INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

January 2024

The total **zero-day vulnerabilities** count for January month: 257

Command Injection	CSRF	Local File Inclusion	SQLi	Malicious File Upload	XML External Entity	Host Header Injection	Cross-site Scripting
21	20	11	72	9	2	2	120

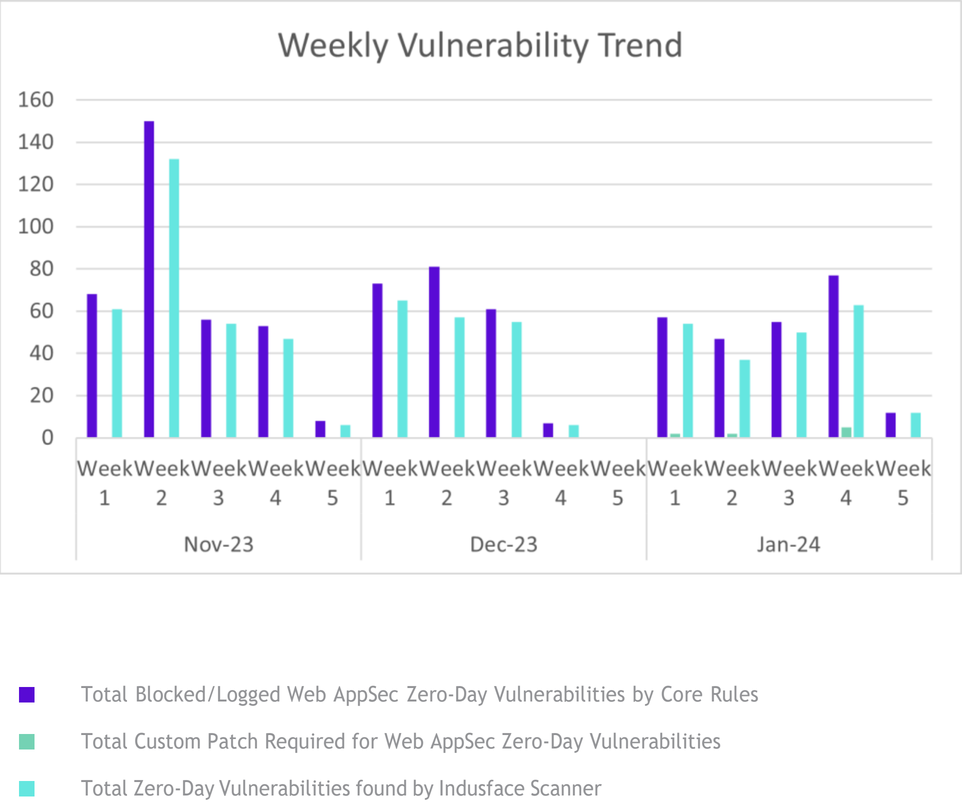
Zero-day vulnerabilities protected through core rules	246
Zero-day vulnerabilities protected through custom rules	9
Zero-day vulnerabilities protected through SaaS rules	2
Zero-day vulnerabilities for which protection cannot be done	0
Zero-day vulnerabilities found by Indusface WAS	216

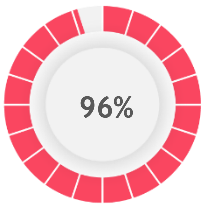
- To enable custom rules, please contact support@indusface.com
- Since the attack vectors are unknown, Indusface cannot determine whether these vulnerabilities are protected.
- Get detailed insights on zero-day vulnerabilities.

Vulnerability Trend:

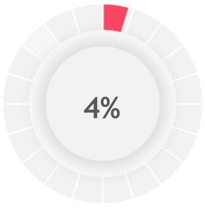
The weekly trend displays the total number of vulnerabilities discovered and the type of protection provided for the last quarter.

Weekly Vulnerability Trend

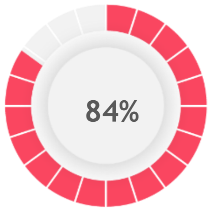




of the zero-day vulnerabilities were protected by the core rules in the last month

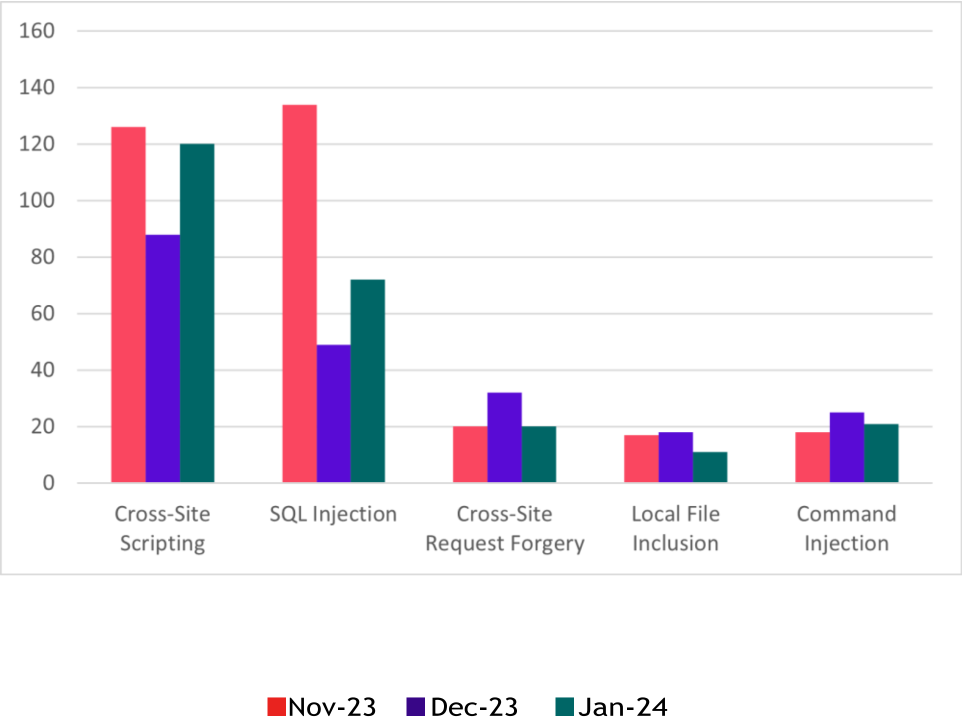


of the zero-day vulnerabilities were protected by the custom rules in the last month



