INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

September 2024

The total **zero-day vulnerabilities** count for August month: 313

Command Injection	CSRF	SQL Injection	Local File Inclusion	Cross-Site Scripting
37	30	81	22	143

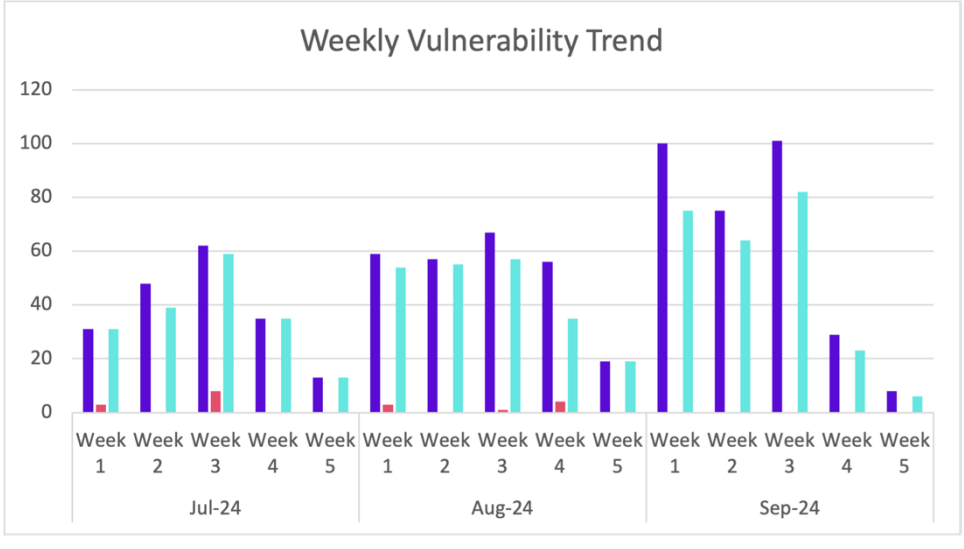
Zero-day vulnerabilities protected through core rules	313
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities found by Indusface WAS	250

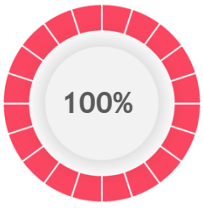
- To enable custom rules, please contact support@indusface.com
- Learn more about zero-day vulnerabilities, detection, and prevention, here

Vulnerability Trend:

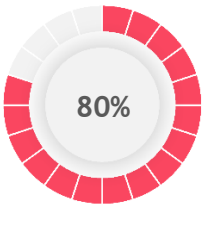
The weekly trend displays the total number of vulnerabilities discovered and the type of protection provided for the last quarter.

Weekly Vulnerability Trend



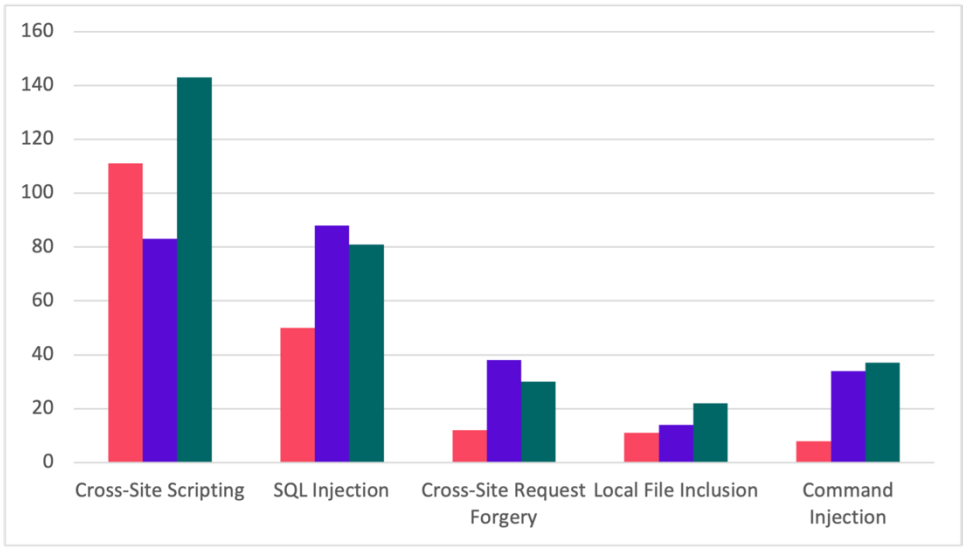


of the zero-day vulnerabilities were protected by the core rules in the last month



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

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-8234	Zyxel NWA1100-N 1.00(AACE.1)C0 formSysCmd/formUpgradeCert/formDelcert os command injection	A vulnerability was found in Zyxel NWA1100-N 1.00C0 and classified as critical. This issue affects the function formSysCmd/formUpgradeCert/formDelcert. The manipulation leads to os command injection. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. The identification of this vulnerability is CVE-2024-8234. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	N
CVE-2024-45302	RestSharp up to 111.x RestRequest.AddHeader crlf injection (GHSA-4rr6-2v9v-wcpc)	A vulnerability has been found in RestSharp up to 111.x and classified as critical. This vulnerability affects the function RestRequest.AddHeader. The manipulation leads to crlf injection. This vulnerability was named CVE-2024-45302. The attack can be initiated 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-2024-44916	SeaCMS 13.1 admin_ip.php command injection	A vulnerability which was classified as critical was found in SeaCMS 13.1. This affects an unknown part of the file admin_ip.php. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2024-44916. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-44916	SeaCMS 13.1 admin_ip.php command injection	A vulnerability which was classified as critical was found in SeaCMS 13.1. This affects an unknown part of the file admin_ip.php. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2024-44916. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-44400	D-Link DI-8400 16.07.26A1 upgrade_filter_asp command injection	A vulnerability has been found in D-Link DI-8400 16.07.26A1 and classified as critical. This vulnerability affects the function upgrade_filter_asp. The manipulation leads to command injection. This vulnerability was named CVE-2024-44400. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-8523	lmxcms up to 1.4 SQL Command Execution Module admin.php formatData data code injection	A vulnerability was found in lmxcms up to 1.4 and classified as critical. Affected by this issue is the function formatData of the file /admin.phpmAcquisi&atestcj&lid1 of the component SQL Command Execution Module. The manipulation of the argument data leads to code injection. This vulnerability is handled as CVE-2024-8523. The attack may 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. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-44408	D-Link DIR-823G 1.0.2B05_20181207 Configuration File information disclosure	A vulnerability which was classified as problematic was found in D-Link DIR-823G 1.0.2B05_20181207. Affected is an unknown function of the component Configuration File Handler. The manipulation leads to information disclosure. This vulnerability is traded as CVE-2024-44408. Access to the local network is required for this attack to succeed. There is no exploit available.	Patched by core rule	Y
CVE-2024-44401	D-Link DI-8100G 17.12.20A1 upgrade_filter.asp sub47A60C command injection	A vulnerability classified as critical was found in D-Link DI-8100G 17.12.20A1. Affected by this vulnerability is the function sub47A60C of the file upgrade_filter.asp. The manipulation leads to command injection. This vulnerability is known as CVE-2024-44401. The attack can be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-44402	D-Link DI-8100G 17.12.20A1 msp_info.htm command injection	A vulnerability which was classified as critical was found in D-Link DI-8100G 17.12.20A1. Affected is an unknown function of the file msp_info.htm. The manipulation leads to command injection. This vulnerability is traded as CVE-2024-44402. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-44845	DrayTek Vigor3900 1.5.1.6 filter_string value command injection	A vulnerability was found in DrayTek Vigor3900 1.5.1.6. It has been rated as critical. Affected by this issue is the function filter_string. The manipulation of the	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument value leads to command injection. This vulnerability is handled as CVE-2024-44845. The attack may be launched remotely. There is no exploit available.		
CVE-2024-44844	DrayTek Vigor3900 1.5.1.6 run_command name command injection	A vulnerability was found in DrayTek Vigor3900 1.5.1.6. It has been declared as critical. Affected by this vulnerability is the function run_command. The manipulation of the argument name leads to command injection. This vulnerability is known as CVE-2024-44844. The attack can be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-8574	TOTOLINK AC1200 T8 4.1.5cu.861_B20230220 /cgi-bin/cstecgi.cgi setParentalRules slaveIpList os command injection	A vulnerability has been found in TOTOLINK AC1200 T8 4.1.5cu.861_B20230220 and classified as critical. This vulnerability affects the function setParentalRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument slaveIpList leads to os command injection. This vulnerability was named CVE-2024-8574. 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-2024-44410	D-Link DI-8300 16.07.26A1 upgrade_filter_asp command injection	A vulnerability classified as critical has been found in D-Link DI-8300 16.07.26A1. This affects the function upgrade_filter_asp. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2024-44410. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-44411	D-Link DI-8300 16.07.26A1 msp_info_htm command injection	A vulnerability classified as critical was found in D-Link DI-8300 16.07.26A1. This vulnerability affects the function msp_info_htm. The manipulation leads to command injection. This vulnerability was named CVE-2024-44411. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2023-36103	Tenda AC15 15.03.05.20 POST Request goform/SetIPTVCfg command injection	A vulnerability was found in Tenda AC15 15.03.05.20. It has been rated as critical. Affected by this issue is some unknown functionality of the file goform/SetIPTVCfg of the component POST Request Handler. The manipulation leads to command injection. This vulnerability is handled as CVE-2023-36103. The attack may be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-44466	Comfast CF-XR11 2.7.2 HTTP POST Request /usr/bin/webmgnt sub_424CB4 iface command injection	A vulnerability which was classified as critical has been found in Comfast CF-XR11 2.7.2. This issue affects the function sub_424CB4 of the file /usr/bin/webmgnt of the component HTTP POST Request Handler. The manipulation of the argument iface leads to command injection. The identification of this vulnerability is CVE-2024-44466. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-6091	significant-gravitas AutoGPT up to 0.5.0 Denylist Setting os command injection	A vulnerability which was classified as very critical was found in significant-gravitas AutoGPT up to 0.5.0. Affected is an unknown function of the component Denylist Setting Handler. The manipulation 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
		6091. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-7129	Appointment Booking Calendar Plugin up to 1.6.7.42 on WordPress Twig Template os command injection	A vulnerability was found in Appointment Booking Calendar Plugin up to 1.6.7.42 on WordPress and classified as critical. Affected by this issue is some unknown functionality of the component Twig Template Handler. The manipulation leads to os command injection. This vulnerability is handled as CVE-2024-7129. 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-2024-46048	Tenda FH451 1.0.0.9 formexeCommand command injection	A vulnerability was found in Tenda FH451 1.0.0.9. It has been classified as critical. Affected is the function formexeCommand. The manipulation leads to command injection. This vulnerability is traded as CVE-2024-46048. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	N
CVE-2024-8864	composiohq composio up to 0.5.6 calculator.py Calculator code injection	A vulnerability has been found in composiohq composio up to 0.5.6 and classified as critical. Affected by this vulnerability is the function Calculator of the file python/composio/tools/local/mathematical/actions/calculator.py. The manipulation leads to code injection. This vulnerability is known as CVE-2024-8864. The attack needs to be approached within the local network. Furthermore there is an exploit	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-6258	zephyrproject-rtos Zephyr up to 3.6 BT rfcomm_handle_data net_buf heap-based overflow (GHSA-7833-fcpm-3ggm)	A vulnerability has been found in zephyrproject-rtos Zephyr up to 3.6 and classified as critical. This vulnerability affects the function rfcomm_handle_data of the component BT. The manipulation of the argument net_buf leads to heap-based buffer overflow. This vulnerability was named CVE-2024-6258. Access to the local network is required for this attack. There is no exploit available.	Patched by core rule	Y
CVE-2024-8211	D-Link DNS-1550-04 up to 20240814 /cgi-bin/hd_config.cgi cgi_FMT_Std2R1_DiskMGR f_newly_dev command injection (SAP10383)	A vulnerability was found in D-Link DNS-120 DNR-202L DNS-315L DNS-320 DNS-320L DNS-320LW DNS-321 DNR-322L DNS-323 DNS-325 DNS-326 DNS-327L DNR-326 DNS-340L DNS-343 DNS-345 DNS-726-4 DNS-1100-4 DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_Std2R1_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_newly_dev leads to command injection. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability was named CVE-2024-8211. The attack can be initiated remotely. Furthermore there is an exploit available. Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. It is recommended to replace the affected	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component with an alternative.		
