is traded as CVE-2023-6278. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-24135	SourceCodester Product Inventory with Export to Excel 1.0 Add Product Product Name/Product Code cross site scripting	A vulnerability has been found in SourceCodester Product Inventory with Export to Excel 1.0 and classified as problematic. This vulnerability affects unknown code of the component Add Product. The manipulation of the argument Product Name/Product Code leads to cross site scripting. This vulnerability was named CVE-2024-24135. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-7200	EventON Plugin up to 4.4.0 on WordPress cross site scripting	A vulnerability classified as problematic was found in EventON Plugin up to 4.4.0 on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is known as CVE-2023-7200. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-5956	Wp-Adv-Quiz Plugin up to 1.0.2 on WordPress Setting cross site scripting	A vulnerability was found in Wp-Adv-Quiz Plugin up to 1.0.2 on WordPress. It has been classified as problematic. This affects an unknown part of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-5956. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-1099	Rebuild up to 3.5.5 /filex/read-raw getFileOfData url cross site scripting	A vulnerability was found in Rebuild up to 3.5.5. It has been classified as problematic. Affected is the function getFileOfData of the file /filex/read-raw. The manipulation of the argument url leads to cross site scripting. This vulnerability is traded as CVE-2024-1099. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-22569	POSCMS 4.6.2 index.php cross site scripting	A vulnerability classified as problematic has been found in POSCMS 4.6.2. Affected is an unknown function of the file /index.phpcinstall&mindex&step2&is_install_db0. The manipulation leads to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross site scripting. This vulnerability is traded as CVE-2024-22569. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2023-7167	Persian Fonts Plugin up to 1.6 on WordPress cross site scripting	A vulnerability has been found in Persian Fonts Plugin up to 1.6 on WordPress and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-7167. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-1103	CodeAstro Real Estate Management System 1.0 Feedback Form profile.php Your Feedback cross site scripting	A vulnerability was found in CodeAstro Real Estate Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file profile.php of the component Feedback Form. The manipulation of the argument Your Feedback with the input <img srcx onerroralert> leads to cross site scripting. This vulnerability is handled as CVE-2024-1103. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-22569	POSCMS 4.6.2 index.php cross site scripting	A vulnerability classified as problematic has been found in POSCMS 4.6.2. Affected is an unknown function of the file /index.phpcinstall&am	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		p;mindex&step2&is_install_db0. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-22569. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2024-24570	Statamic CMS up to 3.4.16/4.45.x cross site scripting (GHSA-vqxq-hvxw-9mv9)	A vulnerability was found in Statamic CMS up to 3.4.16/4.45.x. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to basic cross site scripting. The identification of this vulnerability is CVE-2024-24570. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-24945	Travel Journal 1.0 write-journal.php Share Your Moments cross site scripting	A vulnerability has been found in Travel Journal 1.0 and classified as problematic. This vulnerability affects unknown code of the file /travel-journal/write-journal.php. The manipulation of the argument Share Your Moments leads to cross site scripting. This vulnerability was named CVE-2024-24945. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-24041	Travel Journal 1.0 write-journal.php location cross site scripting	A vulnerability which was classified as problematic was found in Travel Journal 1.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This affects an unknown part of the file /travel-journal/write-journal.php. The manipulation of the argument location leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-24041. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-24062	springboot-manager 1.6 /sys/role cross site scripting	A vulnerability was found in springboot-manager 1.6. It has been classified as problematic. Affected is an unknown function of the file /sys/role. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-24062. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-24061	springboot-manager 1.6 /sysContent/add cross site scripting	A vulnerability was found in springboot-manager 1.6 and classified as problematic. This issue affects some unknown processing of the file /sysContent/add. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-24061. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-24060	springboot-manager 1.6 /sys/user cross site scripting	A vulnerability has been found in springboot-manager 1.6 and classified as problematic. This vulnerability affects unknown code of the file /sys/user. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation leads to cross site scripting. This vulnerability was named CVE-2024-24060. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-24571	WillyXJ facileManager up to 4.5.0 cross site scripting (GHSA-h7w3-xv88-2xqj)	A vulnerability which was classified as problematic has been found in WillyXJ facileManager up to 4.5.0. This issue affects some unknown processing. The manipulation leads to basic cross site scripting. The identification of this vulnerability is CVE-2024-24571. The attack may be initiated remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y
CVE-2024-23034	EyouCMS 1.6.5 URL input cross site scripting (Issue 57)	A vulnerability was found in EyouCMS 1.6.5. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component URL Handler. The manipulation of the argument input leads to cross site scripting. This vulnerability is known as CVE-2024-23034. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-22927	EyouCMS 1.6.5 URL func cross site scripting (Issue 57)	A vulnerability which was classified as problematic was found in EyouCMS 1.6.5. This affects an unknown part of the component	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		URL Handler. The manipulation of the argument func leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-22927. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-24160	MRCMS 3.0 saveinfo.do cross site scripting	A vulnerability has been found in MRCMS 3.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/system/saveinfo.do. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-24160. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-1215	SourceCodester CRUD without Page Reload 1.0 fetch_data.php username/city cross site scripting	A vulnerability was found in SourceCodester CRUD without Page Reload 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file fetch_data.php. The manipulation of the argument username/city leads to cross site scripting. This vulnerability is handled as CVE-2024-1215. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-23031	EyouCMS 1.6.5 URL is_water cross site scripting (Issue 57)	A vulnerability was found in EyouCMS 1.6.5. It has been rated as problematic. Affected by this issue is some unknown functionality of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component URL Handler. The manipulation of the argument is_water leads to cross site scripting. This vulnerability is handled as CVE-2024-23031. The attack may be launched remotely. There is no exploit available.		