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-2023-51100	Tenda W9 1.0.0.7(4456)_CN formGetDiagnoseInfo command injection	A vulnerability which was classified as critical was found in Tenda W9 1.0.0.7_CN. Affected is the function formGetDiagnoseInfo. The manipulation leads to command injection. This vulnerability is traded as CVE-2023-51100. The attack needs to be approached within the local network. There is no exploit available.	Patched by core rule	N
CVE-2023-51099	Tenda W9 1.0.0.7(4456)_CN formexeCommand command injection	A vulnerability was found in Tenda W9 1.0.0.7_CN. It has been classified as critical. This affects the function formexeCommand. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2023-51099. The attack needs to be done within the local network. There is no exploit available.	Patched by core rule	N
CVE-2023-7116	WeiYe-Jing datax-web 2.1.2 HTTP POST Request /api/log/killJob processId os command injection	A vulnerability which was classified as critical has been found in WeiYe-Jing datax-web 2.1.2. Affected by this issue is some unknown functionality of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/api/log/killJob of the component HTTP POST Request Handler. The manipulation of the argument processId leads to os command injection. This vulnerability is handled as CVE-2023-7116. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2023-51664	tj-actions changed-files up to 40.x Filename command injection (GHSA-mcph-m25j-8j63)	A vulnerability was found in tj-actions changed-files up to 40.x. It has been rated as critical. Affected by this issue is some unknown functionality of the component Filename Handler. The manipulation leads to command injection. This vulnerability is handled as CVE-2023-51664. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2023-50094	reNgine up to 2.0.2 api/tools/waf_detector/ url os command injection	A vulnerability which was classified as critical has been found in reNgine up to 2.0.2. Affected by this issue is some unknown functionality of the file api/tools/waf_detector/. The manipulation of the argument url leads to os command injection. This vulnerability is handled as CVE-2023-50094. 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 core rule	Y
CVE-2024-0291	Totolink LR1200GB 9.1.0u.6619_B20230130 /cgi-bin/cstecgi.cgi UploadFirmwareFile FileName command injection	A vulnerability was found in Totolink LR1200GB 9.1.0u.6619_B20230130. It has been rated as critical. This issue affects the function UploadFirmwareFile of the file /cgi-bin/cstecgi.cgi. The manipulation of the	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument FileName leads to command injection. The identification of this vulnerability is CVE-2024-0291. 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.		
CVE-2024-0294	Totolink LR1200GB 9.1.0u.6619_B20230130 /cgi-bin/cstecgi.cgi setUssd ussd os command injection	A vulnerability which was classified as critical has been found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected by this issue is the function setUssd of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ussd leads to os command injection. This vulnerability is handled as CVE-2024-0294. 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.	Patched by core rule	N
CVE-2024-0297	Totolink N200RE 9.3.5u.6139_B20201216 /cgi-bin/cstecgi.cgi UploadFirmwareFile FileName os command injection	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216 and classified as critical. This issue affects the function UploadFirmwareFile of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument FileName leads to os command injection. The identification of this vulnerability is CVE-2024-0297. 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	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-0293	Totolink LR1200GB 9.1.0u.6619_B20230130 /cgi-bin/cstecgi.cgi setUploadSetting FileName os command injection	A vulnerability classified as critical was found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected by this vulnerability is the function setUploadSetting of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument FileName leads to os command injection. This vulnerability is known as CVE-2024-0293. The attack can be launched 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	N
CVE-2024-0295	Totolink LR1200GB 9.1.0u.6619_B20230130 /cgi-bin/cstecgi.cgi setWanCfg hostName os command injection	A vulnerability which was classified as critical was found in Totolink LR1200GB 9.1.0u.6619_B20230130. This affects the function setWanCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument hostName leads to os command injection. This vulnerability is uniquely identified as CVE-2024-0295. 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	N
CVE-2024-0292	Totolink LR1200GB 9.1.0u.6619_B20230130 /cgi-bin/cstecgi.cgi setOpModeCfg hostName os command injection	A vulnerability classified as critical has been found in Totolink LR1200GB 9.1.0u.6619_B20230130. Affected is the function setOpModeCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument hostName leads to os command injection. This vulnerability is traded as CVE-2024-	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		0292. It is possible to launch the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-0296	Totolink N200RE 9.3.5u.6139_B20201216 /cgi-bin/cstecgi.cgi NTPSyncWithHost host_time os command injection	A vulnerability has been found in Totolink N200RE 9.3.5u.6139_B20201216 and classified as critical. This vulnerability affects the function NTPSyncWithHost of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument host_time leads to os command injection. This vulnerability was named CVE-2024-0296. 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 core rule	N
CVE-2024-0298	Totolink N200RE 9.3.5u.6139_B20201216 /cgi-bin/cstecgi.cgi setDiagnosisCfg ip os command injection	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B20201216. It has been classified as critical. Affected is the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ip leads to os command injection. This vulnerability is traded as CVE-2024-0298. It is possible to launch 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	N
CVE-2024-0299	Totolink N200RE 9.3.5u.6139_B20201216 /cgi-bin/cstecgi.cgi setTracerouteCfg	A vulnerability was found in Totolink N200RE 9.3.5u.6139_B2020121	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	command os command injection	6. It has been declared as critical. Affected by this vulnerability is the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument command leads to os command injection. This vulnerability is known as CVE-2024-0299. The attack can 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-2023-49235	TRENDnet TV-IP1314PI 5.5.3 200714 Debug Information libremote_dbg.so popen os command injection	A vulnerability which was classified as critical has been found in TRENDnet TV-IP1314PI 5.5.3 200714. Affected by this issue is the function popen of the file libremote_dbg.so of the component Debug Information Handler. The manipulation leads to os command injection. This vulnerability is handled as CVE-2023-49235. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-49237	TRENDnet TV-IP1314PI 5.5.3 Language Pack system command injection	A vulnerability has been found in TRENDnet TV-IP1314PI 5.5.3 and classified as critical. This vulnerability affects the function system of the component Language Pack Handler. The manipulation leads to command injection. This vulnerability was named CVE-2023-49237. The attack needs to be done within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2023-51972	Tenda AX1803 1.0.0.1 fromAdvSetLanIp command injection	A vulnerability which was classified as critical was found in Tenda AX1803 1.0.0.1. This affects the function fromAdvSetLanIp. The manipulation leads to command injection.	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is uniquely identified as CVE-2023-51972. The attack needs to be initiated within the local network. There is no exploit available.		
CVE-2023-31446	Cassia Gateway XC1000_2.1.1.2303082218/XC2000_2.1.1.2303090947 /bypass/config queueUrl os command injection	A vulnerability classified as critical was found in Cassia Gateway XC1000_2.1.1.2303082218/XC2000_2.1.1.2303090947. This vulnerability affects unknown code of the file /bypass/config. The manipulation of the argument queueUrl leads to os command injection. This vulnerability was named CVE-2023-31446. The attack can only be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-0778	Uniview ISC 2500-S up to 20210930 VM.php setNatConfig natAddress/natPort/natServerPort os command injection	A vulnerability which was classified as critical has been found in Uniview ISC 2500-S up to 20210930. Affected by this issue is the function setNatConfig of the file /Interface/DevManage/VM.php. The manipulation of the argument natAddress/natPort/natServerPort leads to os command injection. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability is handled as CVE-2024-0778. The attack needs to be initiated within the local network. Furthermore there is an exploit available. Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	Patched by core rule	Y
CVE-2023-51887	MathTex up to 1.05 URL command injection	A vulnerability classified as critical has been found in MathTex up to 1.05. This affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		an unknown part of the component URL Handler. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2023-51887. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2023-36177	badaix Snapcast 0.27.0 JSON-RPC-API information disclosure	A vulnerability which was classified as problematic was found in badaix Snapcast 0.27.0. Affected is an unknown function of the component JSON-RPC-API. The manipulation leads to information disclosure. This vulnerability is traded as CVE-2023-36177. It is possible to launch the attack remotely. 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-2023-5991	Hotel Booking Lite Plugin up to 4.8.4 on WordPress cross-site request forgery	A vulnerability which was classified as problematic was found in Hotel Booking Lite Plugin up to 4.8.4 on WordPress. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-5991. 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	N
CVE-2023-6532	WP Blogs Planetarium Plugin up to 1.0 on WordPress Setting cross-site request forgery	A vulnerability has been found in WP Blogs Planetarium Plugin up to 1.0 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-2023-6532. The attack can be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2023-52072	sunkaifei FlyCMS 1.0 userconfig_updagte cross-site request forgery	A vulnerability classified as problematic has been found in sunkaifei FlyCMS 1.0. This affects an unknown part of the file /system/site/userconfig_updagte. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-52072. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2023-52074	sunkaifei FlyCMS 1.0 webconfig_updagte cross-site request forgery	A vulnerability which was classified as problematic has been found in sunkaifei FlyCMS 1.0. This issue affects some unknown processing of the file system/site/webconfig_	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		updagte. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-52074. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-52073	sunkaifei FlyCMS 1.0 config_footer_updagte cross-site request forgery	A vulnerability classified as problematic was found in sunkaifei FlyCMS 1.0. This vulnerability affects unknown code of the file /system/site/config_footer_updagte. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-52073. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2023-7083	Voting Record Plugin up to 2.0 on WordPress Setting cross-site request forgery	A vulnerability was found in Voting Record Plugin up to 2.0 on WordPress. It has been classified as problematic. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-7083. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2023-6292	Ecwid Ecommerce Shopping Cart Plugin up to 6.12.4 on WordPress Setting cross-site request forgery	A vulnerability was found in Ecwid Ecommerce Shopping Cart Plugin up to 6.12.4 on WordPress. It has been classified as problematic. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-6292. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component.		
CVE-2021-24870	WP Fastest Cache Plugin 0.9.5 on WordPress AJAX Action wpfc_save_cdn_integration cross-site request forgery	A vulnerability was found in WP Fastest Cache Plugin 0.9.5 on WordPress. It has been rated as problematic. Affected by this issue is the function wpfc_save_cdn_integration of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2021-24870. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	N
CVE-2023-7125	PeepSo Community Plugin up to 6.3.1.1 on WordPress cross-site request forgery	A vulnerability was found in PeepSo Community Plugin up to 6.3.1.1 on WordPress. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-7125. 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-2022-1617	WP-Invoice Plugin up to 4.3.1 on WordPress Setting cross-site request forgery	A vulnerability has been found in WP-Invoice Plugin up to 4.3.1 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-2022-1617. The attack can be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2022-1618	Coru LFMember Plugin up to 1.0.2 on WordPress Setting cross-site request forgery	A vulnerability classified as problematic was found in Coru LFMember Plugin up to 1.0.2 on WordPress. This	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-1618. The attack can be initiated remotely. There is no exploit available.		
CVE-2022-3899	3dprint Plugin up to 3.5.6.8 on WordPress cross-site request forgery	A vulnerability which was classified as problematic was found in 3dprint Plugin up to 3.5.6.8 on WordPress. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-3899. 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-2021-25117	WP-PostRatings Plugin up to 1.86.0 on WordPress postratings_image cross-site request forgery	A vulnerability has been found in WP-PostRatings Plugin up to 1.86.0 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality of the file wp-admin/admin.phppagewp-postratings/postratings-options.php. The manipulation of the argument postratings_image leads to cross-site request forgery. This vulnerability is known as CVE-2021-25117. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	N
CVE-2023-3178	POST SMTP Mailer Plugin up to 2.5.6 on WordPress AJAX Action manage_postman_smtp cross-site request forgery	A vulnerability classified as problematic was found in POST SMTP Mailer Plugin up to 2.5.6 on WordPress. This vulnerability affects the function manage_postman_smtp of the component AJAX	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Action Handler. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-3178. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2022-1760	Core Control Plugin up to 1.2.1 on WordPress Setting cross-site request forgery	A vulnerability was found in Core Control Plugin up to 1.2.1 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-2022-1760. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-22715	Stupid Simple CMS up to 1.2.4 /admin-edit.php cross-site request forgery	A vulnerability was found in Stupid Simple CMS up to 1.2.4. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin-edit.php. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2024-22715. The attack may be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-22416	pyLoad up to 0.5.0b3.dev77 API cross-site request forgery (GHSA-pgpj-v85q-h5fm)	A vulnerability classified as problematic was found in pyLoad up to 0.5.0b3.dev77. Affected by this vulnerability is an unknown functionality of the component API. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2024-22416. The attack can be launched remotely. There is no exploit available.	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		It is recommended to upgrade the affected component.		
CVE-2023-6499	lasTunes Plugin up to 3.6.1 on WordPress cross-site request forgery	A vulnerability which was classified as problematic was found in lasTunes Plugin up to 3.6.1 on WordPress. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-6499. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2023-6501	Splashscreen Plugin up to 0.20 on WordPress cross-site request forgery	A vulnerability which was classified as problematic has been found in Splashscreen Plugin up to 0.20 on WordPress. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-6501. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2023-6625	Product Enquiry for WooCommerce Plugin up to 3.0 on WordPress cross-site request forgery	A vulnerability which was classified as problematic was found in Product Enquiry for WooCommerce Plugin up to 3.0 on WordPress. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-6625. 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	N

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-5672	WP Mail Log Plugin up to 1.1.2 on WordPress path traversal	A vulnerability classified as problematic was found in WP Mail Log Plugin up to 1.1.2 on WordPress. This vulnerability affects unknown code. The manipulation leads to path traversal. This vulnerability was named CVE-2023-5672. An attack has to be approached locally. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2023-50255	linuxdeepin developer-center up to 5.12.20 deepin-compressor path traversal	A vulnerability was found in linuxdeepin developer-center up to 5.12.20. It has been classified as critical. Affected is an unknown function of the component deepin-compressor. The manipulation leads to relative path traversal. This vulnerability is traded as CVE-2023-50255. 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-2023-7134	SourceCodester Medicine Tracking System 1.0 page path traversal	A vulnerability was found in SourceCodester Medicine Tracking System 1.0. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument page leads to path traversal: &039;../filedir&039;. The identification of this vulnerability is CVE-2023-7134. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-21633	iBotPeaches Apktool	A vulnerability which was	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	up to 2.9.1 path traversal (GHSA-2hqv-2xv4-5h5w)	classified as critical has been found in iBotPeaches Apktool up to 2.9.1. Affected by this issue is some unknown functionality. The manipulation leads to path traversal. This vulnerability is handled as CVE-2024-21633. The attack may be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	core rule	
CVE-2023-47473	fuwushe iFair up to 23.8_ad0 path traversal	A vulnerability was found in fuwushe iFair up to 23.8_ad0. It has been classified as problematic. This affects an unknown part. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-47473. The attack needs to be approached within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2023-37607	Automatic-Systems SOC FL9600 FastLine lego_T04E00 path traversal	A vulnerability classified as critical was found in Automatic-Systems SOC FL9600 FastLine lego_T04E00. Affected by this vulnerability is an unknown functionality. The manipulation leads to path traversal. This vulnerability is known as CVE-2023-37607. The attack can be launched remotely. There is no exploit.	Patched by core rule	Y
CVE-2023-29962	S-CMS 5.0 path traversal	A vulnerability was found in S-CMS 5.0. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to path traversal. This vulnerability is handled as CVE-2023-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		29962. Access to the local network is required for this attack to succeed. There is no exploit available.		
CVE-2023-50916	Kyocera Device Manager prior 3.1.1213.0 UNC path traversal	A vulnerability classified as critical has been found in Kyocera Device Manager. This affects an unknown part of the component UNC Handler. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-50916. The attack can only be done within the local network. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2023-2252	Directorist Plugin up to 7.5.3 on WordPress CSV File Import file path traversal	A vulnerability was found in Directorist Plugin up to 7.5.3 on WordPress. It has been rated as critical. This issue affects some unknown processing of the component CSV File Import. The manipulation of the argument file leads to path traversal. The identification of this vulnerability is CVE-2023-2252. 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-2021-24566	WooCommerce Currency Switcher FOX Plugin up to 1.3.6 on WordPress Shortcode path traversal	A vulnerability has been found in WooCommerce Currency Switcher FOX Plugin up to 1.3.6 on WordPress and classified as critical. This vulnerability affects unknown code of the component Shortcode Handler. The manipulation leads to path traversal. This vulnerability was named CVE-2021-24566.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-0882	qwdigital LinkWechat 5.1.0 Universal Download Interface resource name path traversal	A vulnerability was found in qwdigital LinkWechat 5.1.0. It has been classified as problematic. This affects an unknown part of the file /linkwechat-api/common/download/resource of the component Universal Download Interface. The manipulation of the argument name with the input /profile/../../../../../etc/passwd leads to path traversal: &039;../filedir&039;. This vulnerability is uniquely identified as CVE-2024-0882. 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