CVE-2024-8210	D-Link DNS-1550-04 up to 20240814 /cgi-bin/hd_config.cgi sprintf f_mount command injection (SAP10383)	A vulnerability was found in D-Link DNS-120 DNR-202L DNS-315L DNS-320 DNS-320L DNS-320LW DNS-321 DNR-322L DNS-323 DNS-325 DNS-326 DNS-327L DNR-326 DNS-340L DNS-343 DNS-345 DNS-726-4 DNS-1100-4 DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function sprintf of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_mount leads to command injection. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability is uniquely identified as CVE-2024-8210. It is possible to initiate the attack remotely. Furthermore there is an exploit available. Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. It is recommended to replace the affected component with an alternative.	Patched by core rule	N
CVE-2024-8214	D-Link DNS-1550-04 up to 20240814 /cgi-bin/hd_config.cgi cgi_FMT_Std2R5_2nd_DiskMGR f_source_dev command injection (SAP10383)	A vulnerability classified as critical was found in D-Link DNS-120 DNR-202L DNS-315L DNS-320 DNS-320L DNS-320LW DNS-321 DNR-322L DNS-323 DNS-325 DNS-326 DNS-327L DNR-326 DNS-340L DNS-343 DNS-345 DNS-726-4 DNS-1100-4 DNS-1200-05 and DNS-1550-04 up to 20240814. Affected by this vulnerability is the function cgi_FMT_Std2R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection.	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability is known as CVE-2024-8214. The attack can be launched remotely. Furthermore there is an exploit available. Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. It is recommended to replace the affected component with an alternative.		
CVE-2024-8213	D-Link DNS-1550-04 up to 20240814 /cgi-bin/hd_config.cgi cgi_FMT_R12R5_1st_DiskMGR f_source_dev command injection (SAP10383)	A vulnerability classified as critical has been found in D-Link DNS-120 DNR-202L DNS-315L DNS-320 DNS-320L DNS-320LW DNS-321 DNR-322L DNS-323 DNS-325 DNS-326 DNS-327L DNR-326 DNS-340L DNS-343 DNS-345 DNS-726-4 DNS-1100-4 DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_FMT_R12R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability is traded as CVE-2024-8213. It is possible to launch the attack remotely. Furthermore there is an exploit available. Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. It is recommended to replace the affected component with an alternative.	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-8212	D-Link DNS-1550-04 up to 20240814 /cgi-bin/hd_config.cgi cgi_FMT_R12R5_2nd_DiskMGR f_source_dev command injection (SAP10383)	A vulnerability was found in D-Link DNS-120 DNR-202L DNS-315L DNS-320 DNS-320L DNS-320LW DNS-321 DNR-322L DNS-323 DNS-325 DNS-326 DNS-327L DNR-326 DNS-340L DNS-343 DNS-345 DNS-726-4 DNS-1100-4 DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_R12R5_2nd_DiskMGR of the file /cgi-bin/hd_config.cgi. The manipulation of the argument f_source_dev leads to command injection. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. The identification of this vulnerability is CVE-2024-8212. The attack may be initiated remotely. Furthermore there is an exploit available. Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced. It is recommended to replace the affected component with an alternative.	Patched by core rule	N
CVE-2024-43804	Roxy-WI up to 8.0 server_mod.subprocess_execute os command injection (GHSA-qc52-vwwj-5585)	A vulnerability was found in Roxy-WI up to 8.0. It has been declared as critical. This vulnerability affects the function server_mod.subprocess_execute. The manipulation leads to os command injection. This vulnerability was named CVE-2024-43804. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-44845	DrayTek Vigor3900 1.5.1.6 filter_string value command injection	A vulnerability was found in DrayTek Vigor3900 1.5.1.6. It has been rated as critical. Affected by this	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		issue is the function filter_string. The manipulation of the argument value leads to command injection. This vulnerability is handled as CVE-2024-44845. The attack may be launched remotely. There is no exploit available.		
CVE-2024-44844	DrayTek Vigor3900 1.5.1.6 run_command name command injection	A vulnerability was found in DrayTek Vigor3900 1.5.1.6. It has been declared as critical. Affected by this vulnerability is the function run_command. The manipulation of the argument name leads to command injection. This vulnerability is known as CVE-2024-44844. The attack can be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-8574	TOTOLINK AC1200 T8 4.1.5cu.861_B20230220 /cgi-bin/cstecgi.cgi setParentalRules slaveIpList os command injection	A vulnerability has been found in TOTOLINK AC1200 T8 4.1.5cu.861_B20230220 and classified as critical. This vulnerability affects the function setParentalRules of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument slaveIpList leads to os command injection. This vulnerability was named CVE-2024-8574. 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-2023-36103	Tenda AC15 15.03.05.20 POST Request goform/SetIPTVCfg command injection	A vulnerability was found in Tenda AC15 15.03.05.20. It has been rated as critical. Affected by this issue is some unknown functionality of the file goform/SetIPTVCfg of the component POST Request Handler. 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 handled as CVE-2023-36103. The attack may be launched remotely. There is no exploit available.		
CVE-2024-44466	Comfast CF-XR11 2.7.2 HTTP POST Request /usr/bin/webmgnt sub_424CB4 iface command injection	A vulnerability which was classified as critical has been found in Comfast CF-XR11 2.7.2. This issue affects the function sub_424CB4 of the file /usr/bin/webmgnt of the component HTTP POST Request Handler. The manipulation of the argument iface leads to command injection. The identification of this vulnerability is CVE-2024-44466. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-46048	Tenda FH451 1.0.0.9 formexeCommand command injection	A vulnerability was found in Tenda FH451 1.0.0.9. It has been classified as critical. Affected is the function formexeCommand. The manipulation leads to command injection. This vulnerability is traded as CVE-2024-46048. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	N
CVE-2024-9001	TOTOLINK T10 4.1.8cu.5207 /cgi-bin/cstecgi.cgi setTracerouteCfg command os command injection	A vulnerability was found in TOTOLINK T10 4.1.8cu.5207. It has been declared as critical. This vulnerability affects the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument command leads to os command injection. This vulnerability was named CVE-2024-9001. 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-2024-9006	jeanmarc77 123solar	A vulnerability was	Patched by	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	1.8.4.5 config/config_invt1.php PASSOx code injection (Issue 74)	found in jeanmarc77 123solar 1.8.4.5. It has been rated as critical. Affected by this issue is some unknown functionality of the file config/config_invt1.php. The manipulation of the argument PASSOx leads to code injection. This vulnerability is handled as CVE-2024-9006. The attack may be launched remotely. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue.	core rule	
CVE-2024-9004	D-Link DAR-7000 up to 20240912 Backup_Server_commit.php host os command injection (SAP10354)	A vulnerability classified as critical has been found in D-Link DAR-7000 up to 20240912. Affected is an unknown function of the file /view/DBManage/Backup_Server_commit.php. The manipulation of the argument host leads to os command injection. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability is traded as CVE-2024-9004. It is possible to launch the attack remotely. Furthermore there is an exploit available. It is recommended to replace the affected component with an alternative.	Patched by core rule	N
CVE-2024-6845	Chatbot with ChatGPT Plugin up to 2.4.5 on WordPress REST Endpoint authorization	A vulnerability was found in Chatbot with ChatGPT Plugin up to 2.4.5 on WordPress. It has been declared as problematic. This vulnerability affects unknown code of the component REST Endpoint. The manipulation leads to incorrect authorization. This vulnerability was named CVE-2024-6845. The attack can be initiated 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.		

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-7861	Misiek Paypal Plugin up to 1.1.20090324 on WordPress cross-site request forgery	A vulnerability was found in Misiek Paypal Plugin up to 1.1.20090324 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2024-7861. The attack may be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-42791	Kashipara Music Management System 1.0 ajax.php cross-site request forgery	A vulnerability classified as problematic was found in Kashipara Music Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /music/ajax.phpactiondelete_genre. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2024-42791. The attack can be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-7820	ILC Thickbox Plugin up to 1.0 on WordPress Setting cross-site request forgery	A vulnerability was found in ILC Thickbox Plugin up to 1.0 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 request forgery. This vulnerability is known as CVE-2024-7820. The attack can be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-7862	Blog Introduction Plugin up to 0.3.0 on WordPress Setting cross-site request forgery	A vulnerability classified as problematic was found in Blog Introduction Plugin up to 0.3.0 on WordPress. This vulnerability affects unknown code of the component Setting	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Handler. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2024-7862. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-7860	Simple Headline Rotator PLugin up to 1.0 on WordPress cross-site request forgery	A vulnerability classified as problematic has been found in Simple Headline Rotator PLugin up to 1.0 on WordPress. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2024-7860. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-8197	freakingwildchild Visual Sound Plugin up to 1.03 on WordPress Setting cross-site request forgery	A vulnerability which was classified as problematic was found in freakingwildchild Visual Sound Plugin up to 1.03 on WordPress. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-8197. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-7863	Favicon Generator Plugin up to 1.5 on WordPress File Upload cross-site request forgery	A vulnerability which was classified as problematic was found in Favicon Generator Plugin up to 1.5 on WordPress. Affected is an unknown function of the component File Upload. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-7863. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-8043	Vikinghammer Tweet Plugin up to 0.2.4 on WordPress cross-site request forgery	A vulnerability which was classified as problematic has been found in Vikinghammer Tweet Plugin up to 0.2.4	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		on WordPress. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2024-8043. The attack may be launched remotely. There is no exploit available.		
CVE-2024-8052	Review Ratings Plugin up to 1.6 on WordPress cross-site request forgery	A vulnerability classified as problematic was found in Review Ratings Plugin up to 1.6 on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2024-8052. The attack can be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-8091	Enhanced Search Box Plugin up to 0.6.1 on WordPress Setting cross-site request forgery	A vulnerability has been found in Enhanced Search Box Plugin up to 0.6.1 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-2024-8091. The attack can be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-8044	infolinks Ad Wrap Plugin up to 1.0.2 on WordPress Setting cross-site request forgery	A vulnerability was found in infolinks Ad Wrap Plugin up to 1.0.2 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 request forgery. This vulnerability is handled as CVE-2024-8044. The attack may be launched remotely. There is no exploit available.	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-8047	Visual Sound Plugin up to 1.06 on WordPress Setting cross-site request forgery	A vulnerability classified as problematic has been found in Visual Sound Plugin up to 1.06 on WordPress. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-8047. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-7690	DN Popup Plugin up to 1.2.2 on WordPress Setting cross-site request forgery	A vulnerability was found in DN Popup Plugin up to 1.2.2 on WordPress and classified 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-2024-7690. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-7688	AZIndex Plugin up to 0.8.1 on WordPress cross-site request forgery	A vulnerability was found in AZIndex Plugin up to 0.8.1 on WordPress. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-7688. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-7687	AZIndex Plugin up to 0.8.1 on WordPress cross-site request forgery	A vulnerability was found in AZIndex Plugin up to 0.8.1 on WordPress and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-7687. The attack may be initiated remotely. There is no	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit available.		
CVE-2024-7817	Misiek Photo Album Plugin up to 1.4.3 on WordPress cross-site request forgery	A vulnerability was found in Misiek Photo Album Plugin up to 1.4.3 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2024-7817. The attack may be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-7818	Misiek Photo Album Plugin up to 1.4.3 on WordPress cross-site request forgery	A vulnerability was found in Misiek Photo Album Plugin up to 1.4.3 on WordPress and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-7818. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-8054	MM-Breaking News Plugin up to 0.7.9 on WordPress cross-site request forgery	A vulnerability was found in MM-Breaking News Plugin up to 0.7.9 on WordPress. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-8054. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-7859	Visual Sound Plugin up to 1.03 on WordPress Setting cross-site request forgery	A vulnerability has been found in Visual Sound Plugin up to 1.03 on WordPress and classified as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2024-7859. The attack can be	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		initiated remotely. There is no exploit available.		