CVE-2024-23032	EyouCMS 1.6.5 URL num cross site scripting (Issue 57)	A vulnerability was found in EyouCMS 1.6.5. It has been classified as problematic. Affected is an unknown function of the component URL Handler. The manipulation of the argument num leads to cross site scripting. This vulnerability is traded as CVE-2024-23032. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-46344	Solar-Log Base 15 6.0.1 Build 161 Web Portal #ilang=DE&b=c_smartenergy_swgroups cross site scripting	A vulnerability was found in Solar-Log Base 15 6.0.1 Build 161. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /ilangDE&bc_smartenergy_swgroups of the component Web Portal. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-46344. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-23033	EyouCMS up to 1.6.4 URL path cross site scripting (Issue 57)	A vulnerability was found in EyouCMS up to 1.6.4 and classified as problematic. This issue affects some	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown processing of the component URL Handler. The manipulation of the argument path leads to cross site scripting. The identification of this vulnerability is CVE-2024-23033. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-21485	ploty dash prior 2.0.16/2.13.0/2.15.0 cross site scripting (Issue 2729)	A vulnerability was found in ploty dash. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-21485. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-24388	XunRuiCMS up to 4.6.2 Background Login cross site scripting	A vulnerability has been found in XunRuiCMS up to 4.6.2 and classified as problematic. This vulnerability affects unknown code of the component Background Login. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-24388. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-49950	Logpoint SIEM up to 7.2.x Jinja Template cross site scripting	A vulnerability was found in Logpoint SIEM up to 7.2.x and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		classified as problematic. This issue affects some unknown processing of the component Jinja Template Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-49950. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-24397	Stimulsoft Dashboard.JS prior 2024.1.2 ReportName cross site scripting	A vulnerability was found in Stimulsoft Dashboard.JS. It has been classified as problematic. This affects an unknown part. The manipulation of the argument ReportName leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-24397. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-1265	CodeAstro University Management System 1.0 Attendance Management /att_add.php Student Name cross site scripting	A vulnerability classified as problematic has been found in CodeAstro University Management System 1.0. Affected is an unknown function of the file /att_add.php of the component Attendance Management. The manipulation of the argument Student Name leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is traded as CVE-2024-1265. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2024-1269	SourceCodester Product Management System 1.0 /supplier.php supplier_name/supplier_contact cross site scripting	A vulnerability has been found in SourceCodester Product Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /supplier.php. The manipulation of the argument supplier_name/supplier_contact leads to cross site scripting. This vulnerability was named CVE-2024-1269. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-24594	Allegro AI ClearML Debug Samples Tab cross site scripting	A vulnerability classified as problematic has been found in Allegro AI ClearML. Affected is an unknown function of the component Debug Samples Tab. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-24594. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-1106	Shariff Wrapper Plugin up to 4.6.9 on WordPress cross site scripting	A vulnerability was found in Shariff Wrapper Plugin up to 4.6.9 on WordPress. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is uniquely identified as CVE-2024-1106. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-1266	CodeAstro University Management System 1.0 Student Registration Form /st_reg.php Address cross site scripting	A vulnerability classified as problematic was found in CodeAstro University Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /st_reg.php of the component Student Registration Form. The manipulation of the argument Address leads to cross site scripting. This vulnerability is known as CVE-2024-1266. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-24574	thorsten phpMyFAQ up to 3.2.4 Echo attachments.php filename cross site scripting (GHSA-7m8g-fprr-47fx)	A vulnerability was found in thorsten phpMyFAQ up to 3.2.4 and classified as problematic. This issue affects some unknown processing of the file phpMyFAQ\phpmyfaq\admin\attachments.php of the component Echo Handler. The manipulation of the argument filename leads to cross site scripting. The identification of this vulnerability is CVE-2024-24574. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-24396	Stimulsoft Dashboard.JS prior	A vulnerability was found in Stimulsoft	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	2024.1.2 Search Bar cross site scripting	Dashboard.JS. It has been classified as problematic. This affects an unknown part of the component Search Bar. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-24396. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-1257	Jspxcms 10.2.0 find_text.do cross site scripting	A vulnerability was found in Jspxcms 10.2.0. It has been classified as problematic. Affected is an unknown function of the file /ext/collect/find_text.do. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-1257. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-1256	Jspxcms 10.2.0 filter_text.do cross site scripting	A vulnerability was found in Jspxcms 10.2.0 and classified as problematic. This issue affects some unknown processing of the file /ext/collect/filter_text.do. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-1256. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-24130	Mail2World v12	A vulnerability has	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Business Control Center resellercenter/login.asp Usr cross site scripting	been found in Mail2World v12 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file resellercenter/login.asp of the component Business Control Center. The manipulation of the argument Usr leads to cross site scripting. This vulnerability is known as CVE-2024-24130. The attack can be launched remotely. There is no exploit available.	core rule	
CVE-2024-24131	SuperWebMailer 9.31.0.01799 api.php cross site scripting	A vulnerability which was classified as problematic has been found in SuperWebMailer 9.31.0.01799. This issue affects some unknown processing of the file api.php. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-24131. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-24115	Cotonti CMS 0.9.24 Edit Page cross site scripting	A vulnerability which was classified as problematic has been found in Cotonti CMS 0.9.24. This issue affects some unknown processing of the component Edit Page. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-24115. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-25365	October CMS 3.2.0	A vulnerability was	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	MP3 File cross site scripting	found in October CMS 3.2.0. It has been classified as problematic. Affected is an unknown function of the component MP3 File Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-25365. It is possible to launch the attack remotely. There is no exploit available.	core rule	
CVE-2024-24494	Daily Habit Tracker 1.0 add-tracker.php cross site scripting	A vulnerability was found in Daily Habit Tracker 1.0. It has been classified as problematic. Affected is an unknown function of the file add-tracker.php. The manipulation of the argument day/exercise/pray/read_book/vitamins/laundry/alcohol/meat leads to cross site scripting. This vulnerability is traded as CVE-2024-24494. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-39683	EasyEmail up to 4.12.2 cross site scripting	A vulnerability which was classified as problematic was found in EasyEmail up to 4.12.2. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-39683. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-31506	Grav up to 1.7.44 ISINDEX Element onmouseover cross site scripting	A vulnerability has been found in Grav up to 1.7.44 and classified as problematic. This vulnerability affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown code of the component ISINDEX Element Handler. The manipulation of the argument onmouseover leads to cross site scripting. This vulnerability was named CVE-2023-31506. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-0604	Best Gallery Plugin up to 2.4.7 on WordPress Setting cross site scripting	A vulnerability classified as problematic was found in Best Gallery Plugin up to 2.4.7 on WordPress. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-0604. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-0559	Enhanced Text Widget Plugin up to 1.6.5 on WordPress cross site scripting	A vulnerability was found in Enhanced Text Widget Plugin up to 1.6.5 on WordPress. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-0559. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-0719	Tabs Shortcode and Widget Plugin up to 1.17 on WordPress cross site scripting	A vulnerability classified as problematic has been found in Tabs Shortcode and Widget Plugin up to 1.17 on WordPress. This affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		an unknown part of the component Shortcode Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-0719. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-1871	SourceCodester Employee Management System 1.0 Project Assignment Report /process/assignp.php pname cross site scripting	A vulnerability which was classified as problematic was found in SourceCodester Employee Management System 1.0. Affected is an unknown function of the file /process/assignp.php of the component Project Assignment Report. The manipulation of the argument pname leads to cross site scripting. This vulnerability is traded as CVE-2024-1871. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	N