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-5931	rtMedia Plugin/BuddyPress Plugin/bbPress Plugin up to 4.6.15 on WordPress unrestricted upload	A vulnerability was found in rtMedia Plugin BuddyPress Plugin and bbPress Plugin up to 4.6.15 on WordPress. It has been classified as critical. Affected is an unknown function. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2023-5931. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by custom rule	N
CVE-2024-0185	RRJ Nueva Ecija Engineer Online Portal 1.0 Avatar dasboard_teacher.php unrestricted upload	A vulnerability was found in RRJ Nueva Ecija Engineer Online Portal 1.0. It has been rated as critical. This issue affects some unknown processing of the file dasboard_teacher.php of the component Avatar Handler. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2024-0185. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by custom rule	N
CVE-2024-0192	RRJ Nueva Ecija Engineer Online Portal 1.0 Add Downloadable downloadable.php unrestricted upload	A vulnerability was found in RRJ Nueva Ecija Engineer Online Portal 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file downloadable.php of the component Add Downloadable. The	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation leads to unrestricted upload. This vulnerability is known as CVE-2024-0192. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2024-0194	CodeAstro Internet Banking System up to 1.0 Profile Picture pages_account.php unrestricted upload	A vulnerability which was classified as critical has been found in CodeAstro Internet Banking System up to 1.0. This issue affects some unknown processing of the file pages_account.php of the component Profile Picture Handler. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2024-0194. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by custom rule	N
CVE-2022-1538	Theme Demo Import Plugin up to 1.1.0 on WordPress Imported File unrestricted upload	A vulnerability which was classified as problematic has been found in Theme Demo Import Plugin up to 1.1.0 on WordPress. This issue affects some unknown processing of the component Imported File Handler. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2022-1538. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-31314	Falcon Security ejinshan 8+ unrestricted upload	A vulnerability classified as problematic has been found in Falcon Security ejinshan 8+. Affected is an unknown function. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2021-31314. The attack can only be done within the local network. There is no exploit available.	Patched by custom rule	N
CVE-2024-22895	DedeCMS 5.7.112 module_upload.php unrestricted upload	A vulnerability classified as problematic was found in DedeCMS 5.7.112. This vulnerability affects unknown code of the file uploads/dede/module_upload.php. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2024-22895. Access to the local network is required for this attack. There is no exploit available.	Patched by custom rule	N
CVE-2023-7082	Import any XML or CSV File Plugin up to 3.7.2 on WordPress ZIP File unrestricted upload	A vulnerability classified as problematic was found in Import any XML or CSV File Plugin up to 3.7.2 on WordPress. This vulnerability affects unknown code of the component ZIP File Handler. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-7082. The attack can be initiated remotely. There is no exploit available.	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		It is recommended to upgrade the affected component.		
CVE-2024-0783	Project Worlds Online Admission System 1.0 documents.php unrestricted upload	A vulnerability was found in Project Worlds Online Admission System 1.0 and classified as critical. This issue affects some unknown processing of the file documents.php. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2024-0783. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by custom rule	N