CVE-2024-3163	Easy Property Listings Plugin up to 3.5.3 on WordPress cross-site request forgery	A vulnerability classified as problematic was found in Easy Property Listings Plugin up to 3.5.3 on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2024-3163. 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-2024-7864	Favicon Generator Plugin up to 2.0 on WordPress Path Validation output_sub_admin_page_0 cross-site request forgery	A vulnerability was found in Favicon Generator Plugin up to 2.0 on WordPress and classified as problematic. This issue affects the function output_sub_admin_page_0 of the component Path Validation Handler. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-7864. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	N
CVE-2024-6862	lunary-ai lunary up to 1.4.9 cross-site request forgery	A vulnerability has been found in lunary-ai lunary up to 1.4.9 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2024-6862. 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-2024-42792	Kashipara Music Management	A vulnerability was found in Kashipara	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	System 1.0 ajax.php cross-site request forgery	Music Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /music/ajax.phpactiondelete_playlist. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2024-42792. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-6017	Music Request Manager Plugin up to 1.3 on WordPress cross-site request forgery	A vulnerability which was classified as problematic has been found in Music Request Manager Plugin up to 1.3 on WordPress. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-6017. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-42793	Kashipara Music Management System 1.0 ajax.php cross-site request forgery	A vulnerability was found in Kashipara Music Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /music/ajax.phpactionsave_user. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2024-42793. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-8414	SourceCodester Insurance Management System 1.0 cross-site request forgery	A vulnerability has been found in SourceCodester Insurance Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2024-8414. The attack can be launched remotely. Furthermore there is an	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit available.		
CVE-2024-8093	Posts Reminder Plugin up to 0.20 on WordPress Setting cross-site request forgery	A vulnerability has been found in Posts Reminder Plugin up to 0.20 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-2024-8093. The attack can be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-46086	FrogCMS 0.9.5 cross-site request forgery	A vulnerability was found in FrogCMS 0.9.5 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin//plugin/file_manager/delete/123. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2024-46086. The attack may be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-46394	FrogCMS 0.9.5 /admin/ cross-site request forgery	A vulnerability was found in FrogCMS 0.9.5. It has been classified as problematic. This affects an unknown part of the file /admin//user/add. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2024-46394. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-7892	adstxt Plugin up to 1.0.0 on WordPress Setting cross-site request forgery	A vulnerability was found in adstxt Plugin up to 1.0.0 on WordPress. It has been classified as problematic. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2024-7892. It is	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		possible to initiate the attack remotely. There is no exploit available.		

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-42471	actions toolkit up to 2.1.6 path traversal	A vulnerability was found in actions toolkit up to 2.1.6. It has been rated as critical. Affected by this issue is some unknown functionality. The manipulation leads to path traversal. This vulnerability is handled as CVE-2024-42471. 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-2024-43797	advplyr audiobookshelf up to 2.12.x Role-Based Access Control path traversal	A vulnerability classified as critical has been found in advplyr audiobookshelf up to 2.12.x. This affects an unknown part of the component Role-Based Access Control. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2024-43797. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-44720	SeaCMS 13.1 admin_safe.php path traversal (Issue 22)	A vulnerability was found in SeaCMS 13.1. It has been rated as problematic. Affected by this issue is some unknown functionality of the file admin_safe.php.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The manipulation leads to path traversal. This vulnerability is handled as CVE-2024-44720. Access to the local network is required for this attack. There is no exploit available.		
CVE-2024-44867	PHPOK 3.0 /autoload/file.php path traversal	A vulnerability was found in PHPOK 3.0. It has been declared as problematic. This vulnerability affects unknown code of the file /autoload/file.php. The manipulation leads to path traversal. This vulnerability was named CVE-2024-44867. The attack can only be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-8711	SourceCodester Food Ordering Management System 1.0 /includes/ exposure of information through directory listing	A vulnerability which was classified as problematic has been found in SourceCodester Food Ordering Management System 1.0. Affected by this issue is some unknown functionality of the file /includes/. The manipulation leads to exposure of information through directory listing. This vulnerability is handled as CVE-2024-8711. The attack may be launched remotely. Furthermore there is an exploit available. It is recommended to apply restrictive	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		firewalling.		
CVE-2024-8706	JFinalCMS up to 20240903 com.cms.util.TemplateUtils /admin/template/update fileName path traversal (IAOSJG)	A vulnerability was found in JFinalCMS up to 20240903. It has been classified as problematic. This affects the function update of the file /admin/template/update of the component com.cms.util.TemplateUtils. The manipulation of the argument fileName leads to path traversal. This vulnerability is uniquely identified as CVE-2024-8706. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8694	JFinalCMS up to 20240903 com.cms.controller.admin.TemplateController /admin/template/update fileName path traversal (IAOKSQ)	A vulnerability which was classified as problematic was found in JFinalCMS up to 20240903. This affects the function update of the file /admin/template/update of the component com.cms.controller.admin.TemplateController. The manipulation of the argument fileName leads to path traversal. This vulnerability is uniquely identified as CVE-2024-8694. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8782	JFinalCMS up to 1.0 /admin/template/edit delete name path traversal (IAOSJG)	A vulnerability was found in JFinalCMS up to 1.0. It has been rated as critical. This issue affects the function delete of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/admin/template/edit. The manipulation of the argument name leads to path traversal. The identification of this vulnerability is CVE-2024-8782. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-8865	composiohq composio up to 0.5.8 composio\server\api.py path file path traversal	A vulnerability was found in composiohq composio up to 0.5.8 and classified as problematic. Affected by this issue is the function path of the file composio\server\api.py. The manipulation of the argument file leads to path traversal. This vulnerability is handled as CVE-2024-8865. The attack can only be done within the local network. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-8875	vedees wcms up to 0.3.2 /wex/finder.php path traversal	A vulnerability classified as critical was found in vedees wcms up to 0.3.2. Affected by this vulnerability is an unknown functionality of the file /wex/finder.php. The manipulation of the argument p leads to path traversal. This vulnerability is known as CVE-2024-8875. The attack can be launched	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-8876	xiaohe4966 TpMeCMS up to 1.3.3.1 /index/ajax/lang path traversal	A vulnerability which was classified as problematic has been found in xiaohe4966 TpMeCMS up to 1.3.3.1. Affected by this issue is some unknown functionality of the file /index/ajax/lang. The manipulation of the argument lang leads to path traversal. This vulnerability is handled as CVE-2024-8876. The attack may be launched remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-44761	EQ Enterprise Management System up to 1.x Requests path traversal	A vulnerability was found in EQ Enterprise Management System up to 1.x. It has been rated as critical. This issue affects some unknown processing of the component Requests Handler. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2024-44761. The attack can only be initiated within the local network. 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-2024-8304	jpress up to 5.1.1 Template Module /admin/template/edit path traversal (Issue 189)	A vulnerability has been found in jpress up to 5.1.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/template/edit of the component Template Module Handler. The manipulation leads to path traversal. This vulnerability is known as CVE-2024-8304. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8782	JFinalCMS up to 1.0 /admin/template/edit delete name path traversal (IAOSJG)	A vulnerability was found in JFinalCMS up to 1.0. It has been rated as critical. This issue affects the function delete of the file /admin/template/edit. The manipulation of the argument name leads to path traversal. The identification of this vulnerability is CVE-2024-8782. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8865	composiohq composio up to 0.5.8 composio\server\api.py path file path traversal	A vulnerability was found in composiohq composio up to 0.5.8 and classified as problematic. Affected by this issue is the function path of the file composio\server\api.py. The manipulation	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the argument file leads to path traversal. This vulnerability is handled as CVE-2024-8865. The attack can only be done within the local network. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-8875	vedees wcms up to 0.3.2 /wex/finder.php path traversal	A vulnerability classified as critical was found in vedees wcms up to 0.3.2. Affected by this vulnerability is an unknown functionality of the file /wex/finder.php. The manipulation of the argument p leads to path traversal. This vulnerability is known as CVE-2024-8875. 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-2024-8876	xiaohe4966 TpMeCMS up to 1.3.3.1 /index/ajax/lang path traversal	A vulnerability which was classified as problematic has been found in xiaohe4966 TpMeCMS up to 1.3.3.1. Affected by this issue is some unknown functionality of the file /index/ajax/lang. The manipulation of the argument lang leads to path traversal.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is handled as CVE-2024-8876. The attack may be launched remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.		
CVE-2024-8752	Smart HMI WebIQ 2.15.19 path traversal	A vulnerability was found in Smart HMI WebIQ 2.15.19 and classified as critical. Affected by this issue is some unknown functionality. The manipulation leads to path traversal. This vulnerability is handled as CVE-2024-8752. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-47049	czim file-handling package up to 1.4.x/2.2.x makeFromUrl/makeFromAny server-side request forgery	A vulnerability was found in czim file-handling package up to 1.4.x/2.2.x. It has been classified as critical. This affects the function makeFromUrl/makeFromAny. The manipulation leads to server-side request forgery. This vulnerability is uniquely identified as CVE-2024-47049. Access to the local network is required for this attack to succeed. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-9032	SourceCodester Simple Forum-Discussion System	A vulnerability which was classified as critical was found in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	1.0 /index.php page path traversal	SourceCodester Simple Forum-Discussion System 1.0. Affected is an unknown function of the file /index.php. The manipulation of the argument page leads to path traversal. This vulnerability is traded as CVE-2024-9032. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2023-26691	CS-Cart MultiVendor 4.16.1 ZIP File path traversal	A vulnerability classified as critical was found in CS-Cart MultiVendor 4.16.1. This vulnerability affects unknown code of the component ZIP File Handler. The manipulation leads to path traversal. This vulnerability was named CVE-2023-26691. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-26687	CS-Cart MultiVendor 4.16.1 PDF Add-on product_data path traversal	A vulnerability was found in CS-Cart MultiVendor 4.16.1. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component PDF Add-on. The manipulation of the argument product_data leads to path traversal. This vulnerability is known as CVE-2023-26687. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-41444	SeaCMS 12.9 index.php key sql injection	A vulnerability was found in SeaCMS 12.9 and classified as critical. Affected by this issue is some unknown functionality of the file /js/player/dmplayer/dmku/index.phpacso. The manipulation of the argument key leads to sql injection. This vulnerability is handled as CVE-2024-41444. The attack needs to be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-42913	RuoYi CMS 4.7.9 /sasfs1 job_id sql injection	A vulnerability which was classified as critical has been found in RuoYi CMS 4.7.9. Affected by this issue is some unknown functionality of the file /sasfs1. The manipulation of the argument job_id leads to sql injection. This vulnerability is handled as CVE-2024-42913. The attack needs to be done within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-45059	portabilis i-educar up to 2.9 GET Parameter sql injection	A vulnerability has been found in portabilis i-educar up to 2.9 and classified as critical. Affected by this vulnerability is an unknown functionality of the component GET Parameter Handler. The manipulation leads to sql injection. This vulnerability is known as CVE-2024-45059. The attack can be launched remotely.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		There is no exploit available. It is recommended to apply a patch to fix this issue.		
CVE-2024-8303	dingfanzu CMS up to 29d67d9044f6f93378e6eb6ff92272217ff7225c /ajax/getBasicInfo.php username sql injection	A vulnerability classified as critical has been found in dingfanzu CMS up to 29d67d9044f6f93378e6eb6ff92272217ff7225c. This affects an unknown part of the file /ajax/getBasicInfo.php. The manipulation of the argument username leads to sql injection. This vulnerability is uniquely identified as CVE-2024-8303. 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. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.	Patched by core rule	Y
CVE-2024-41370	Organizr 1.90 chat/setlike.php sql injection	A vulnerability which was classified as critical has been found in Organizr 1.90. This issue affects some unknown processing of the file chat/setlike.php. The manipulation leads to sql injection. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The identification of this vulnerability is CVE-2024-41370. The attack may be initiated remotely. There is no exploit available.		