Host Header Injection

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-1064	Arcadia Technology Crafty Controller up to 4.2.2 HTTP Host http headers for scripting syntax (Issue 327)	A vulnerability was found in Arcadia Technology Crafty Controller up to 4.2.2. It has been classified as problematic. Affected is an unknown function of the component HTTP Handler. The manipulation of the argument Host leads to improper neutralization of http headers for scripting syntax. This vulnerability is traded as CVE-2024-1064. It is possible to launch the attack remotely. There is no exploit available.	Patched by default in SaaS	Y

XML External Entity Vulnerability

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-52239	Magic xpi Integration Platform 4.13.4 XML Parser onItemImport xml external entity reference	A vulnerability was found in Magic xpi Integration Platform 4.13.4 and classified as problematic. Affected by this issue is the function onItemImport of the component XML Parser. The manipulation leads to xml external entity reference. This vulnerability is handled as CVE-2023-52239. Access to the local network is required for this attack to succeed. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y

Indusface is a leading application security SaaS company that secures critical Web, Mobile & API applications of 5000+ global customers using its award-winning fully managed platform that integrates a web application scanner, web application firewall, DDoS &, BOT Mitigation, CDN, and threat intelligence engine. The company has been funded by Tata Capital Growth Fund, is Great Place to Work certified, mentioned by analysts like Gartner, Forrester, etc. in their reports, and has been the recipient of many awards such as the Economic Times Top 25, NASSCOM DSCI Top Security Company, Deloitte Asia Top 100, and several other such prestigious recognitions.

Indusface is the only cloud WAAP (WAF) vendor with 100% customer recommendation for 3 consecutive years

A Customers' Choice for 2022 and 2023 Gartner® Peer Insights™