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-5674	WP Mail Log Plugin up to 1.1.2 on WordPress sql injection	A vulnerability has been found in WP Mail Log Plugin up to 1.1.2 on WordPress and classified as critical. This vulnerability affects unknown code. The manipulation leads to sql injection. This vulnerability was named CVE-2023-5674. The attack needs to be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2023-5203	WP Sessions Time Monitoring Full Automatic Plugin up to 1.0.8 on WordPress Query Parameter sql injection	A vulnerability was found in WP Sessions Time Monitoring Full Automatic Plugin up to 1.0.8 on WordPress. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Query Parameter Handler. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-5203. 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-2023-5645	WP Mail Log Plugin up to 1.1.2 on WordPress sql injection	A vulnerability was found in WP Mail Log Plugin up to 1.1.2 on WordPress. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation leads to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		sql injection. This vulnerability is handled as CVE-2023-5645. The attack needs to be approached within the local network. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-52096	SteVe Community ocpp-jaxb up to 0.0.7 StartTransaction Open Charge Point Protocol sql injection (Issue 13)	A vulnerability classified as critical has been found in SteVe Community ocpp-jaxb up to 0.0.7. Affected is an unknown function of the component StartTransaction Open Charge Point Protocol. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-52096. The attack needs to be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2023-7123	SourceCodester Medicine Tracking System 1.0 Master.php id/name/description sql injection	A vulnerability which was classified as critical has been found in SourceCodester Medicine Tracking System 1.0. This issue affects some unknown processing of the file /classes/Master.php fsave_medicine. The manipulation of the argument id/name/description leads to sql injection. The identification of this vulnerability is CVE-2023-7123. The attack may be initiated remotely. Furthermore there is an exploit	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		available.		
CVE-2023-7128	code-projects Voting System 1.0 Admin Login /admin/ username sql injection	A vulnerability which was classified as critical has been found in code-projects Voting System 1.0. This issue affects some unknown processing of the file /admin/ of the component Admin Login. The manipulation of the argument username leads to sql injection. The identification of this vulnerability is CVE-2023-7128. The attack can only be done within the local network. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-7155	SourceCodester Free and Open Source Inventory Management System 1.0 edit_product.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Free and Open Source Inventory Management System 1.0. This affects an unknown part of the file /ample/app/action/edit_product.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-7155. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-7156	Campcodes Online College Library System 1.0 Search index.php category sql injection	A vulnerability has been found in Campcodes Online College Library System 1.0 and classified as critical. This vulnerability affects unknown code of the file index.php of the component Search. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument category leads to sql injection. This vulnerability was named CVE-2023-7156. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2023-7157	SourceCodester Free and Open Source Inventory Management System 1.0 sell_return_data.php columns[0][data] sql injection	A vulnerability was found in SourceCodester Free and Open Source Inventory Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /app/ajax/sell_return_data.php. The manipulation of the argument columns[0][data] leads to sql injection. The identification of this vulnerability is CVE-2023-7157. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-7161	Netentsec NS-ASG Application Security Gateway 6.3.1 Login index.php check_VirtualSiteId sql injection	A vulnerability classified as critical has been found in Netentsec NS-ASG Application Security Gateway 6.3.1. This affects an unknown part of the file index.phpparaindex of the component Login. The manipulation of the argument check_VirtualSiteId leads to sql injection. This vulnerability is uniquely identified as CVE-2023-7161. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-7131	code-projects Intern Membership	A vulnerability was found in code-projects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Management System 2.0 User Registration /user_registration/ userName sql injection	Intern Membership Management System 2.0 and classified as critical. Affected by this issue is some unknown functionality of the file /user_registration/ of the component User Registration. The manipulation of the argument userName leads to sql injection. This vulnerability is handled as CVE-2023-7131. The attack needs to be initiated within the local network. Furthermore there is an exploit available.		
CVE-2023-7129	code-projects Voting System 1.0 Voters Login voter sql injection	A vulnerability which was classified as critical was found in code-projects Voting System 1.0. Affected is an unknown function of the component Voters Login. The manipulation of the argument voter leads to sql injection. This vulnerability is traded as CVE-2023-7129. The attack can only be initiated within the local network. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-7180	Tongda OA 2017 up to 11.9 delete.php PROJ_ID_STR sql injection	A vulnerability has been found in Tongda OA 2017 up to 11.9 and classified as critical. Affected by this vulnerability is an unknown functionality of the file general/project/proj/delete.php. The manipulation of the argument PROJ_ID_STR leads to sql injection. This vulnerability is known as CVE-2023-7180. Access to the local network is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		required for this attack to succeed. 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 upgrade the affected component.		
CVE-2023-7179	Campcodes Online College Library System 1.0 HTTP POST Request /admin/category_row.php id sql injection	A vulnerability which was classified as critical was found in Campcodes Online College Library System 1.0. Affected is an unknown function of the file /admin/category_row.php of the component HTTP POST Request Handler. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-7179. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-7177	Campcodes Online College Library System 1.0 HTTP POST Request /admin/book_add.php category sql injection	A vulnerability classified as critical was found in Campcodes Online College Library System 1.0. This vulnerability affects unknown code of the file /admin/book_add.php of the component HTTP POST Request Handler. The manipulation of the argument category leads to sql injection. This vulnerability was named CVE-2023-7177. The attack can be initiated remotely. Furthermore there is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		an exploit available.		
CVE-2023-7175	Campcodes Online College Library System 1.0 HTTP POST Request /admin/borrow_add.php student sql injection	A vulnerability was found in Campcodes Online College Library System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/borrow_add.php of the component HTTP POST Request Handler. The manipulation of the argument student leads to sql injection. This vulnerability is handled as CVE-2023-7175. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-50071	SourceCodester Customer Support System 1.0 ajax.php id/name sql injection	A vulnerability was found in SourceCodester Customer Support System 1.0 and classified as critical. This issue affects some unknown processing of the file /customer_support/ajax.phpactionsave_department. The manipulation of the argument id/name leads to sql injection. The identification of this vulnerability is CVE-2023-50071. Access to the local network is required for this attack. There is no exploit available.	Patched by core rule	Y
CVE-2023-50035	PHPGurukul Small CRM 3.0 User Login Panel password sql injection	A vulnerability has been found in PHPGurukul Small CRM 3.0 and classified as critical. This vulnerability affects unknown code of the component User Login Panel. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument password leads to sql injection. This vulnerability was named CVE-2023-50035. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2023-7172	PHPGurukul Hospital Management System 1.0 Admin Dashboard sql injection	A vulnerability which was classified as critical has been found in PHPGurukul Hospital Management System 1.0. Affected by this issue is some unknown functionality of the component Admin Dashboard. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-7172. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-41543	jeecg-boot 3.5.3 /sys/replicate/check sql injection	A vulnerability which was classified as critical was found in jeecg-boot 3.5.3. This affects an unknown part of the file /sys/replicate/check. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-41543. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-41542	jeecg-boot 3.5.3 jmreport/qurestSql sql injection	A vulnerability which was classified as critical has been found in jeecg-boot 3.5.3. Affected by this issue is some unknown functionality of the file jmreport/qurestSql. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		41542. The attack may be launched remotely. There is no exploit available.		
CVE-2023-50070	SourceCodester Customer Support System 1.0 ajax.php department_id/customer_id/subject sql injection	A vulnerability was found in SourceCodester Customer Support System 1.0. It has been classified as critical. This affects an unknown part of the file /customer_support/ajax.phpactionsave_ticket. The manipulation of the argument department_id/customer_id/subject leads to sql injection. This vulnerability is uniquely identified as CVE-2023-50070. The attack can only be done within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2023-50589	Grupo Embras GEOSIAP ERP 2.2.167.02 Login Page codLogin sql injection	A vulnerability was found in Grupo Embras GEOSIAP ERP 2.2.167.02. It has been rated as critical. Affected by this issue is some unknown functionality of the component Login Page. The manipulation of the argument codLogin leads to sql injection. This vulnerability is handled as CVE-2023-50589. The attack can only be initiated within the local network. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-50578	Mingsoft MCMS 5.2.9 /content/list.do categoryType sql injection	A vulnerability which was classified as critical was found in Mingsoft MCMS 5.2.9. Affected is an unknown function of the file /content/list.do. The manipulation of the argument	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		categoryType leads to sql injection. This vulnerability is traded as CVE-2023-50578. Access to the local network is required for this attack to succeed. There is no exploit available.		
CVE-2020-26625	Gila CMS up to 1.15.4 user_id sql injection (ID 176301)	A vulnerability was found in Gila CMS up to 1.15.4. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation of the argument user_id leads to sql injection. This vulnerability is known as CVE-2020-26625. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2020-26624	Gila CMS up to 1.15.4 Login Portal ID sql injection (ID 176301)	A vulnerability was found in Gila CMS up to 1.15.4. It has been declared as critical. This vulnerability affects unknown code of the component Login Portal. The manipulation of the argument ID leads to sql injection. This vulnerability was named CVE-2020-26624. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2020-26623	Gila CMS up to 1.15.4 Login Portal Area sql injection (ID 176301)	A vulnerability was found in Gila CMS up to 1.15.4 and classified as critical. This issue affects some unknown processing of the component Login Portal. The manipulation of the argument Area 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-2020-26623. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-50864	Kashipara Group Travel Website 1.0 hotelDetails.php hotelId sql injection	A vulnerability classified as critical has been found in Kashipara Group Travel Website 1.0. Affected is an unknown function of the file hotelDetails.php. The manipulation of the argument hotelId leads to sql injection. This vulnerability is traded as CVE-2023-50864. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-50743	Kashipara Group Online Notice Board System 1.0 registration.php dd sql injection	A vulnerability has been found in Kashipara Group Online Notice Board System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file registration.php. The manipulation of the argument dd leads to sql injection. This vulnerability is known as CVE-2023-50743. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-0247	CodeAstro Online Food Ordering System 1.0 Admin Panel /admin/ Username sql injection	A vulnerability classified as critical was found in CodeAstro Online Food Ordering System 1.0. This vulnerability affects unknown code of the file /admin/ of the component Admin Panel. The manipulation of the argument Username leads to sql injection.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability was named CVE-2024-0247. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2023-39853	Dzzoffice 2.01 Network Disk Backend doobj/doevent sql injection	A vulnerability classified as critical has been found in Dzzoffice 2.01. Affected is an unknown function of the component Network Disk Backend. The manipulation of the argument doobj/doevent leads to sql injection. This vulnerability is traded as CVE-2023-39853. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-0306	Kashipara Dynamic Lab Management System up to 1.0 admin_login_process.php admin_password sql injection	A vulnerability was found in Kashipara Dynamic Lab Management System up to 1.0. It has been classified as critical. This affects an unknown part of the file /admin/admin_login_process.php. The manipulation of the argument admin_password leads to sql injection. This vulnerability is uniquely identified as CVE-2024-0306. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-0301	fhs-opensource iparking 1.5.22.RELEASE PayTempOrderAction.java getData sql injection	A vulnerability classified as critical was found in fhs-opensource iparking 1.5.22.RELEASE. This vulnerability affects the function getData of the file src/main/java/com/xhb	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/pay/action/PayTempOrderAction.java. The manipulation leads to sql injection. This vulnerability was named CVE-2024-0301. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-0287	Kashipara Food Management System 1.0 itemBillPdf.php printid sql injection	A vulnerability was found in Kashipara Food Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file itemBillPdf.php. The manipulation of the argument printid leads to sql injection. This vulnerability is handled as CVE-2024-0287. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-0289	Kashipara Food Management System 1.0 stock_entry_submit.php itemype sql injection	A vulnerability classified as critical was found in Kashipara Food Management System 1.0. This vulnerability affects unknown code of the file stock_entry_submit.php. The manipulation of the argument itemype leads to sql injection. This vulnerability was named CVE-2024-0289. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-0290	Kashipara Food Management System 1.0 stock_edit.php item_type sql injection	A vulnerability which was classified as critical has been found in Kashipara Food Management System 1.0. 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
		stock_edit.php. The manipulation of the argument item_type leads to sql injection. The identification of this vulnerability is CVE-2024-0290. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-0288	Kashipara Food Management System 1.0 rawstock_used_damaged_submit.php product_name sql injection	A vulnerability classified as critical has been found in Kashipara Food Management System 1.0. This affects an unknown part of the file rawstock_used_damaged_submit.php. The manipulation of the argument product_name leads to sql injection. This vulnerability is uniquely identified as CVE-2024-0288. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-50162	EmpireCMS 7.5 DoExecSql sql injection	A vulnerability was found in EmpireCMS 7.5. It has been classified as critical. Affected is the function DoExecSql. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023-50162. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-0355	PHPGurukul Dairy Farm Shop Management System up to 1.1 add-category.php category sql injection	A vulnerability which was classified as critical was found in PHPGurukul Dairy Farm Shop Management System up to 1.1. Affected is an unknown function of the file add-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		category.php. The manipulation of the argument category leads to sql injection. This vulnerability is traded as CVE-2024-0355. Access to the local network is required for this attack. Furthermore there is an exploit available.		
CVE-2024-0362	PHPGurukul Hospital Management System 1.0 change-password.php cpass sql injection	A vulnerability classified as critical was found in PHPGurukul Hospital Management System 1.0. Affected by this vulnerability is an unknown functionality of the file admin/change-password.php. The manipulation of the argument cpass leads to sql injection. This vulnerability is known as CVE-2024-0362. Access to the local network is required for this attack. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-0363	PHPGurukul Hospital Management System 1.0 admin/patient-search.php searchdata sql injection	A vulnerability which was classified as critical has been found in PHPGurukul Hospital Management System 1.0. Affected by this issue is some unknown functionality of the file admin/patient-search.php. The manipulation of the argument searchdata leads to sql injection. This vulnerability is handled as CVE-2024-0363. Access to the local network is required for this attack to succeed. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-0361	PHPGurukul Hospital	A vulnerability classified as critical has	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Management System 1.0 admin/contact.php mobnum sql injection	been found in PHPGurukul Hospital Management System 1.0. Affected is an unknown function of the file admin/contact.php. The manipulation of the argument mobnum leads to sql injection. This vulnerability is traded as CVE-2024-0361. The attack needs to be initiated within the local network. Furthermore there is an exploit available.		
CVE-2024-0359	code-projects Simple Online Hotel Reservation System 1.0 login.php username/password sql injection	A vulnerability was found in code-projects Simple Online Hotel Reservation System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file login.php. The manipulation of the argument username/password leads to sql injection. This vulnerability was named CVE-2024-0359. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-0360	PHPGurukul Hospital Management System 1.0 edit-doctor-specialization.php doctorspecilization sql injection	A vulnerability was found in PHPGurukul Hospital Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file admin/edit-doctor-specialization.php. The manipulation of the argument doctorspecilization leads to sql injection. The identification of this vulnerability is CVE-2024-0360. The attack needs to be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		done within the local network. Furthermore there is an exploit available.		