CVE-2024-41372	Organizr 1.90 chat/settyping.php sql injection	A vulnerability classified as critical was found in Organizr 1.90. This vulnerability affects unknown code of the file chat/settyping.php. The manipulation leads to sql injection. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability was named CVE-2024-41372. Access to the local network is required for this attack to succeed. There is no exploit available.	Patched by core rule	Y
CVE-2024-8332	master-nan Sweet-CMS up to 5f441e022b8876f07cde709c77b5be6d2f262e3f /table/index sql injection	A vulnerability was found in master-nan Sweet-CMS up to 5f441e022b8876f07cde709c77b5be6d2f262e3f. It has been declared as critical. This vulnerability affects unknown code of the file /table/index. The manipulation leads to sql injection. This vulnerability was named CVE-2024-8332. The attack can be initiated remotely. There is no exploit available. This product is using a rolling release to provide continious delivery. Therefore no version details for affected nor updated releases are available. It is recommended to apply a patch to fix this	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		issue.		
CVE-2024-41370	Organizr 1.90 chat/setlike.php sql injection	A vulnerability which was classified as critical has been found in Organizr 1.90. This issue affects some unknown processing of the file chat/setlike.php. The manipulation leads to sql injection. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. The identification of this vulnerability is CVE-2024-41370. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-45622	ASIS Aplikasi Sistem Sekolah using CodeIgniter up to 3.2.0 index.php username sql injection	A vulnerability classified as critical was found in ASIS Aplikasi Sistem Sekolah using CodeIgniter up to 3.2.0. Affected by this vulnerability is an unknown functionality of the file index.php. The manipulation of the argument username leads to sql injection. This vulnerability is known as CVE-2024-45622. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-6926	Viral Signup Plugin up to 2.1 on WordPress AJAX Action sql injection	A vulnerability was found in Viral Signup Plugin up to 2.1 on WordPress. It has been rated as critical. This issue affects some unknown processing of the component AJAX Action Handler. The manipulation leads to sql injection. The identification of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		this vulnerability is CVE-2024-6926. The attack may be initiated remotely. There is no exploit available.		
CVE-2024-44817	ZZCMS up to 2023 adv2.php id sql injection	A vulnerability has been found in ZZCMS up to 2023 and classified as critical. Affected by this vulnerability is an unknown functionality of the file adv2.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2024-44817. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-44587	itsourcecode Alton Management System 1.0 /noncombo_save.php menu sql injection	A vulnerability was found in itsourcecode Alton Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /noncombo_save.php. The manipulation of the argument menu leads to sql injection. This vulnerability is traded as CVE-2024-44587. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-44739	SourceCodester Simple Forum Website 1.0 id sql injection	A vulnerability has been found in SourceCodester Simple Forum Website 1.0 and classified as critical. This vulnerability affects unknown code of the file /php-sqlite-forum/pagemanage_user. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		44739. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-8395	FlyCASS Cockpit Access Security System/Known Crewmember sql injection	A vulnerability was found in FlyCASS Cockpit Access Security System and Known Crewmember. It has been classified as critical. Affected is an unknown function. The manipulation leads to sql injection. This vulnerability is traded as CVE-2024-8395. 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-2024-8557	SourceCodester Food Ordering Management System 1.0 cancel-order.php id sql injection	A vulnerability classified as critical has been found in SourceCodester Food Ordering Management System 1.0. This affects an unknown part of the file /foms/routers/cancel-order.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-8557. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8569	code-projects Hospital Management System 1.0 user-login.php username sql injection	A vulnerability has been found in code-projects Hospital Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file user-login.php. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument username leads to sql injection. This vulnerability is known as CVE-2024-8569. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2024-8567	itsourcecode Payroll Management System 1.0 ajax.php id sql injection	A vulnerability which was classified as critical has been found in itsourcecode Payroll Management System 1.0. This issue affects some unknown processing of the file /ajax.phpactiondelete_deductions. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-8567. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8570	itsourcecode Tailoring Management System 1.0 /inccatadd.php title sql injection	A vulnerability was found in itsourcecode Tailoring Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /inccatadd.php. The manipulation of the argument title leads to sql injection. This vulnerability is handled as CVE-2024-8570. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-45771	RapidCMS 1.3.1 /resource/runlogin.php password sql injection (Issue 17)	A vulnerability classified as critical was found in RapidCMS 1.3.1. Affected by this vulnerability is an unknown functionality	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the file /resource/runlogin.php . The manipulation of the argument password leads to sql injection. This vulnerability is known as CVE-2024-45771. The attack can be launched remotely. There is no exploit available.		
CVE-2024-8565	SourceCodesters Clinics Patient Management System 2.0 /print_diseases.php disease/from/to sql injection	A vulnerability was found in SourceCodesters Clinics Patient Management System 2.0. It has been rated as critical. This issue affects some unknown processing of the file /print_diseases.php. The manipulation of the argument disease/from/to leads to sql injection. The identification of this vulnerability is CVE-2024-8565. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-44839	RapidCMS 1.3.1 /default/article.php articleid sql injection (Issue 18)	A vulnerability which was classified as critical has been found in RapidCMS 1.3.1. Affected by this issue is some unknown functionality of the file /default/article.php. The manipulation of the argument articleid leads to sql injection. This vulnerability is handled as CVE-2024-44839. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-44838	RapidCMS 1.3.1 /resource/runlogin.php username sql	A vulnerability classified as critical has been found in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection (Issue 17)	RapidCMS 1.3.1. Affected is an unknown function of the file /resource/runlogin.php . The manipulation of the argument username leads to sql injection. This vulnerability is traded as CVE-2024-44838. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2024-8611	itsourcecode Tailoring Management System 1.0 ssms.php customer sql injection	A vulnerability classified as critical was found in itsourcecode Tailoring Management System 1.0. Affected by this vulnerability is an unknown functionality of the file ssms.php. The manipulation of the argument customer leads to sql injection. This vulnerability is known as CVE-2024-8611. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-44725	AutoCMS 5.4 /admin/robot.php sidebar sql injection (Issue 69)	A vulnerability has been found in AutoCMS 5.4 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/robot.php. The manipulation of the argument sidebar leads to sql injection. This vulnerability is known as CVE-2024-44725. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-8710	code-projects Inventory Management 1.0 Products Table Page	A vulnerability classified as critical was found in code-projects Inventory Management	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	/model/viewProduct.php id sql injection	1.0. Affected by this vulnerability is an unknown functionality of the file /model/viewProduct.php of the component Products Table Page. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2024-8710. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2024-8709	SourceCodester Best House Rental Management System 1.0 /admin_class.php delete_user/save_user id sql injection	A vulnerability classified as critical has been found in SourceCodester Best House Rental Management System 1.0. Affected is the function delete_user/save_user of the file /admin_class.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-8709. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-34334	ORDAT FOSS-Online up to 2.24.00 Forgot Password sql injection	A vulnerability was found in ORDAT FOSS-Online up to 2.24.00 and classified as critical. This issue affects some unknown processing of the component Forgot Password Handler. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2024-34334. The attack may be initiated 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-2024-7766	Adicon Server Plugin up to 1.2 on WordPress sql injection	A vulnerability was found in Adicon Server Plugin up to 1.2 on WordPress. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2024-7766. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-8762	code-projects Crud Operation System 1.0 /updatedata.php sid sql injection	A vulnerability was found in code-projects Crud Operation System 1.0. It has been classified as critical. This affects an unknown part of the file /updatedata.php. The manipulation of the argument sid leads to sql injection. This vulnerability is uniquely identified as CVE-2024-8762. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-44541	evilnapsis Inventio Lite up to 4 /?action=processlogin username sql injection	A vulnerability which was classified as critical has been found in evilnapsis Inventio Lite up to 4. This issue affects some unknown processing of the file /actionprocesslogin. The manipulation of the argument username leads to sql injection. The identification of this vulnerability is CVE-2024-44541. 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.		
CVE-2024-6723	AI Engine Plugin up to 2.4.7 on WordPress sql injection	A vulnerability was found in AI Engine Plugin up to 2.4.7 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-2024-6723. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-8784	QDocs Smart School Management System 7.0.0 Chat /user/chat/mynewuser users[] sql injection	A vulnerability classified as critical was found in QDocs Smart School Management System 7.0.0. Affected by this vulnerability is an unknown functionality of the file /user/chat/mynewuser of the component Chat. The manipulation of the argument users[] with the input 1&039;+AND+))ZNun)+AND+&039;WwBM&039;%3d&039;WwBM as part of POST Request Parameter leads to sql injection. This vulnerability is known as CVE-2024-8784. The attack can be launched remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-8868	code-projects Crud Operation System 1.0 savedata.php	A vulnerability was found in code-projects Crud Operation System	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	sname sql injection	1.0. It has been rated as critical. This issue affects some unknown processing of the file savedata.php. The manipulation of the argument sname leads to sql injection. The identification of this vulnerability is CVE-2024-8868. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-44430	Best Free Law Office Management Software 1.0 register_case.php sql injection	A vulnerability which was classified as critical was found in Best Free Law Office Management Software 1.0. Affected is an unknown function of the file kortex_lite/control/register_case.php. The manipulation leads to sql injection. This vulnerability is traded as CVE-2024-44430. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-8217	SourceCodester E-Commerce Website 1.0 /Admin/registration.php fname sql injection	A vulnerability has been found in SourceCodester E-Commerce Website 1.0 and classified as critical. This vulnerability affects unknown code of the file /Admin/registration.php. The manipulation of the argument fname leads to sql injection. This vulnerability was named CVE-2024-8217. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8222	SourceCodester	A vulnerability	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Music Gallery Site 1.0 id sql injection	classified as critical has been found in SourceCodester Music Gallery Site 1.0. This affects an unknown part of the file /admin/pagemusics/manage_music. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-8222. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	core rule	
CVE-2024-8219	code-projects Responsive Hotel Site 1.0 index.php name/phone/email sql injection	A vulnerability was found in code-projects Responsive Hotel Site 1.0. It has been classified as critical. Affected is an unknown function of the file index.php. The manipulation of the argument name/phone/email leads to sql injection. This vulnerability is traded as CVE-2024-8219. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8218	code-projects Online Quiz Site 1.0 index.php loginid sql injection	A vulnerability was found in code-projects Online Quiz Site 1.0 and classified as critical. This issue affects some unknown processing of the file index.php. The manipulation of the argument loginid leads to sql injection. The identification of this vulnerability is CVE-2024-8218. 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-2024-8221	SourceCodester Music Gallery Site 1.0 manage_category.php id sql injection	A vulnerability was found in SourceCodester Music Gallery Site 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/categories/manage_category.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-8221. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8220	itsourcecode Tailoring Management System 1.0 staffedit.php id/stafftype/address/fullname/phonenumber/salary sql injection	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file staffedit.php. The manipulation of the argument id/stafftype/address/fullname/phonenumber/salary leads to sql injection. This vulnerability is known as CVE-2024-8220. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8223	SourceCodester Music Gallery Site 1.0 Master.php id sql injection	A vulnerability classified as critical was found in SourceCodester Music Gallery Site 1.0. This vulnerability affects unknown code of the file /classes/Master.phpfdelete_category. The manipulation of the argument id 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-2024-8223. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-41236	Kashipara Responsive School Management System 3.2.0 Admin Login Page /smsa/admin_login.php username sql injection	A vulnerability was found in Kashipara Responsive School Management System 3.2.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /smsa/admin_login.php of the component Admin Login Page. The manipulation of the argument username leads to sql injection. This vulnerability is handled as CVE-2024-41236. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-8302	dingfanzu CMS up to 29d67d9044f6f93378e6eb6ff92272217ff7225c /ajax/chpwd.php username sql injection	A vulnerability was found in dingfanzu CMS up to 29d67d9044f6f93378e6eb6ff92272217ff7225c. It has been rated as critical. Affected by this issue is some unknown functionality of the file /ajax/chpwd.php. The manipulation of the argument username leads to sql injection. This vulnerability is handled as CVE-2024-8302. 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. Continious delivery	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		with rolling releases is used by this product. Therefore no version details of affected nor updated releases are available.		