CVE-2024-0357	coderd-repos Eva 1.0.0 HTTP POST Request /system/traceLog/page property sql injection	A vulnerability was found in coderd-repos Eva 1.0.0 and classified as critical. Affected by this issue is some unknown functionality of the file /system/traceLog/page of the component HTTP POST Request Handler. The manipulation of the argument property leads to sql injection. This vulnerability is handled as CVE-2024-0357. The attack needs to be approached within the local network. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-48864	SEMCMS 4.8 /web_inc.php languageID sql injection	A vulnerability which was classified as critical has been found in SEMCMS 4.8. This issue affects some unknown processing of the file /web_inc.php. The manipulation of the argument languageID leads to sql injection. The identification of this vulnerability is CVE-2023-48864. The attack needs to be approached within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2020-26630	Hospital Management System 4.0 Doctor Specialization sql injection (ID 176302)	A vulnerability was found in Hospital Management System 4.0. It has been classified as critical. This affects an unknown part. The manipulation of the argument Doctor Specialization leads to sql injection. This vulnerability is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		uniquely identified as CVE-2020-26630. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-0389	SourceCodester Student Attendance System 1.0 attendance_report.php class_id sql injection	A vulnerability which was classified as critical was found in SourceCodester Student Attendance System 1.0. Affected is an unknown function of the file attendance_report.php. The manipulation of the argument class_id leads to sql injection. This vulnerability is traded as CVE-2024-0389. The attack can only be done within the local network. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2020-26627	Hospital Management System 4.0 Admin Remark sql injection (ID 176302)	A vulnerability was found in Hospital Management System 4.0. It has been declared as critical. This vulnerability affects unknown code. The manipulation of the argument Admin Remark leads to sql injection. This vulnerability was named CVE-2020-26627. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-52064	wuzhicms 4.1.0 /core/admin/copyfrom.php keywords sql injection (Issue 208)	A vulnerability was found in wuzhicms 4.1.0. It has been declared as critical. This vulnerability affects unknown code of the file /core/admin/copyfrom.php. The manipulation of the argument keywords leads to sql injection.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability was named CVE-2023-52064. The attack can only be done within the local network. There is no exploit available.		
CVE-2024-0502	SourceCodester House Rental Management System 1.0 Edit User manage_user.php id/name/username sql injection	A vulnerability was found in SourceCodester House Rental Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file manage_user.php of the component Edit User. The manipulation of the argument id/name/username leads to sql injection. This vulnerability is handled as CVE-2024-0502. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-0480	Taokeyun up to 1.0.5 HTTP POST Request Drs.php index cid sql injection	A vulnerability was found in Taokeyun up to 1.0.5. It has been declared as critical. Affected by this vulnerability is the function index of the file application/index/controller/m/Drs.php of the component HTTP POST Request Handler. The manipulation of the argument cid leads to sql injection. This vulnerability is known as CVE-2024-0480. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-0543	CodeAstro Real Estate Management System up to 1.0 propertydetail.php pid sql injection	A vulnerability classified as critical has been found in CodeAstro Real Estate Management System up to 1.0. This affects an unknown part of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		file propertydetail.php. The manipulation of the argument pid leads to sql injection. This vulnerability is uniquely identified as CVE-2024-0543. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-0523	CmsEasy up to 7.7.7 language_admin.php getslide_child_action sid sql injection	A vulnerability was found in CmsEasy up to 7.7.7. It has been declared as critical. Affected by this vulnerability is the function getslide_child_action in the library lib/admin/language_admin.php. The manipulation of the argument sid leads to sql injection. This vulnerability is known as CVE-2024-0523. The attack can be launched 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-2024-0558	DedeBIZ 6.3.0 makehtml_freelist_action.php startid sql injection	A vulnerability has been found in DedeBIZ 6.3.0 and classified as critical. This vulnerability affects unknown code of the file /admin/makehtml_freelist_action.php. The manipulation of the argument startid leads to sql injection. This vulnerability was named CVE-2024-0558. The attack can be initiated remotely. Furthermore there is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2023-0224	GiveWP Plugin up to 2.24.0 on WordPress sql injection	A vulnerability was found in GiveWP Plugin up to 2.24.0 on WordPress. It has been classified as critical. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-0224. 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-2023-2655	WD Contact Form Plugin up to 1.13.23 on WordPress sql injection	A vulnerability classified as critical was found in WD Contact Form Plugin up to 1.13.23 on WordPress. This vulnerability affects unknown code. The manipulation leads to sql injection. This vulnerability was named CVE-2023-2655. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-4797	SendPress Newsletters Plugin up to 4.9.2 on WordPress sql injection	A vulnerability which was classified as critical has been found in SendPress Newsletters Plugin up to 4.9.2 on WordPress. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-4797. 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-2024-22628	Budget and Expense Tracker System 1.0 date_end sql injection	A vulnerability was found in Budget and Expense Tracker System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /expense_budget/admin/pagereports/budget&amp;date_start2023-12-28. The manipulation of the argument date_end leads to sql injection. This vulnerability was named CVE-2024-22628. The attack needs to be done within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-22626	Complete Supplier Management System 1.0 edit_retailer.php id sql injection	A vulnerability has been found in Complete Supplier Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /Supply_Management_System/admin/edit_retailer.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2024-22626. The attack needs to be approached within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2021-24151	WP Editor Plugin up to 1.2.6 on WordPress Setting sql injection	A vulnerability was found in WP Editor Plugin up to 1.2.6 on WordPress and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		classified as critical. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2021-24151. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-22625	Complete Supplier Management System 1.0 edit_category.php id sql injection	A vulnerability which was classified as critical was found in Complete Supplier Management System 1.0. Affected is an unknown function of the file /Supply_Management_System/admin/edit_category.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-22625. Access to the local network is required for this attack to succeed. There is no exploit available.	Patched by core rule	Y
CVE-2021-24869	WP Fastest Cache Plugin 0.9.5 on WordPress set_urls_with_terms sql injection	A vulnerability classified as critical has been found in WP Fastest Cache Plugin 0.9.5 on WordPress. This affects the function set_urls_with_terms. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2021-24869. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		It is recommended to upgrade the affected component.		
CVE-2024-22627	Complete Supplier Management System 1.0 edit_distributor.php id sql injection	A vulnerability classified as critical was found in Complete Supplier Management System 1.0. This vulnerability affects unknown code of the file /Supply_Management_System/admin/edit_distributor.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-22627. The attack needs to be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2022-3764	Form Vibes Plugin prior 1.4.6 on WordPress delete_entries sql injection	A vulnerability has been found in Form Vibes Plugin on WordPress and classified as critical. This vulnerability affects unknown code. The manipulation of the argument delete_entries leads to sql injection. This vulnerability was named CVE-2022-3764. 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-2024-0655	Novel-Plus 4.3.0-RC1 /novel/bookSetting/list sort sql injection	A vulnerability has been found in Novel-Plus 4.3.0-RC1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /novel/bookSetting/list. The manipulation of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the argument sort leads to sql injection. This vulnerability is known as CVE-2024-0655. Access to the local network is required for this attack to succeed. Furthermore there is an exploit available.		
CVE-2023-52285	ExamSys 9150244 Pages.php s_score2 sql injection	A vulnerability which was classified as critical has been found in ExamSys 9150244. This issue affects some unknown processing of the file /Support/action/Pages.php. The manipulation of the argument s_score2 leads to sql injection. The identification of this vulnerability is CVE-2023-52285. Access to the local network is required for this attack to succeed. There is no exploit available.	Patched by core rule	Y
CVE-2024-0651	PHPGurukul Company Visitor Management System 1.0 search-visitor.php sql injection	A vulnerability was found in PHPGurukul Company Visitor Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file search-visitor.php. The manipulation leads to sql injection. This vulnerability is known as CVE-2024-0651. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-0784	biantaibao octopus 1.0 /system/role/list dataScope sql injection	A vulnerability was found in biantaibao octopus 1.0. It has been classified as critical. Affected is an	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown function of the file /system/role/list. The manipulation of the argument dataScope leads to sql injection. This vulnerability is traded as CVE-2024-0784. It is possible to launch the attack remotely. Furthermore there is an exploit available. This product is using a rolling release to provide continious delivery. Therefore no version details for affected nor updated releases are available.		
CVE-2024-23646	Pimcore admin-ui-classic-bundle up to 1.3.1 ZIP File selectedIds sql injection	A vulnerability which was classified as critical has been found in Pimcore admin-ui-classic-bundle up to 1.3.1. This issue affects some unknown processing of the component ZIP File Handler. The manipulation of the argument selectedIds leads to sql injection. The identification of this vulnerability is CVE-2024-23646. 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-2024-0883	SourceCodester Online Tours & Travels Management System 1.0 admin/pay.php prepare id sql injection	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0. It has been declared as critical. This vulnerability affects the function prepare of the file admin/pay.php. The manipulation of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the argument id leads to sql injection. This vulnerability was named CVE-2024-0883. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-0884	SourceCodester Online Tours & Travels Management System 1.0 payment.php exec id sql injection	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0. It has been rated as critical. This issue affects the function exec of the file payment.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-0884. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-27150	openCRX 5.2.0 Manage Activity Name cross site scripting	A vulnerability was found in openCRX 5.2.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Manage Activity Handler. The manipulation of the argument Name leads to cross site scripting. This vulnerability is handled as CVE-2023-27150. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-6166	Quiz Maker Plugin prior 6.4.9.5 on WordPress URL cross site scripting	A vulnerability was found in Quiz Maker Plugin on WordPress and classified as problematic. Affected by this issue is some unknown functionality of the component URL Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-6166. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2023-6268	JSON Content Importer Plugin up to 1.5.3 on WordPress tab cross site scripting	A vulnerability has been found in JSON Content Importer Plugin up to 1.5.3 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument tab 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-2023-6268. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-7124	code-projects E-Commerce Site 1.0 search.php keyword cross site scripting	A vulnerability which was classified as problematic was found in code-projects E-Commerce Site 1.0. Affected is an unknown function of the file search.php. The manipulation of the argument keyword with the input &lt;video/srcx onerroralert&gt; leads to cross site scripting. This vulnerability is traded as CVE-2023-7124. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-50470	SeaCMS 12.8 admin_video.php action cross site scripting	A vulnerability was found in SeaCMS 12.8. It has been declared as problematic. This vulnerability affects unknown code of the file admin_video.php. The manipulation of the argument action leads to cross site scripting. This vulnerability was named CVE-2023-50470. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-7149	code-projects QR Code Generator 1.0 download.php file cross site scripting	A vulnerability was found in code-projects QR Code Generator 1.0. It has been classified as problematic. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects an unknown part of the file /download.phpfileauthor.png. The manipulation of the argument file with the input &quot;&gt;&lt;iMg srcN onerroralert&gt; leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-7149. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2023-7135	code-projects Record Management System 1.0 Offices /main/offices.php officename cross site scripting	A vulnerability classified as problematic has been found in code-projects Record Management System 1.0. Affected is an unknown function of the file /main/offices.php of the component Offices Handler. The manipulation of the argument officename with the input &quot;&gt;&lt;script src&quot; leads to cross site scripting. This vulnerability is traded as CVE-2023-7135. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-7136	code-projects Record Management System 1.0 Document Type /main/doctype.php docname cross site scripting	A vulnerability classified as problematic was found in code-projects Record Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /main/doctype.php of the component Document Type Handler. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument docname with the input &quot;&gt;&lt;script src&quot; leads to cross site scripting. This vulnerability is known as CVE-2023-7136. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2023-7132	code-projects Intern Membership Management System 2.0 User Registration /user_registration/ userName/firstName/lastName/userEmail cross site scripting	A vulnerability was found in code-projects Intern Membership Management System 2.0. It has been classified as problematic. This affects an unknown part of the file /user_registration/ of the component User Registration. The manipulation of the argument userName/firstName/lastName/userEmail with the input &quot;&gt;&lt;ScRiPt&gt;confirm&lt;/ScRiPt&gt;h0la leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-7132. Access to the local network is required for this attack. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-7166	Novel-Plus up to 4.2.0 HTTP POST Request /user/updateUserInfo nickName cross site scripting	A vulnerability classified as problematic has been found in Novel-Plus up to 4.2.0. This affects an unknown part of the file /user/updateUserInfo of the component HTTP POST Request Handler. The manipulation of the argument nickName 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-2023-7166. It is possible to initiate the attack remotely. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue.		
CVE-2023-7133	y_project RuoYi 4.7.8 HTTP POST Request /login rememberMe cross site scripting	A vulnerability was found in y_project RuoYi 4.7.8. It has been declared as problematic. This vulnerability affects unknown code of the file /login of the component HTTP POST Request Handler. The manipulation of the argument rememberMe with the input falsen3f0m&lt;script&gt;alert&lt;/script&gt;p86o0 leads to cross site scripting. This vulnerability was named CVE-2023-7133. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-49469	Shaarli 0.12.2 Search Tag cross site scripting (Issue 2038)	A vulnerability was found in Shaarli 0.12.2. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Search Tag Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-49469. The attack may be launched 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-2023-7143	code-projects Client Details System 1.0 /admin/regester.php fname/lname/email/contact cross site scripting	A vulnerability was found in code-projects Client Details System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/regester.php. The manipulation of the argument fname/lname/email/contact leads to cross site scripting. This vulnerability is handled as CVE-2023-7143. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-50069	WireMock up to 3.2.0.0 cross site scripting (Issue 51)	A vulnerability was found in WireMock up to 3.2.0.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-50069. 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-2023-7173	PHPGurukul Hospital Management System 1.0 registration.php First Name cross site scripting	A vulnerability which was classified as problematic was found in PHPGurukul Hospital Management System 1.0. This affects an unknown part of the file registration.php. The manipulation of the argument First Name leads to cross site scripting. This vulnerability is uniquely identified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2023-7173. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2023-7171	Novel-Plus up to 4.2.0 Friendly Link FriendLinkController.java cross site scripting	A vulnerability was found in Novel-Plus up to 4.2.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file novel-admin/src/main/java/com/java2nb/novel/controller/FriendLinkController.java of the component Friendly Link Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-7171. The attack can be launched remotely. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y