CVE-2024-8301	dingfanzu CMS up to 29d67d9044f6f93378e6eb6ff92272217ff7225c /ajax/checkin.php username sql injection	A vulnerability was found in dingfanzu CMS up to 29d67d9044f6f93378e6eb6ff92272217ff7225c. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /ajax/checkin.php. The manipulation of the argument username leads to sql injection. This vulnerability is known as CVE-2024-8301. 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. This product takes the approach of rolling releases to provide continious delivery. Therefore version details for affected and updated releases are not available.	Patched by core rule	Y
CVE-2024-8343	SourceCodester Sentiment Based Movie Rating System 1.0 User Registration Users.php email sql injection	A vulnerability which was classified as critical was found in SourceCodester Sentiment Based Movie Rating System 1.0. Affected is an unknown function of the file /classes/Users.phpfsave_client of the component User Registration Handler. The manipulation of the argument email leads to sql injection.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is traded as CVE-2024-8343. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2024-8344	Campcodes Supplier Management System 1.0 /admin/edit_area.php id sql injection	A vulnerability has been found in Campcodes Supplier Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/edit_area.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2024-8344. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8345	SourceCodester Music Gallery Site 1.0 Users.php id sql injection	A vulnerability was found in SourceCodester Music Gallery Site 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /classes/Users.phpfdelete. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-8345. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8346	SourceCodester Computer Laboratory Management System 1.0 SystemSettings.php update_settings_info name sql injection	A vulnerability classified as critical has been found in SourceCodester Computer Laboratory Management System 1.0. Affected is the function update_settings_info	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the file /classes/SystemSettings.phpfupdate_settings. The manipulation of the argument name leads to sql injection. This vulnerability is traded as CVE-2024-8346. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2024-8347	SourceCodester Computer Laboratory Management System 1.0 Master.php delete_record id sql injection	A vulnerability classified as critical was found in SourceCodester Computer Laboratory Management System 1.0. Affected by this vulnerability is the function delete_record of the file /classes/Master.phpfdelete_record. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2024-8347. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8348	SourceCodester Computer Laboratory Management System 1.0 Master.php delete_category id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Computer Laboratory Management System 1.0. Affected by this issue is the function delete_category of the file /classes/Master.phpfdelete_category. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-8348. The attack may 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-2024-8336	SourceCodester Music Gallery Site 1.0 Master.php id sql injection	A vulnerability classified as critical was found in SourceCodester Music Gallery Site 1.0. Affected by this vulnerability is an unknown functionality of the file /php-music/classes/Master.phpfdelete_music. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2024-8336. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8335	OpenRapid RapidCMS up to 1.3.1 /resource/runlogon.php username sql injection	A vulnerability classified as critical has been found in OpenRapid RapidCMS up to 1.3.1. Affected is an unknown function of the file /resource/runlogon.php. The manipulation of the argument username leads to sql injection. This vulnerability is traded as CVE-2024-8335. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8331	OpenRapid RapidCMS up to 1.3.1 user-move-run.php username sql injection	A vulnerability was found in OpenRapid RapidCMS up to 1.3.1. It has been classified as critical. This affects an unknown part of the file /admin/user/user-move-run.php. The manipulation of the argument username leads to sql injection. This vulnerability is uniquely identified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2024-8331. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-8340	SourceCodester Electric Billing Management System 1.0 /Actions.php username sql injection	A vulnerability classified as critical has been found in SourceCodester Electric Billing Management System 1.0. This affects an unknown part of the file /Actions.phpalogin. The manipulation of the argument username leads to sql injection. This vulnerability is uniquely identified as CVE-2024-8340. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8339	SourceCodester Electric Billing Management System 1.0 Connection Code /?page=tracks code sql injection	A vulnerability was found in SourceCodester Electric Billing Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /pagetracks of the component Connection Code Handler. The manipulation of the argument code leads to sql injection. This vulnerability is handled as CVE-2024-8339. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8368	code-projects Hospital Management System 1.0 Login index.php username sql injection	A vulnerability was found in code-projects Hospital Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file index.php of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component Login. The manipulation of the argument username leads to sql injection. This vulnerability is handled as CVE-2024-8368. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-8380	SourceCodester Contact Manager with Export to VCF 1.0 Delete Contact delete-account.php contact sql injection	A vulnerability was found in SourceCodester Contact Manager with Export to VCF 1.0. It has been rated as critical. This issue affects some unknown processing of the file /endpoint/delete-account.php of the component Delete Contact Handler. The manipulation of the argument contact leads to sql injection. The identification of this vulnerability is CVE-2024-8380. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-44921	SeaCMS 12.9 index.php id sql injection	A vulnerability was found in SeaCMS 12.9. It has been classified as critical. This affects an unknown part of the file /dmplayer/dmku/index.phpacdel. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-44921. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-8416	SourceCodester Food Ordering Management	A vulnerability was found in SourceCodester Food	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	System 1.0 ticket-status.php ticket_id sql injection	Ordering Management System 1.0. It has been classified as critical. This affects an unknown part of the file /routers/ticket-status.php. The manipulation of the argument ticket_id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-8416. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-8415	SourceCodester Food Ordering Management System 1.0 /routers/add-ticket.php id sql injection	A vulnerability was found in SourceCodester Food Ordering Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /routers/add-ticket.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-8415. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-44727	SourceCodeHero Event Management System 1.0 /event/admin/login.php username sql injection	A vulnerability was found in SourceCodeHero Event Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /event/admin/login.php. The manipulation of the argument username leads to sql injection. The identification of this vulnerability is CVE-2024-44727. The attack may be initiated	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remotely. There is no exploit available.		
CVE-2024-8395	FlyCASS Cockpit Access Security System/Known Crewmember sql injection	A vulnerability was found in FlyCASS Cockpit Access Security System and Known Crewmember. It has been classified as critical. Affected is an unknown function. The manipulation leads to sql injection. This vulnerability is traded as CVE-2024-8395. 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-2024-8557	SourceCodester Food Ordering Management System 1.0 cancel-order.php id sql injection	A vulnerability classified as critical has been found in SourceCodester Food Ordering Management System 1.0. This affects an unknown part of the file /foms/routers/cancel-order.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-8557. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8569	code-projects Hospital Management System 1.0 user-login.php username sql injection	A vulnerability has been found in code-projects Hospital Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file user-login.php. The manipulation of the argument username	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		leads to sql injection. This vulnerability is known as CVE-2024-8569. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2024-8567	itsourcecode Payroll Management System 1.0 ajax.php id sql injection	A vulnerability which was classified as critical has been found in itsourcecode Payroll Management System 1.0. This issue affects some unknown processing of the file /ajax.phpactiondelete_deductions. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-8567. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8570	itsourcecode Tailoring Management System 1.0 /inccatadd.php title sql injection	A vulnerability was found in itsourcecode Tailoring Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /inccatadd.php. The manipulation of the argument title leads to sql injection. This vulnerability is handled as CVE-2024-8570. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8565	SourceCodesters Clinics Patient Management System 2.0 /print_diseases.php disease/from/to sql injection	A vulnerability was found in SourceCodesters Clinics Patient Management System 2.0. It has been rated as critical. This issue affects some unknown processing of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the file /print_diseases.php. The manipulation of the argument disease/from/to leads to sql injection. The identification of this vulnerability is CVE-2024-8565. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-8611	itsourcecode Tailoring Management System 1.0 ssms.php customer sql injection	A vulnerability classified as critical was found in itsourcecode Tailoring Management System 1.0. Affected by this vulnerability is an unknown functionality of the file ssms.php. The manipulation of the argument customer leads to sql injection. This vulnerability is known as CVE-2024-8611. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8710	code-projects Inventory Management 1.0 Products Table Page /model/viewProduct.php id sql injection	A vulnerability classified as critical was found in code-projects Inventory Management 1.0. Affected by this vulnerability is an unknown functionality of the file /model/viewProduct.php of the component Products Table Page. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2024-8710. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8709	SourceCodester Best House Rental Management	A vulnerability classified as critical has been found in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	System 1.0 /admin_class.php delete_user/save_user id sql injection	SourceCodester Best House Rental Management System 1.0. Affected is the function delete_user/save_user of the file /admin_class.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-8709. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2024-34334	ORDAT FOSS-Online up to 2.24.00 Forgot Password sql injection	A vulnerability was found in ORDAT FOSS-Online up to 2.24.00 and classified as critical. This issue affects some unknown processing of the component Forgot Password Handler. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2024-34334. 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-2024-8762	code-projects Crud Operation System 1.0 /updatedata.php sid sql injection	A vulnerability was found in code-projects Crud Operation System 1.0. It has been classified as critical. This affects an unknown part of the file /updatedata.php. The manipulation of the argument sid leads to sql injection. This vulnerability is uniquely identified as CVE-2024-8762. It is possible to initiate the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack remotely. Furthermore there is an exploit available.		
CVE-2024-8868	code-projects Crud Operation System 1.0 savedata.php sname sql injection	A vulnerability was found in code-projects Crud Operation System 1.0. It has been rated as critical. This issue affects some unknown processing of the file savedata.php. The manipulation of the argument sname leads to sql injection. The identification of this vulnerability is CVE-2024-8868. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-44430	Best Free Law Office Management Software 1.0 register_case.php sql injection	A vulnerability which was classified as critical was found in Best Free Law Office Management Software 1.0. Affected is an unknown function of the file kortex_lite/control/register_case.php. The manipulation leads to sql injection. This vulnerability is traded as CVE-2024-44430. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-8945	CodeCanyon RISE Ultimate Project Manager 3.7.0 save id sql injection	A vulnerability has been found in CodeCanyon RISE Ultimate Project Manager 3.7.0 and classified as critical. This vulnerability affects unknown code of the file /index.php/dashboard/save. The manipulation of the argument id leads to sql injection. This vulnerability was	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		named CVE-2024-8945. The attack can be initiated remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.		
CVE-2024-8944	code-projects Hospital Management System 1.0 check_availability.php email sql injection	A vulnerability which was classified as critical was found in code-projects Hospital Management System 1.0. This affects an unknown part of the file check_availability.php. The manipulation of the argument email leads to sql injection. This vulnerability is uniquely identified as CVE-2024-8944. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9008	SourceCodester Best Online News Portal 1.0 Comment Section /news-details.php name sql injection	A vulnerability classified as critical was found in SourceCodester Best Online News Portal 1.0. This vulnerability affects unknown code of the file /news-details.php of the component Comment Section. The manipulation of the argument name leads to sql injection. This vulnerability was named CVE-2024-9008. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-46382	linlinjava litemall 1.8.0 AdminGoodscontroller.java goodsId/goodsSn/name parameters sql	A vulnerability has been found in linlinjava litemall 1.8.0 and classified as critical. Affected by this vulnerability is an	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection (Issue 552)	unknown functionality of the file AdminGoodscontroller.java. The manipulation of the argument goodsId/goodsSn/name parameters leads to sql injection. This vulnerability is known as CVE-2024-46382. The attack can be launched remotely. There is no exploit available.		
CVE-2024-9011	code-projects Crud Operation System 1.0 updata.php sid sql injection	A vulnerability which was classified as critical was found in code-projects Crud Operation System 1.0. Affected is an unknown function of the file updata.php. The manipulation of the argument sid leads to sql injection. This vulnerability is traded as CVE-2024-9011. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9009	code-projects Online Quiz Site 1.0 showtest.php subid sql injection	A vulnerability which was classified as critical has been found in code-projects Online Quiz Site 1.0. This issue affects some unknown processing of the file showtest.php. The manipulation of the argument subid leads to sql injection. The identification of this vulnerability is CVE-2024-9009. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9093	SourceCodester Profile Registration without Reload	A vulnerability classified as critical has been found in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Refresh 1.0 GET Parameter del.php list sql injection	SourceCodester Profile Registration without Reload Refresh 1.0. This affects an unknown part of the file del.php of the component GET Parameter Handler. The manipulation of the argument list leads to sql injection. This vulnerability is uniquely identified as CVE-2024-9093. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-42789	Kashipara Music Management System 1.0 controller.php page cross site scripting	A vulnerability was found in Kashipara Music Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /music/controller.phppagetest. The manipulation of the argument page leads to cross site scripting. The identification of this vulnerability is CVE-2024-42789. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-7816	Gixaw Chat Plugin up to 1.0 on WordPress cross-site request forgery	A vulnerability was found in Gixaw Chat Plugin up to 1.0 on WordPress. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-7816. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-44796	PicUploader fcf82ea /auth/AzureRedirect .php error_description cross site scripting (ID 90)	A vulnerability which was classified as problematic has been found in PicUploader fcf82ea. Affected by this issue is some unknown functionality of the file /auth/AzureRedirect.php. The manipulation of the argument error_description leads to cross site scripting. This vulnerability is handled as CVE-2024-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		44796. The attack may be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.		