CVE-2023-52257	LogoBee 0.2 updates.php id cross site scripting (ID 174815)	A vulnerability was found in LogoBee 0.2. It has been classified as problematic. Affected is an unknown function of the file updates.php. The manipulation of the argument id leads to cross site scripting. This vulnerability is traded as CVE-2023-52257. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-52265	IDURAR up to 2.0.1 PATCH Request /api/email/update cross site scripting	A vulnerability classified as problematic was found in IDURAR up to 2.0.1. Affected by this vulnerability is an unknown functionality of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/api/email/update of the component PATCH Request Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-52265. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-52269	MDaemon Security Gateway up to 9.0.3 Message Content Filtering Rule cross site scripting	A vulnerability classified as problematic has been found in MDaemon Security Gateway up to 9.0.3. Affected is an unknown function of the component Message Content Filtering Rule Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-52269. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-0181	RRJ Nueva Ecija Engineer Online Portal 1.0 Admin Panel /admin/admin_user.php Firstname/Lastname/Username cross site scripting	A vulnerability was found in RRJ Nueva Ecija Engineer Online Portal 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/admin_user.php of the component Admin Panel. The manipulation of the argument Firstname/Lastname/Username leads to cross site scripting. This vulnerability is known as CVE-2024-0181. The attack can be launched remotely.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Furthermore there is an exploit available.		
CVE-2023-6485	Html5 Video Player Plugin up to 2.5.18 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic has been found in Html5 Video Player Plugin up to 2.5.18 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-2023-6485. 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-2024-0184	RRJ Nueva Ecija Engineer Online Portal 1.0 Add Enginer /admin/edit_teacher.php Firstname/Lastname cross site scripting	A vulnerability was found in RRJ Nueva Ecija Engineer Online Portal 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/edit_teacher.php of the component Add Enginer. The manipulation of the argument Firstname/Lastname leads to cross site scripting. This vulnerability was named CVE-2024-0184. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-0183	RRJ Nueva Ecija Engineer Online Portal 1.0 NIA Office /admin/students.php cross site scripting	A vulnerability was found in RRJ Nueva Ecija Engineer Online Portal 1.0. It has been classified as problematic. This affects an unknown part of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/admin/students.php of the component NIA Office. The manipulation leads to basic cross site scripting. This vulnerability is uniquely identified as CVE-2024-0183. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2023-6037	WP TripAdvisor Review Slider Plugin up to 11.8 on WordPress Setting cross site scripting	A vulnerability classified as problematic was found in WP TripAdvisor Review Slider Plugin up to 11.8 on WordPress. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-6037. 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-2023-6524	MapPress Maps Plugin up to 2.88.13 on WordPress cross site scripting	A vulnerability was found in MapPress Maps Plugin up to 2.88.13 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-6524. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-0190	RRJ Nueva Ecija Engineer Online Portal 1.0 Quiz	A vulnerability was found in RRJ Nueva Ecija Engineer Online	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	add_quiz.php Quiz Title/Quiz Description cross site scripting	Portal 1.0 and classified as problematic. This issue affects some unknown processing of the file add_quiz.php of the component Quiz Handler. The manipulation of the argument Quiz Title/Quiz Description with the input &lt;/title&gt;&lt;scRipt&gt;alert&lt;/scRipt&gt; leads to cross site scripting. The identification of this vulnerability is CVE-2024-0190. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-0189	RRJ Nueva Ecija Engineer Online Portal 1.0 Create Message teacher_message.php Content cross site scripting	A vulnerability has been found in RRJ Nueva Ecija Engineer Online Portal 1.0 and classified as problematic. This vulnerability affects unknown code of the file teacher_message.php of the component Create Message Handler. The manipulation of the argument Content with the input &lt;/title&gt;&lt;scRipt&gt;alert&lt;/scRipt&gt; leads to cross site scripting. This vulnerability was named CVE-2024-0189. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-21911	TinyMCE up to 5.5.x Editor cross site scripting (GHSA-w7jx-j77m-wp65)	A vulnerability was found in TinyMCE up to 5.5.x. It has been declared as problematic. Affected by this vulnerability is an unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		functionality of the component Committer. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-21911. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-50092	APIIDA API Gateway Manager for Broadcom Layer7 2023.2 cross site scripting	A vulnerability was found in APIIDA API Gateway Manager for Broadcom Layer7 2023.2 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-50092. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-6621	POST SMTP Plugin up to 2.8.6 on WordPress msg cross site scripting	A vulnerability classified as problematic was found in POST SMTP Plugin up to 2.8.6 on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation of the argument msg leads to cross site scripting. This vulnerability is known as CVE-2023-6621. 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-2024-21908	TinyMCE up to 5.8.x Editor cross site	A vulnerability classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	scripting	problematic has been found in TinyMCE up to 5.8.x. Affected is an unknown function of the component Committer. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-21908. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-21910	TinyMCE up to 5.9.x Link cross site scripting (ID 366)	A vulnerability was found in TinyMCE up to 5.9.x. It has been classified as problematic. Affected is an unknown function of the component Link Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-21910. 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-2023-50630	xiweicheng TMS 2.28.0 Click Here cross site scripting	A vulnerability was found in xiweicheng TMS 2.28.0. It has been declared as problematic. This vulnerability affects unknown code of the component Click Here. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-50630. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-21636	view_component up to 3.8.x cross site scripting (GHSA-wf2x-8w6j-qw37)	A vulnerability has been found in view_component up to 3.8.x and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-21636. 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-2023-3726	OCSInventory 2.12.0 Email Template cross site scripting	A vulnerability was found in OCSInventory 2.12.0. It has been classified as problematic. Affected is an unknown function of the component Email Template Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-3726. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-7215	Chanzhaoyu chatgpt-web 2.11.1 Description cross site scripting (Issue 2001)	A vulnerability which was classified as problematic has been found in Chanzhaoyu chatgpt-web 2.11.1. This issue affects some unknown processing. The manipulation of the argument Description with the input &lt;image src onerrorprompt&gt; leads to cross site scripting. The identification of this vulnerability is CVE-2023-7215. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-0266	Project Worlds Online Lawyer Management System 1.0 User Registration First Name cross site scripting	A vulnerability classified as problematic has been found in Project Worlds Online Lawyer Management System 1.0. Affected is an unknown function of the component User Registration. The manipulation of the argument First Name leads to cross site scripting. This vulnerability is traded as CVE-2024-0266. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-0282	Kashipara Food Management System up to 1.0 addmaterialsubmit.php tin cross site scripting	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been classified as problematic. This affects an unknown part of the file addmaterialsubmit.php. The manipulation of the argument tin leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-0282. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-0286	PHPGurukul Hospital Management System 1.0 Contact Form index.php#contact_us Name/Email/Message cross site scripting	A vulnerability which was classified as problematic was found in PHPGurukul Hospital Management System 1.0. This affects an unknown part of the file index.phpcontact_us of the component Contact Form. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument Name/Email/Message leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-0286. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-0262	Online Job Portal 1.0 Create News Page /Admin/News.php cross site scripting	A vulnerability was found in Online Job Portal 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /Admin/News.php of the component Create News Page. The manipulation of the argument News with the input &lt;/title&gt;&lt;scRipt&gt;alert&lt;/scRipt&gt; leads to cross site scripting. This vulnerability is handled as CVE-2024-0262. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-0283	Kashipara Food Management System up to 1.0 party_details.php party_name cross site scripting	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file party_details.php. The manipulation of the argument party_name leads to cross site scripting. This vulnerability was named CVE-2024-0283. The attack can 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-2024-0284	Kashipara Food Management System up to 1.0 party_submit.php party_address cross site scripting	A vulnerability was found in Kashipara Food Management System up to 1.0. It has been rated as problematic. This issue affects some unknown processing of the file party_submit.php. The manipulation of the argument party_address leads to cross site scripting. The identification of this vulnerability is CVE-2024-0284. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-6555	Email Subscription Popup Plugin up to 1.2.19 on WordPress cross site scripting	A vulnerability was found in Email Subscription Popup Plugin up to 1.2.19 on WordPress. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-6555. 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-2022-28975	Infoblox NIOS 8.5.2-409296 VLAN View Name cross site scripting	A vulnerability was found in Infoblox NIOS 8.5.2-409296. It has been classified as problematic. This affects an unknown part. The manipulation of the argument VLAN View Name leads to cross site scripting. This vulnerability is uniquely identified as CVE-2022-28975. It is possible to initiate the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack remotely. There is no exploit available.		
CVE-2023-26998	NetScout nGeniusOne 6.3.4 Alert Configuration Page cross site scripting	A vulnerability was found in NetScout nGeniusOne 6.3.4. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Alert Configuration Page. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-26998. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-27000	NetScout nGeniusOne 6.3.4 Profile/Exclusion List Page name cross site scripting	A vulnerability classified as problematic was found in NetScout nGeniusOne 6.3.4. Affected by this vulnerability is an unknown functionality of the component Profile/Exclusion List Page. The manipulation of the argument name leads to cross site scripting. This vulnerability is known as CVE-2023-27000. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-0345	CodeAstro Vehicle Booking System 1.0 User Registration usr/usr-register.php Full_Name/Last_Name/Address cross site scripting	A vulnerability which was classified as problematic was found in CodeAstro Vehicle Booking System 1.0. This affects an unknown part of the file usr/usr-register.php of the component User Registration. The manipulation of the argument Full_Name/Last_Name /Address with the input &lt;script&gt;alert&lt;/	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		script&gt; leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-0345. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-0343	CodeAstro Simple House Rental System 5.6 Login Panel cross site scripting	A vulnerability classified as problematic was found in CodeAstro Simple House Rental System 5.6. Affected by this vulnerability is an unknown functionality of the component Login Panel. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-0343. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-0346	CodeAstro Vehicle Booking System 1.0 Feedback Page user-give-feedback.php My Testemonial cross site scripting	A vulnerability has been found in CodeAstro Vehicle Booking System 1.0 and classified as problematic. This vulnerability affects unknown code of the file usr/user-give-feedback.php of the component Feedback Page. The manipulation of the argument My Testemonial leads to cross site scripting. This vulnerability was named CVE-2024-0346. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-51252	PublicCMS up to 4.0 Online Preview cross site scripting	A vulnerability was found in PublicCMS up to 4.0. It has been classified as problematic. Affected is an unknown function	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the component Online Preview. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-51252. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2023-50136	JFinalcms 5.0.0 New Custom Table Creation name cross site scripting	A vulnerability was found in JFinalcms 5.0.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component New Custom Table Creation. The manipulation of the argument name leads to cross site scripting. This vulnerability is known as CVE-2023-50136. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-47861	WWBN AVideo 11.6 HTTP Request channelBody.php cross site scripting (TALOS-2023-1884)	A vulnerability was found in WWBN AVideo 11.6. It has been classified as problematic. This affects an unknown part of the file channelBody.php of the component HTTP Request Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-47861. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2022-4958	qkmc-rk redbbs 1.0 Post title cross site scripting	A vulnerability classified as problematic has been found in qkmc-rk redbbs 1.0. Affected is an unknown function	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the component Post Handler. The manipulation of the argument title leads to cross site scripting. This vulnerability is traded as CVE-2022-4958. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2023-38827	Follet School Solutions Destiny 20_0_1_AU4 presentonesearchresultsform.do cross site scripting	A vulnerability was found in Follet School Solutions Destiny 20_0_1_AU4 and classified as problematic. This issue affects some unknown processing of the file presentonesearchresultsform.do. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-38827. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2022-4959	qkmc-rk redbbs 1.0 Nickname cross site scripting	A vulnerability classified as problematic was found in qkmc-rk redbbs 1.0. Affected by this vulnerability is an unknown functionality of the component Nickname Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2022-4959. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2020-26628	Hospital Management System 4.0 Edit Profile Page username cross site scripting (ID 176302)	A vulnerability has been found in Hospital Management System 4.0 and classified as problematic. This vulnerability affects unknown code of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component Edit Profile Page. The manipulation of the argument username leads to cross site scripting. This vulnerability was named CVE-2020-26628. The attack can be initiated remotely. There is no exploit available.		
CVE-2023-48728	WWBN AVideo 11.6 HTTP Request functiongetOpenGraph cross site scripting (TALOS-2023-1883)	A vulnerability classified as problematic was found in WWBN AVideo 11.6. Affected by this vulnerability is the function functiongetOpenGraph of the component HTTP Request Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-48728. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-0501	SourceCodester House Rental Management System 1.0 Manage Invoice Details cross site scripting	A vulnerability has been found in SourceCodester House Rental Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Manage Invoice Details. The manipulation of the argument Invoice leads to cross site scripting. This vulnerability is known as CVE-2024-0501. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-0499	SourceCodester House Rental Management System 1.0	A vulnerability which was classified as problematic has been found in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	index.php page cross site scripting	SourceCodester House Rental Management System 1.0. This issue affects some unknown processing of the file index.php. The manipulation of the argument page leads to cross site scripting. The identification of this vulnerability is CVE-2024-0499. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-0503	code-projects Online FIR System 1.0 registercomplaint.php Name/Address cross site scripting	A vulnerability was found in code-projects Online FIR System 1.0. It has been classified as problematic. This affects an unknown part of the file registercomplaint.php. The manipulation of the argument Name/Address leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-0503. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-0504	code-projects Simple Online Hotel Reservation System 1.0 Make a Reservation Page add_reserve.php Firstname/Lastname cross site scripting	A vulnerability has been found in code-projects Simple Online Hotel Reservation System 1.0 and classified as problematic. This vulnerability affects unknown code of the file add_reserve.php of the component Make a Reservation Page. The manipulation of the argument Firstname/Lastname with the input &lt;script&gt;alert&lt;/script&gt; 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-2024-0504. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-0476	Blood Bank & Donor Management 1.0 request-received-bydonar.php cross site scripting	A vulnerability which was classified as problematic was found in Blood Bank & Donor Management 1.0. This affects an unknown part of the file request-received-bydonar.php. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-0476. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-0500	SourceCodester House Rental Management System 1.0 Manage Tenant Details Name cross site scripting	A vulnerability which was classified as problematic was found in SourceCodester House Rental Management System 1.0. Affected is an unknown function of the component Manage Tenant Details. The manipulation of the argument Name leads to cross site scripting. This vulnerability is traded as CVE-2024-0500. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-7084	Voting Record Plugin up to 2.0 on WordPress cross site scripting	A vulnerability was found in Voting Record Plugin up to 2.0 on WordPress and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The identification of this vulnerability is CVE-2023-7084. The attack may be initiated remotely. There is no exploit available.		