CVE-2024-42818	fastapi-admin pro 0.1.4 Product Name cross site scripting	A vulnerability was found in fastapi-admin pro 0.1.4. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument Product Name leads to cross site scripting. This vulnerability is known as CVE-2024-42818. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-44797	Gazelle 63b3370 enable_requests.php view cross site scripting (ID 130)	A vulnerability which was classified as problematic was found in Gazelle 63b3370. This affects an unknown part of the file /managers/enable_requests.php. The manipulation of the argument view leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-44797. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-44793	Gazelle 63b3370 multiple_freeleech.php torrents cross site scripting (ID 131)	A vulnerability was found in Gazelle 63b3370. It has been rated as problematic. This issue affects some unknown processing of the file /managers/multiple_freeleech.php. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument torrents leads to cross site scripting. The identification of this vulnerability is CVE-2024-44793. The attack may be initiated remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.		
CVE-2024-44794	PicUploader fcf82ea OnedriveRedirect.php error_description cross site scripting (ID 91)	A vulnerability classified as problematic has been found in PicUploader fcf82ea. Affected is an unknown function of the file /master/auth/OnedriveRedirect.php. The manipulation of the argument error_description leads to cross site scripting. This vulnerability is traded as CVE-2024-44794. It is possible to launch the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y
CVE-2024-44795	Gazelle 63b3370 /login/disabled.php username cross site scripting (ID 129)	A vulnerability classified as problematic was found in Gazelle 63b3370. Affected by this vulnerability is an unknown functionality of the file /login/disabled.php. The manipulation of the argument username leads to cross site scripting. This vulnerability is known as CVE-2024-44795. The attack can be launched remotely. There is no exploit	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		available. It is recommended to apply a patch to fix this issue.		
CVE-2024-42816	fastapi-admin 0.1.4 Create Product Product Name cross site scripting	A vulnerability classified as problematic has been found in fastapi-admin 0.1.4. Affected is an unknown function of the component Create Product Handler. The manipulation of the argument Product Name leads to cross site scripting. This vulnerability is traded as CVE-2024-42816. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-42787	Kashipara Music Management System 1.0 ajax.php title/description cross site scripting	A vulnerability classified as problematic has been found in Kashipara Music Management System 1.0. This affects an unknown part of the file /music/ajax.phpactions ave_playlist. The manipulation of the argument title/description leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-42787. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-42788	Kashipara Music Management System 1.0 ajax.php title/artist cross site scripting	A vulnerability was found in Kashipara Music Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /music/ajax.phpactions ave_music. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument title/artist leads to cross site scripting. This vulnerability was named CVE-2024-42788. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-43788	Webpack up to 5.93.x cross site scripting (GHSA-4vvj-4cpr-p986)	A vulnerability has been found in Webpack up to 5.93.x and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-43788. 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-2022-39997	Teldats RS123/RS123w weak password	A vulnerability was found in Teldats RS123 and RS123w. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to weak password requirements. This vulnerability is handled as CVE-2022-39997. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2022-39996	Teldats RS123/RS123w upgrade/query.php cmdcookie cross site scripting	A vulnerability classified as problematic was found in Teldats RS123 and RS123w. 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
		upgrade/query.php. The manipulation of the argument cmdcookie leads to cross site scripting. This vulnerability is known as CVE-2022-39996. The attack can be launched remotely. There is no exploit available.		
CVE-2024-43805	Jupyterlab cross site scripting (GHSA-9q39-rmj3-p4r2)	A vulnerability was found in Jupyterlab. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-43805. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-45046	PHPOffice PhpSpreadsheet up to 2.0.x cross site scripting	A vulnerability classified as problematic has been found in PHPOffice PhpSpreadsheet up to 2.0.x. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-45046. 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-2024-45048	PHPOffice PhpSpreadsheet up to 2.2.0 xml external entity reference	A vulnerability classified as problematic was found in PHPOffice PhpSpreadsheet up to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		2.2.0. Affected by this vulnerability is an unknown functionality. The manipulation leads to xml external entity reference. This vulnerability is known as CVE-2024-45048. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-45057	portabilis i-educar up to 2.9 clsCampos.inc.php cross site scripting	A vulnerability classified as problematic was found in portabilis i-educar up to 2.9. This vulnerability affects unknown code of the file ieducar/intranet/include/clsCampos.inc.php. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-45057. 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-2024-5417	Gutentor Plugin up to 3.3.5 on WordPress Block Option cross site scripting	A vulnerability which was classified as problematic was found in Gutentor Plugin up to 3.3.5 on WordPress. Affected is an unknown function of the component Block Option Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-5417. It is possible to launch the attack remotely. There is no	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit available. It is recommended to upgrade the affected component.		
CVE-2024-7132	Page Builder Gutenberg Blocks Plugin up to 3.1.12 on WordPress Block cross site scripting	A vulnerability which was classified as problematic has been found in Page Builder Gutenberg Blocks Plugin up to 3.1.12 on WordPress. This issue affects some unknown processing of the component Block Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-7132. 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-2024-6927	Viral Signup Plugin up to 2.1 on WordPress Setting cross site scripting	A vulnerability classified as problematic was found in Viral Signup Plugin up to 2.1 on WordPress. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-6927. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-41371	Organizr 1.90 api.php cross site scripting	A vulnerability was found in Organizr 1.90. It has been rated as problematic. Affected by this issue is some unknown functionality of the file api.php. The manipulation leads to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross site scripting. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability is handled as CVE-2024-41371. The attack may be launched remotely. There is no exploit available.		
CVE-2024-44716	DedeBIZ 6.3.0 cross site scripting	A vulnerability was found in DedeBIZ 6.3.0 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-44716. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-44717	DedeBIZ 6.2.x cross site scripting	A vulnerability which was classified as problematic has been found in DedeBIZ 6.2.x. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-44717. 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-2024-41351	bjyadmin a560fd5 getContent.php cross site scripting	A vulnerability which was classified as problematic was found in bjyadmin a560fd5. This affects an unknown part of the file Public/statics/umeditor	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		1_2_3/php/getContent.php. The manipulation leads to cross site scripting. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability is uniquely identified as CVE-2024-41351. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-41350	bjyadmin a560fd5 imageUp.php cross site scripting	A vulnerability has been found in bjyadmin a560fd5 and classified as problematic. This vulnerability affects unknown code of the file Public/statics/umeditor1_2_3/php/imageUp.php. The manipulation leads to cross site scripting. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability was named CVE-2024-41350. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-44918	SeaCMS 12.9 admin_datarelate.php cross site scripting	A vulnerability was found in SeaCMS 12.9. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file admin_datarelate.php. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-44918. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-8337	SourceCodester Contact Manager with Export to VCF 1.0 index.html contact_name cross site scripting	A vulnerability which was classified as problematic has been found in SourceCodester Contact Manager with Export to VCF 1.0. Affected by this issue is some unknown functionality of the file index.html. The manipulation of the argument contact_name leads to cross site scripting. This vulnerability is handled as CVE-2024-8337. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6585	Lightdash 0.510.3/0.1027.2 cross site scripting (GHSA-6529-6jv3-66q2)	A vulnerability was found in Lightdash 0.510.3/0.1027.2. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-6585. 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-2024-44918	SeaCMS 12.9 admin_datarelate.php cross site scripting	A vulnerability was found in SeaCMS 12.9. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file admin_datarelate.php. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-44918. 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-2024-45528	CodeAstro Membership Management System 1.0 add_members.php fullname cross site scripting	A vulnerability has been found in CodeAstro Membership Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file add_members.php. The manipulation of the argument fullname leads to cross site scripting. This vulnerability was named CVE-2024-45528. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-7354	Ninja Forms Plugin up to 3.8.10 on WordPress cross site scripting	A vulnerability has been found in Ninja Forms Plugin up to 3.8.10 on WordPress and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-7354. 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-2024-7691	Flaming Forms Plugin up to 1.0.1 on WordPress cross site scripting	A vulnerability was found in Flaming Forms Plugin up to 1.0.1 on WordPress. It has been classified as problematic. 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-2024-7691. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2024-7692	Flaming Forms Plugin up to 1.0.1 on WordPress cross site scripting	A vulnerability was found in Flaming Forms Plugin up to 1.0.1 on WordPress. 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-2024-7692. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-45527	REDCap 14.7.0 New Project Action index.php project title cross site scripting	A vulnerability which was classified as problematic has been found in REDCap 14.7.0. This issue affects some unknown processing of the file index.phplogout1 of the component New Project Action Handler. The manipulation of the argument project title leads to basic cross site scripting. The identification of this vulnerability is CVE-2024-45527. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-42901	LimeSurvey 6.5.12 CSV File injection	A vulnerability classified as problematic has been found in LimeSurvey 6.5.12. This affects an unknown part of the component CSV File Handler. The manipulation leads to injection.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is uniquely identified as CVE-2024-42901. The attack can only be done within the local network. There is no exploit available. It is recommended to apply a patch to fix this issue.		
CVE-2024-43413	Xibo CMS up to 4.0.x Data Entry Page cross site scripting (GHSA-pfxp-vxh7-2h9f)	A vulnerability was found in Xibo CMS up to 4.0.x. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Data Entry Page. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-43413. 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-2024-43412	Xibo CMS up to 4.0.x Generic File Module cross site scripting (GHSA-336f-wrgx-57gg)	A vulnerability was found in Xibo CMS up to 4.0.x. It has been declared as problematic. This vulnerability affects unknown code of the component Generic File Module. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-43412. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-42904	SysPass 3.2.x ClientController.php name cross site scripting	A vulnerability which was classified as problematic was found in SysPass 3.2.x. Affected is an unknown function of the file /Controllers/ClientController.php. The manipulation of the argument name leads to cross site scripting. This vulnerability is traded as CVE-2024-42904. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-45389	CloudCannon pagefind up to 1.1.0 document.currentScript.src cross site scripting	A vulnerability which was classified as problematic was found in CloudCannon pagefind up to 1.1.0. Affected is an unknown function. The manipulation of the argument document.currentScript.src leads to cross site scripting. This vulnerability is traded as CVE-2024-45389. 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-2024-6888	Secure Copy Content Protection and Content Locking Plugin Setting cross site scripting	A vulnerability classified as problematic has been found in Secure Copy Content Protection and Content Locking Plugin up to 4.1.6 on WordPress. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		traded as CVE-2024-6888. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-6020	Fetch Designs Sign-up Sheets Plugin up to 2.2.12 on WordPress REQUEST_URI cross site scripting	A vulnerability classified as problematic was found in Fetch Designs Sign-up Sheets Plugin up to 2.2.12 on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation of the argument REQUEST_URI leads to cross site scripting. This vulnerability is known as CVE-2024-6020. 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-2024-8410	ABCD ABCD2 up to 2.2.0-beta-1 otros_sitios.php sitio path traversal	A vulnerability classified as problematic was found in ABCD ABCD2 up to 2.2.0-beta-1. This vulnerability affects unknown code of the file /abcd/opac/php/otros_sitios.php. The manipulation of the argument sitio leads to path traversal. This vulnerability was named CVE-2024-8410. The attack can be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		not respond in any way.		
CVE-2024-6889	Secure Copy Content Protection and Content Locking Plugin Setting cross site scripting	A vulnerability which was classified as problematic has been found in Secure Copy Content Protection and Content Locking Plugin up to 4.1.6 on WordPress. 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-2024-6889. 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-2024-6722	Woocommerce Chatbot Support AI Plugin up to 1.0.2 on WordPress Setting cross site scripting	A vulnerability was found in Woocommerce Chatbot Support AI Plugin up to 1.0.2 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-2024-6722. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-44818	ZZCMS up to 2023 Header caina.php HTTP_Referer cross site scripting	A vulnerability was found in ZZCMS up to 2023. It has been rated as problematic. This issue affects some unknown processing of the file caina.php of the component Header Handler. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument HTTP_Referer leads to cross site scripting. The identification of this vulnerability is CVE-2024-44818. The attack may be initiated remotely. There is no exploit available.		