CVE-2023-51063	QStar Archive Solutions 3-0 Build 7 Patch 0 qnme-ajax cross site scripting	A vulnerability which was classified as problematic has been found in QStar Archive Solutions 3-0 Build 7 Patch 0. This issue affects some unknown processing of the file qnme-ajaxmethodtree_level. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2023-51063. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-50072	OpenKM 7.1.40 Note Upload cross site scripting	A vulnerability which was classified as problematic was found in OpenKM 7.1.40. This affects an unknown part of the component Note Upload Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-50072. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-51067	QStar Archive Solutions 3-0 Build 7 Link cross site scripting	A vulnerability classified as problematic was found in QStar Archive Solutions 3-0 Build 7. Affected by this vulnerability is an unknown functionality of the component Link Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-51067. 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-2023-51064	QStar Archive Solutions 3-0 Build 7 Patch 0 qnme-ajax cross site scripting	A vulnerability which was classified as problematic was found in QStar Archive Solutions 3-0 Build 7 Patch 0. Affected is an unknown function of the file qnme-ajaxmethodtree_table. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-51064. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-51068	QStar Archive Solutions 3-0 Build 7 Link cross site scripting	A vulnerability which was classified as problematic has been found in QStar Archive Solutions 3-0 Build 7. Affected by this issue is some unknown functionality of the component Link Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-51068. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-0557	DedeBIZ 6.3.0 Website Copyright Setting cross site scripting	A vulnerability which was classified as problematic was found in DedeBIZ 6.3.0. This affects an unknown part of the component Website Copyright Setting. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-0557. It is possible to initiate the attack remotely. Furthermore there is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-0239	Contact Form 7 Connector Plugin up to 1.2.2 on WordPress cross site scripting (cdd-4354-8541)	A vulnerability which was classified as problematic has been found in Contact Form 7 Connector Plugin up to 1.2.2 on WordPress. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-0239. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2023-5558	LearnPress Plugin up to 4.2.5.4 on WordPress cross site scripting	A vulnerability which was classified as problematic was found in LearnPress Plugin up to 4.2.5.4 on WordPress. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-5558. 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-2024-0187	PeepSo Community Plugin up to 6.3.1.1 on WordPress cross site scripting	A vulnerability was found in PeepSo Community Plugin up to 6.3.1.1 on WordPress. It has been rated as problematic. This issue affects some unknown processing.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-0187. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2022-3739	WP Best Quiz Plugin up to 1.0 on WordPress cross site scripting	A vulnerability was found in WP Best Quiz Plugin up to 1.0 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-2022-3739. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-0599	Jspxcms 10.2.0 Document Management Page InfoController.java title cross site scripting	A vulnerability was found in Jspxcms 10.2.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file src\main\java\com\jspxcms\core\web\back\InfoController.java of the component Document Management Page. The manipulation of the argument title leads to cross site scripting. This vulnerability is known as CVE-2024-0599. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-0094	UpQode Google Maps Plugin up to 1.0.5 on WordPress	A vulnerability which was classified as problematic was found	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Shortcode Attribute cross site scripting	in UpQode Google Maps Plugin up to 1.0.5 on WordPress. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-0094. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2023-6046	EventON Plugin up to 2.1 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic was found in EventON Plugin up to 2.1 on WordPress. This affects an unknown part of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-6046. 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-2022-3829	Font Awesome 4 Menus Plugin up to 4.7.0 on WordPress Setting cross site scripting	A vulnerability was found in Font Awesome 4 Menus Plugin up to 4.7.0 on WordPress. It has been classified as problematic. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-3829. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-3647	INDIGITALL IURNY	A vulnerability which	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Plugin up to 3.2.2 on WordPress Setting cross site scripting	was classified as problematic has been found in INDIGITALL IURNY Plugin up to 3.2.2 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-2023-3647. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	core rule	
CVE-2021-24559	Qyrr Plugin 0.7 on WordPress AJAX Action data_uri_to_meta cross site scripting	A vulnerability classified as problematic was found in Qyrr Plugin 0.7 on WordPress. This vulnerability affects the function data_uri_to_meta of the component AJAX Action Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2021-24559. 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-2023-0376	Qubely Plugin up to 1.8.4 on WordPress Block Option cross site scripting	A vulnerability was found in Qubely Plugin up to 1.8.4 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Block Option Handler. 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 known as CVE-2023-0376. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-0389	Calculated Fields Form Plugin up to 1.1.150 on WordPress Setting cross site scripting	A vulnerability was found in Calculated Fields Form Plugin up to 1.1.150 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-0389. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2022-3194	weDevs Dokan Plugin up to 3.6.3 on WordPress cross site scripting	A vulnerability was found in weDevs Dokan Plugin up to 3.6.3 on WordPress and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2022-3194. 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-2023-6005	EventON Plugin up to 2.2.6/4.5.4 on WordPress Setting cross site scripting	A vulnerability was found in EventON Plugin up to 2.2.6/4.5.4 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-6005. 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-2023-6732	Supsystic Ultimate Maps Plugin up to 1.2.15 on WordPress Setting cross site scripting	A vulnerability was found in Supsystic Ultimate Maps Plugin up to 1.2.15 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-6732. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-22191	avo prior 3.2.4 key_value cross site scripting	A vulnerability was found in avo. It has been classified as problematic. This affects an unknown part. The manipulation of the argument key_value 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-2024-22191. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2021-24433	WP-FeedStats Simple Sort & Search Plugin up to 0.0.3 on WordPress URL Protocol indexurl cross site scripting	A vulnerability classified as problematic was found in WP-FeedStats Simple Sort & Search Plugin up to 0.0.3 on WordPress. Affected by this vulnerability is an unknown functionality of the component URL Protocol Handler. The manipulation of the argument indexurl leads to cross site scripting. This vulnerability is known as CVE-2021-24433. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-22491	beetl-bbs 2.0 post/save cross site scripting	A vulnerability has been found in beetl-bbs 2.0 and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument post/save leads to cross site scripting. This vulnerability was named CVE-2024-22491. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-0079	WooCommerce Customer Reviews Plugin up to 5.16.x on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in WooCommerce Customer Reviews Plugin up to 5.16.x on WordPress and classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		problematic. Affected by this issue is some unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-0079. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-7154	Hubbub Lite Plugin up to 1.31.x on WordPress Setting cross site scripting	A vulnerability was found in Hubbub Lite Plugin up to 1.31.x on WordPress. It has been declared as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-7154. 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-2022-23179	Contact Form & Lead Form Elementor Builder Plugin up to 1.6.x on WordPress cross site scripting	A vulnerability classified as problematic has been found in Contact Form & Lead Form Elementor Builder Plugin up to 1.6.x on WordPress. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-23179. It is possible to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-7151	WooCommerce Product Enquiry Plugin up to 3.1 on WordPress page cross site scripting	A vulnerability was found in WooCommerce Product Enquiry Plugin up to 3.1 on WordPress and classified as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument page leads to cross site scripting. This vulnerability is handled as CVE-2023-7151. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2021-24567	Simple Post Plugin up to 1.1 on WordPress Text cross site scripting	A vulnerability which was classified as problematic was found in Simple Post Plugin up to 1.1 on WordPress. This affects an unknown part. The manipulation of the argument Text leads to cross site scripting. This vulnerability is uniquely identified as CVE-2021-24567. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2021-24432	Advanced AJAX Product Filters Plugin prior 1.5.4.7 on WordPress POST Parameter term_id cross site scripting	A vulnerability was found in Advanced AJAX Product Filters Plugin on WordPress. It has been classified as problematic. Affected is an unknown function of the component POST Parameter	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Handler. The manipulation of the argument term_id leads to cross site scripting. This vulnerability is traded as CVE-2021-24432. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2022-0402	Super Forms Plugin up to 6.0.3 on WordPress AJAX Action bob_czy_panstwa_sprawa_zostala_rozwiazana cross site scripting	A vulnerability which was classified as problematic has been found in Super Forms Plugin up to 6.0.3 on WordPress. Affected by this issue is some unknown functionality of the component AJAX Action Handler. The manipulation of the argument bob_czy_panstwa_sprawa_zostala_rozwiazana leads to cross site scripting. This vulnerability is handled as CVE-2022-0402. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2022-2413	simonpedge Slide Anything Plugin up to 2.3.46 on WordPress cross site scripting	A vulnerability was found in simonpedge Slide Anything Plugin up to 2.3.46 on WordPress and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2022-2413. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2022-3836	Seed Social Plugin up to 2.0.3 on WordPress Setting cross site scripting	A vulnerability was found in Seed Social Plugin up to 2.0.3 on WordPress. It has been classified as problematic. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2022-3836. 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-2024-0650	Project Worlds Visitor Management System 1.0 URL dataset.php name cross site scripting	A vulnerability was found in Project Worlds Visitor Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file dataset.php of the component URL Handler. The manipulation of the argument name with the input &quot;&gt;&lt;script&gt;alert&lt;/script&gt; leads to cross site scripting. This vulnerability is traded as CVE-2024-0650. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-36236	Webkil Bagisto up to 1.5.0 SVG File	A vulnerability classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Upload cross site scripting	problematic was found in Webkil Bagisto up to 1.5.0. This vulnerability affects unknown code of the component SVG File Upload. The manipulation leads to cross site scripting. This vulnerability was named CVE-2023-36236. The attack can be initiated remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.		
CVE-2024-22714	Stupid Simple CMS up to 1.2.4 Editing Section cross site scripting	A vulnerability was found in Stupid Simple CMS up to 1.2.4 and classified as problematic. Affected by this issue is some unknown functionality of the component Editing Section. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-22714. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-0652	PHPGurukul Company Visitor Management System 1.0 search-visitor.php cross site scripting	A vulnerability was found in PHPGurukul Company Visitor Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file search-visitor.php. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-0652. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-46952	ABO.CMS 5.9.3	A vulnerability was	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	HTTP Header Referer cross site scripting	found in ABO.CMS 5.9.3. It has been classified as problematic. This affects an unknown part of the component HTTP Header Handler. The manipulation of the argument Referer leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-46952. It is possible to initiate the attack remotely. There is no exploit available.	core rule	
CVE-2024-0647	Sparksuite SimpleMDE up to 1.11.2 iFrame cross site scripting	A vulnerability which was classified as problematic was found in Sparksuite SimpleMDE up to 1.11.2. This affects an unknown part of the component iFrame Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-0647. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-25295	GRN eVEWA3 Community up to 53 Login Panel cross site scripting	A vulnerability was found in GRN eVEWA3 Community up to 53 and classified as problematic. Affected by this issue is some unknown functionality of the component Login Panel. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-25295. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-51807	OFCMS 1.14 Title Addition cross site	A vulnerability which was classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	scripting	problematic was found in OFCMS 1.14. Affected is an unknown function of the component Title Addition. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2023-51807. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2024-22411	avo up to 2.x on Ruby Notifications Avo::BaseAction cross site scripting (GHSA-g8vp-2v5p-9qfh)	A vulnerability was found in avo up to 2.x on Ruby. It has been classified as problematic. Affected is the function Avo::BaseAction of the component Notifications Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-22411. 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-2023-48858	Armex ABO.CMS 5.9 Login Page login.php cross site scripting	A vulnerability which was classified as problematic was found in Armex ABO.CMS 5.9. This affects an unknown part of the file login.php of the component Login Page. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-48858. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-22414	DogukanUrker flaskBlog HTML Template /user/	A vulnerability which was classified as problematic has been	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	cross site scripting (GHSA-mrcw-j96f-p6v6)	found in DogukanUrker flaskBlog. Affected by this issue is some unknown functionality of the file /user/ of the component HTML Template. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-22414. The attack may be launched remotely. There is no exploit available.		
CVE-2024-0776	LinZhaoguan pb-cms 2.0 Comment cross site scripting	A vulnerability which was classified as problematic has been found in LinZhaoguan pb-cms 2.0. Affected by this issue is some unknown functionality of the component Comment Handler. The manipulation with the input &lt;div onmouseenter&quot;alert&quot;&gt; leads to cross site scripting. This vulnerability is handled as CVE-2024-0776. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-0773	CodeAstro Internet Banking System 1.0 pages_client_signup.php Client Full Name cross site scripting	A vulnerability classified as problematic was found in CodeAstro Internet Banking System 1.0. Affected by this vulnerability is an unknown functionality of the file pages_client_signup.php. The manipulation of the argument Client Full Name leads to cross site scripting. This vulnerability is known as CVE-2024-0773. The attack can be launched remotely. Furthermore there is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		an exploit available.		
CVE-2023-6290	SEOPress Plugin up to 7.2 on WordPress Setting cross site scripting	A vulnerability was found in SEOPress Plugin up to 7.2 on WordPress and classified as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-6290. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2023-6456	WP Review Slider Plugin up to 12.x on WordPress Setting cross site scripting	A vulnerability was found in WP Review Slider Plugin up to 12.x 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-2023-6456. 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-2023-7170	EventON-RSVP Plugin up to 2.9.4 on WordPress cross site scripting	A vulnerability classified as problematic has been found in EventON-RSVP Plugin up to 2.9.4 on WordPress. Affected is an unknown function. 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 traded as CVE-2023-7170. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-6626	Product Enquiry for WooCommerce Plugin up to 3.0 on WordPress Setting cross site scripting	A vulnerability has been found in Product Enquiry for WooCommerce Plugin up to 3.0 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 scripting. This vulnerability is known as CVE-2023-6626. 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-2023-7194	Meris Theme up to 1.1.2 on WordPress cross site scripting	A vulnerability was found in Meris Theme up to 1.1.2 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-2023-7194. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-22497	JFinalcms 5.0.0 URL /admin/login password cross site scripting	A vulnerability which was classified as problematic was found in JFinalcms 5.0.0. This affects an unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		part of the file /admin/login of the component URL Handler. The manipulation of the argument password leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-22497. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-22496	JFinalcms 5.0.0 /admin/login username cross site scripting	A vulnerability was found in JFinalcms 5.0.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/login. The manipulation of the argument username leads to cross site scripting. This vulnerability is known as CVE-2024-22496. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-22490	beetl-bbs 2.0 /index keyword cross site scripting	A vulnerability was found in beetl-bbs 2.0. It has been classified as problematic. Affected is an unknown function of the file /index. The manipulation of the argument keyword leads to cross site scripting. This vulnerability is traded as CVE-2024-22490. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-22720	Kanboard 1.2.34 Group Management cross site scripting	A vulnerability which was classified as problematic has been found in Kanboard 1.2.34. This issue	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects some unknown processing of the component Group Management. The manipulation leads to basic cross site scripting. The identification of this vulnerability is CVE-2024-22720. The attack may be initiated remotely. There is no exploit available.		
CVE-2024-0249	Advanced Schedule Posts Plugin up to 2.1.8 on WordPress cross site scripting	A vulnerability which was classified as problematic was found in Advanced Schedule Posts Plugin up to 2.1.8 on WordPress. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-0249. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y

Host Header Injection

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-50093	APIIDA API Gateway Manager for Broadcom Layer7 2023.2.2 Header Host injection	A vulnerability which was classified as problematic was found in APIIDA API Gateway Manager for Broadcom Layer7 2023.2.2. This affects an unknown part of the component Header Handler. The manipulation of the argument Host leads to injection. This vulnerability is uniquely identified as CVE-2023-50093. The attack needs to be approached within the local network. There is no exploit available.	Patched by default in SaaS	Y
CVE-2024-23648	Pimcore admin-ui-classic-bundle up to 1.2.2 injection (GHSA-mrqg-mwh7-q94j)	A vulnerability was found in Pimcore admin-ui-classic-bundle up to 1.2.2. It has been rated as very critical. Affected by this issue is some unknown functionality. The manipulation leads to injection. This vulnerability is handled as CVE-2024-23648. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by default in SaaS	Y

XML External Entity Vulnerability

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-45139	fonttools prior 4.43.0 xml external entity reference (GHSA-6673-4983)	A vulnerability has been found in fonttools and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to xml external entity reference. This vulnerability is known as CVE-2023-45139. 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-2024-23525	Spreadsheet::ParseXLSX up to 0.29 on Perl XML::Twig no_xxe xml external entity reference (Issue 10)	A vulnerability was found in Spreadsheet::ParseXLSX up to 0.29 on Perl and classified as critical. This issue affects the function XML::Twig. The manipulation of the argument no_xxe leads to xml external entity reference. The identification of this vulnerability is CVE-2024-23525. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y

INDUSFACE™

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.

Gartner Peer Insights Customers' Choice 2023™

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™

CONTACT US - +91 265 6133021 | +1 866 537 8234