CVE-2024-8521	Wavelog up to 1.8.0 Live QSO /qso index manual cross site scripting	A vulnerability which was classified as problematic was found in Wavelog up to 1.8.0. Affected is the function index of the file /qso of the component Live QSO. The manipulation of the argument manual leads to cross site scripting. This vulnerability is traded as CVE-2024-8521. It is possible to launch the attack remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-45294	hapifhir HL7 FHIR Core Artifacts up to 6.3.22 xml external entity reference	A vulnerability was found in hapifhir HL7 FHIR Core Artifacts up to 6.3.22. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to xml external entity reference. This vulnerability was named CVE-2024-45294. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-44837	deathbreak Drug 1.0 \bean\Manager.java user cross site scripting	A vulnerability classified as problematic was found in deathbreak Drug 1.0. This vulnerability affects unknown code of the file \bean\Manager.java. The manipulation of the argument user leads to cross site scripting. This vulnerability was named CVE-2024-44837. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-8554	SourceCodester Clinics Patient Management System 2.0 /users.php message cross site scripting	A vulnerability was found in SourceCodester Clinics Patient Management System 2.0 and classified as problematic. This issue affects some unknown processing of the file /users.php. The manipulation of the argument message leads to cross site scripting. The identification of this vulnerability is CVE-2024-8554. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6792	WP ULike Plugin up to 4.7.2.0 on WordPress User Display Name cross site scripting	A vulnerability classified as problematic has been found in WP ULike Plugin up to 4.7.2.0 on WordPress. This affects an unknown part of the component User Display Name Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-6792. It is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-8563	SourceCodester PHP CRUD 1.0 /endpoint/update.php first_name/middle_name/last_name cross site scripting	A vulnerability was found in SourceCodester PHP CRUD 1.0. It has been classified as problematic. This affects an unknown part of the file /endpoint/update.php. The manipulation of the argument first_name/middle_name/last_name leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-8563. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8582	SourceCodester Food Ordering Management System 1.0 /index.php description cross site scripting	A vulnerability was found in SourceCodester Food Ordering Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /index.php. The manipulation of the argument description leads to cross site scripting. This vulnerability is handled as CVE-2024-8582. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8583	SourceCodester Online Bank Management System 1.0 Feedback /mfeedback.php cross site scripting	A vulnerability was found in SourceCodester Online Bank Management System and Online Bank Management	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		System - 1.0. It has been classified as problematic. This affects an unknown part of the file /mfeedback.php of the component Feedback Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-8583. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-8610	SourceCodester Best House Rental Management System 1.0 New Tenant Page /index.php Last Name/First Name/Middle Name cross site scripting	A vulnerability classified as problematic has been found in SourceCodester Best House Rental Management System 1.0. Affected is an unknown function of the file /index.phppagetenants of the component New Tenant Page. The manipulation of the argument Last Name/First Name/Middle Name leads to cross site scripting. This vulnerability is traded as CVE-2024-8610. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8605	code-projects Inventory Management 1.0 Registration Form /view/registration.php cross site scripting	A vulnerability classified as problematic was found in code-projects Inventory Management 1.0. This vulnerability affects unknown code of the file /view/registration.php of the component Registration Form. The manipulation with the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		input <script>alert</script> leads to cross site scripting. This vulnerability was named CVE-2024-8605. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-7918	Pocket Widget Plugin up to 0.1.3 on WordPress Setting cross site scripting	A vulnerability has been found in Pocket Widget Plugin up to 0.1.3 on WordPress and classified as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-7918. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40643	laurent22 joplin up to 3.0.14 Tag cross site scripting	A vulnerability was found in laurent22 joplin up to 3.0.14 and classified as problematic. Affected by this issue is some unknown functionality of the component Tag Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-40643. 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-2024-45406	Craft CMS up to 5.1.1 breadcrumb list/title cross site scripting (GHSA-	A vulnerability classified as problematic has been found in Craft CMS up	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	28h4-788g-rh42)	to 5.1.1. This affects an unknown part. The manipulation of the argument breadcrumb list/title leads to basic cross site scripting. This vulnerability is uniquely identified as CVE-2024-45406. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2023-50883	ONLYOFFICE Docs up to 8.0.0 Macro access control	A vulnerability has been found in ONLYOFFICE Docs up to 8.0.0 and classified as critical. This vulnerability affects unknown code of the component Macro Handler. The manipulation leads to improper access controls. This vulnerability was named CVE-2023-50883. 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-2024-6910	EventON Plugin up to 2.2.16 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic was found in EventON Plugin up to 2.2.16 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-2024-6910. It is possible to initiate the attack remotely. There	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-24510	Alinto SOGo up to 5.9.x Mail import cross site scripting	A vulnerability was found in Alinto SOGo up to 5.9.x. It has been classified as problematic. Affected is the function import of the component Mail. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-24510. 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-2024-5561	Popup Maker Plugin up to 1.19.0 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic has been found in Popup Maker Plugin up to 1.19.0 on WordPress. 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-2024-5561. 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-2024-7955	Starbox Plugin up to 3.5.1 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic was found in Starbox Plugin up to 3.5.1 on WordPress. This affects an unknown part of the component Setting	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-7955. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-7891	Floating Contact Button Plugin up to 2.7 on WordPress Setting cross site scripting	A vulnerability classified as problematic was found in Floating Contact Button Plugin up to 2.7 on WordPress. 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-2024-7891. 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-2024-34831	Gibbon Core 26.0.00 library_manage_catalog_editProcess.php imageLink cross site scripting	A vulnerability was found in Gibbon Core 26.0.00. It has been rated as problematic. This issue affects some unknown processing of the file library_manage_catalog_editProcess.php. The manipulation of the argument imageLink leads to cross site scripting. The identification of this vulnerability is CVE-2024-34831. The attack may be initiated remotely. There is no	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit available.		
CVE-2024-44872	moziloCMS 3.0 cross site scripting	A vulnerability which was classified as problematic has been found in moziloCMS 3.0. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-44872. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-44724	AutoCMS 5.4 /admin/site_add.php txtsite_url code injection (Issue 68)	A vulnerability which was classified as critical was found in AutoCMS 5.4. Affected is an unknown function of the file /admin/site_add.php. The manipulation of the argument txtsite_url leads to code injection. This vulnerability is traded as CVE-2024-44724. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-44676	eladmin up to 2.7 LocalStoreController.java cross site scripting	A vulnerability has been found in eladmin up to 2.7 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file LocalStoreController.java. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-44676. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-45592	DamienHarper	A vulnerability was	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	auditor-bundle up to 5.x Twig Macro source_label cross site scripting (GHSA-78vg-7v27-hj67)	found in DamienHarper auditor-bundle up to 5.x and classified as problematic. This issue affects some unknown processing of the component Twig Macro Handler. The manipulation of the argument source_label leads to cross site scripting. The identification of this vulnerability is CVE-2024-45592. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	core rule	
CVE-2024-43793	halo up to 2.18.x cross site scripting (GHSA-28x9-hppj-m537)	A vulnerability has been found in halo up to 2.18.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-2024-43793. 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-2024-44851	Perfex CRM 1.1.0 Discussion Section Content cross site scripting	A vulnerability which was classified as problematic was found in Perfex CRM 1.1.0. Affected is an unknown function of the component Discussion Section. The manipulation of the argument Content leads to cross site scripting. This vulnerability is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		traded as CVE-2024-44851. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2024-8693	Kaon CG3000 1.01.43 dhcpcd Command -h cross site scripting	A vulnerability which was classified as problematic has been found in Kaon CG3000 1.01.43. Affected by this issue is some unknown functionality of the component dhcpcd Command Handler. The manipulation of the argument -h with the input <script>alert</script> leads to cross site scripting. This vulnerability is handled as CVE-2024-8693. 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	Y
CVE-2024-34335	ORDAT FOSS-Online up to 2.24.00 Login Page cross site scripting	A vulnerability was found in ORDAT FOSS-Online up to 2.24.00. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Login Page. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-34335. The attack can 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-2020-24061	KASDA KW5515 4.3.1.0 Control Panel cross site scripting	A vulnerability classified as problematic was found in KASDA KW5515 4.3.1.0. This vulnerability affects unknown code of the component Control Panel. The manipulation leads to cross site scripting. This vulnerability was named CVE-2020-24061. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-8056	MM-Breaking News Plugin up to 0.7.9 on WordPress REQUEST_URI cross site scripting	A vulnerability classified as problematic has been found in MM-Breaking News Plugin up to 0.7.9 on WordPress. This affects an unknown part. The manipulation of the argument REQUEST_URI leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-8056. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-7822	Quick Code Plugin up to 1.0 on WordPress cross site scripting	A vulnerability classified as problematic was found in Quick Code Plugin up to 1.0 on WordPress. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-7822. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-25282	Redsys 3DSecure 2.0 3DSMethod Authentication cross site scripting	A vulnerability was found in Redsys 3DSecure 2.0. It has been rated as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		problematic. This issue affects some unknown processing of the component 3DSMethod Authentication. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-25282. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-6887	RafflePress Giveaways and Contests Plugin up to 1.12.15 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic was found in RafflePress Giveaways and Contests Plugin up to 1.12.15 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-2024-6887. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-5799	CM Pop-Up Banners Plugin up to 1.7.2 on WordPress cross site scripting	A vulnerability which was classified as problematic has been found in CM Pop-Up Banners Plugin up to 1.7.2 on WordPress. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-5799. The attack may be launched remotely. There is no exploit	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		available. It is recommended to upgrade the affected component.		
CVE-2024-45856	MindsDB ML Engine cross site scripting	A vulnerability was found in MindsDB. It has been classified as problematic. Affected is an unknown function of the component ML Engine. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-45856. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-25285	Redsys 3DSecure 2.0 threeDSMethodNotificationURL cross site scripting	A vulnerability classified as problematic has been found in Redsys 3DSecure 2.0. Affected is an unknown function. The manipulation of the argument threeDSMethodNotificationURL leads to cross site scripting. This vulnerability is traded as CVE-2024-25285. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-44798	PHPGurukul Bus Pass Management System 1.0 pass-bwdates-reports-details.php fromdate/todate cross site scripting	A vulnerability has been found in PHPGurukul Bus Pass Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/pass-bwdates-reports-details.php. The manipulation of the argument fromdate/todate 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-2024-44798. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-6617	NinjaTeam Header Footer Custom Code Plugin up to 1.1 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic has been found in NinjaTeam Header Footer Custom Code Plugin up to 1.1 on WordPress. 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-2024-6617. 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-2024-6850	Sayful Islam Carousel Slider Plugin up to 2.2.3 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic was found in Sayful Islam Carousel Slider Plugin up to 2.2.3 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-2024-6850. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-7133	Sticky Floating Notification Bar, Sticky Menu on	A vulnerability has been found in Sticky Floating Notification	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Scroll, Announcement Banner, and Sticky Header for Any Plugin Setting cross site scripting	Bar Sticky Menu on Scroll Announcement Banner and Sticky Header for Any Plugin up to 2.7.2 on WordPress and classified as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-7133. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-6493	NinjaTeam Header Footer Custom Code Plugin up to 1.1 on WordPress Setting cross site scripting	A vulnerability classified as problematic was found in NinjaTeam Header Footer Custom Code Plugin up to 1.1 on WordPress. 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-2024-6493. 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-2024-8783	OpenTibiaBR MyAAC up to 0.8.16 Post Reply new_post.php post_topic cross site scripting (Issue 121)	A vulnerability classified as problematic has been found in OpenTibiaBR MyAAC up to 0.8.16. Affected is an unknown function of the file system/pages/forum/n	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		ew_post.php of the component Post Reply Handler. The manipulation of the argument post_topic leads to cross site scripting. This vulnerability is traded as CVE-2024-8783. It is possible to launch the attack remotely. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue.		
CVE-2024-8863	aimhubio aim up to 3.24 Text Explorer textbox.tsx dangerouslySetInnerHTML query cross site scripting	A vulnerability which was classified as problematic was found in aimhubio aim up to 3.24. Affected is the function dangerouslySetInnerHTML of the file textbox.tsx of the component Text Explorer. The manipulation of the argument query leads to cross site scripting. This vulnerability is traded as CVE-2024-8863. 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	Y
CVE-2024-8867	Perfex CRM 3.1.6 Parameter Clients.php message cross site scripting	A vulnerability was found in Perfex CRM 3.1.6. It has been declared as problematic. This vulnerability affects unknown code of the file application/controllers/Clients.php of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component Parameter Handler. The manipulation of the argument message leads to cross site scripting. This vulnerability was named CVE-2024-8867. The attack can be initiated remotely. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue.		
CVE-2024-8866	AutoCMS 5.4 /admin/robot.php sidebar cross site scripting (Issue 68)	A vulnerability was found in AutoCMS 5.4. It has been classified as problematic. This affects an unknown part of the file /admin/robot.php. The manipulation of the argument sidebar leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-8866. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-42790	Kashipara Music Management System 1.0 index.php page cross site scripting	A vulnerability has been found in Kashipara Music Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /music/index.phppagetest. The manipulation of the argument page leads to cross site scripting. This vulnerability is known as CVE-2024-42790. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-6018	Music Request Manager Plugin up to 1.3 on WordPress cross site scripting	A vulnerability classified as problematic has been found in Music Request Manager Plugin up to 1.3 on WordPress. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-6018. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-6019	Music Request Manager Plugin up to 1.3 on WordPress cross site scripting	A vulnerability was found in Music Request Manager Plugin up to 1.3 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-2024-6019. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-42906	TestLink up to 1.9.19 Popup file name cross site scripting	A vulnerability was found in TestLink up to 1.9.19. It has been classified as problematic. This affects an unknown part of the component Popup Handler. The manipulation of the argument file name leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-42906. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component.		
CVE-2024-41347	openflights 5234b5b php/settings.php cross site scripting	A vulnerability was found in openflights 5234b5b. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file php/settings.php. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-41347. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-41358	phpipam 1.6 import-load-data.php cross site scripting	A vulnerability was found in phpipam 1.6. It has been classified as problematic. Affected is an unknown function of the file app\admin\import-export\import-load-data.php. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-41358. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-41348	openflights 5234b5b php/alsearch.php cross site scripting	A vulnerability classified as problematic has been found in openflights 5234b5b. This affects an unknown part of the file php/alsearch.php. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-41348. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-41346	openflights 5234b5b	A vulnerability was found in openflights	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	php/submit.php cross site scripting	5234b5b and classified as problematic. This issue affects some unknown processing of the file php/submit.php. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-41346. The attack may be initiated remotely. There is no exploit available.		
CVE-2024-41345	openflights 5234b5b php/trip.php cross site scripting	A vulnerability classified as problematic has been found in openflights 5234b5b. Affected is an unknown function of the file php/trip.php. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-41345. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-44919	SeaCMS 12.9 admin_ads.php description cross site scripting	A vulnerability which was classified as problematic has been found in SeaCMS 12.9. Affected by this issue is some unknown functionality of the file admin_ads.php. The manipulation of the argument description leads to cross site scripting. This vulnerability is handled as CVE-2024-44919. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-41349	unmark 1.9.2 add_by_url.php cross site scripting (Issue 290)	A vulnerability was found in unmark 1.9.2. It has been classified as problematic. Affected is an unknown function of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		application/views/marks/add_by_url.php. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-41349. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2024-45047	sveltejs svelte up to 4.2.18 cross site scripting (GHSA-8266-84wp-wv5c)	A vulnerability was found in sveltejs svelte up to 4.2.18 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-45047. 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-2024-41347	openflights 5234b5b php/settings.php cross site scripting	A vulnerability was found in openflights 5234b5b. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file php/settings.php. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-41347. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-43792	Halo up to 2.16.x cross site scripting	A vulnerability which was classified as problematic was found in Halo up to 2.16.x. Affected is an unknown function. The manipulation leads to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross site scripting. This vulnerability is traded as CVE-2024-43792. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-44920	SeaCMS 12.9 admin_collect_news .php siteurl cross site scripting	A vulnerability which was classified as problematic was found in SeaCMS 12.9. This affects an unknown part of the file admin_collect_news.php. The manipulation of the argument siteurl leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-44920. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-44819	ZZCMS up to 2023 admin/del.php pagename cross site scripting	A vulnerability was found in ZZCMS up to 2023. It has been rated as problematic. Affected by this issue is some unknown functionality of the file admin/del.php. The manipulation of the argument pagename leads to cross site scripting. This vulnerability is handled as CVE-2024-44819. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-8407	alwindoss akademy up to 35caccea888ed63d5489e211c99edff1f62efdba handlers.go emailAddress cross site scripting	A vulnerability was found in alwindoss akademy up to 35caccea888ed63d5489e211c99edff1f62efdba. It has been declared as problematic.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Affected by this vulnerability is an unknown functionality of the file cmd/akademy/handler/handlers.go. The manipulation of the argument emailAddress leads to cross site scripting. This vulnerability is known as CVE-2024-8407. The attack can be launched remotely. Furthermore there is an exploit available. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.		
CVE-2024-8411	ABCD ABCD2 up to 2.2.0-beta-1 /buscar_integrada.php Sub_Expresion cross site scripting	A vulnerability which was classified as problematic has been found in ABCD ABCD2 up to 2.2.0-beta-1. This issue affects some unknown processing of the file /buscar_integrada.php. The manipulation of the argument Sub_Expresion leads to cross site scripting. The identification of this vulnerability is CVE-2024-8411. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-44728	SourceCodeHero Event Management System 1.0 regester.php Full Name/Address/Email/contact cross site	A vulnerability classified as problematic was found in SourceCodeHero Event Management System 1.0. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	scripting	vulnerability affects unknown code of the file /clientdetails/admin/regester.php. The manipulation of the argument Full Name/Address/Email/contact leads to cross site scripting. This vulnerability was named CVE-2024-44728. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-44837	deathbreak Drug 1.0 \bean\Manager.java user cross site scripting	A vulnerability classified as problematic was found in deathbreak Drug 1.0. This vulnerability affects unknown code of the file \bean\Manager.java. The manipulation of the argument user leads to cross site scripting. This vulnerability was named CVE-2024-44837. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-8554	SourceCodester Clinics Patient Management System 2.0 /users.php message cross site scripting	A vulnerability was found in SourceCodester Clinics Patient Management System 2.0 and classified as problematic. This issue affects some unknown processing of the file /users.php. The manipulation of the argument message leads to cross site scripting. The identification of this vulnerability is CVE-2024-8554. 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-2024-8563	SourceCodester PHP CRUD 1.0 /endpoint/update.php first_name/middle_name/last_name cross site scripting	A vulnerability was found in SourceCodester PHP CRUD 1.0. It has been classified as problematic. This affects an unknown part of the file /endpoint/update.php. The manipulation of the argument first_name/middle_name/last_name leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-8563. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8582	SourceCodester Food Ordering Management System 1.0 /index.php description cross site scripting	A vulnerability was found in SourceCodester Food Ordering Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /index.php. The manipulation of the argument description leads to cross site scripting. This vulnerability is handled as CVE-2024-8582. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8583	SourceCodester Online Bank Management System 1.0 Feedback /mfeedback.php cross site scripting	A vulnerability was found in SourceCodester Online Bank Management System and Online Bank Management System - 1.0. It has been classified as problematic. This affects an unknown part of the file /mfeedback.php of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component Feedback Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-8583. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-8610	SourceCodester Best House Rental Management System 1.0 New Tenant Page /index.php Last Name/First Name/Middle Name cross site scripting	A vulnerability classified as problematic has been found in SourceCodester Best House Rental Management System 1.0. Affected is an unknown function of the file /index.phppagetenants of the component New Tenant Page. The manipulation of the argument Last Name/First Name/Middle Name leads to cross site scripting. This vulnerability is traded as CVE-2024-8610. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8605	code-projects Inventory Management 1.0 Registration Form /view/registration.php cross site scripting	A vulnerability classified as problematic was found in code-projects Inventory Management 1.0. This vulnerability affects unknown code of the file /view/registration.php of the component Registration Form. The manipulation with the input <script>alert</script> leads to cross site scripting. This vulnerability was	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		named CVE-2024-8605. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-43793	halo up to 2.18.x cross site scripting (GHSA-28x9-hppj-m537)	A vulnerability has been found in halo up to 2.18.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-2024-43793. 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-2024-44851	Perfex CRM 1.1.0 Discussion Section Content cross site scripting	A vulnerability which was classified as problematic was found in Perfex CRM 1.1.0. Affected is an unknown function of the component Discussion Section. The manipulation of the argument Content leads to cross site scripting. This vulnerability is traded as CVE-2024-44851. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-34335	ORDAT FOSS-Online up to 2.24.00 Login Page cross site scripting	A vulnerability was found in ORDAT FOSS-Online up to 2.24.00. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Login Page. The manipulation leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is known as CVE-2024-34335. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-45856	MindsDB ML Engine cross site scripting	A vulnerability was found in MindsDB. It has been classified as problematic. Affected is an unknown function of the component ML Engine. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-45856. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-44798	PHPGurukul Bus Pass Management System 1.0 pass-bwdates-reports-details.php fromdate/todate cross site scripting	A vulnerability has been found in PHPGurukul Bus Pass Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/pass-bwdates-reports-details.php. The manipulation of the argument fromdate/todate leads to cross site scripting. This vulnerability was named CVE-2024-44798. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-8783	OpenTibiaBR MyAAC up to 0.8.16 Post Reply new_post.php post_topic cross site scripting (Issue 121)	A vulnerability classified as problematic has been found in OpenTibiaBR MyAAC up to 0.8.16. Affected is an unknown function of the file system/pages/forum/n	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		ew_post.php of the component Post Reply Handler. The manipulation of the argument post_topic leads to cross site scripting. This vulnerability is traded as CVE-2024-8783. It is possible to launch the attack remotely. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue.		
CVE-2024-8863	aimhubio aim up to 3.24 Text Explorer textbox.tsx dangerouslySetInnerHTML query cross site scripting	A vulnerability which was classified as problematic was found in aimhubio aim up to 3.24. Affected is the function dangerouslySetInnerHTML of the file textbox.tsx of the component Text Explorer. The manipulation of the argument query leads to cross site scripting. This vulnerability is traded as CVE-2024-8863. 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	Y
CVE-2024-8867	Perfex CRM 3.1.6 Parameter Clients.php message cross site scripting	A vulnerability was found in Perfex CRM 3.1.6. It has been declared as problematic. This vulnerability affects unknown code of the file application/controllers/Clients.php of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component Parameter Handler. The manipulation of the argument message leads to cross site scripting. This vulnerability was named CVE-2024-8867. The attack can be initiated remotely. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue.		
CVE-2024-8866	AutoCMS 5.4 /admin/robot.php sidebar cross site scripting (Issue 68)	A vulnerability was found in AutoCMS 5.4. It has been classified as problematic. This affects an unknown part of the file /admin/robot.php. The manipulation of the argument sidebar leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-8866. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8661	Concrete CMS up to 8.5.17/9.3.3 Next/Previous Nav Block cross site scripting	A vulnerability was found in Concrete CMS up to 8.5.17/9.3.3. It has been rated as problematic. This issue affects some unknown processing of the component Next/Previous Nav Block Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-8661. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component.		
CVE-2024-8951	SourceCodester Resort Reservation System 1.0 manage_fee.php toview cross site scripting	A vulnerability classified as problematic was found in SourceCodester Resort Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the file manage_fee.php. The manipulation of the argument toview leads to cross site scripting. This vulnerability is known as CVE-2024-8951. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-45812	vitejs Vite up to 3.2.10/4.5.4/5.2.13/5.3.5/5.4.5 cross site scripting (GHSA-64vr-g452-qvp3)	A vulnerability which was classified as problematic was found in vitejs Vite up to 3.2.10/4.5.4/5.2.13/5.3.5/5.4.5. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-45812. 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-2024-8660	Concrete CMS up to 9.3.3 Top Navigator Bar cross site scripting	A vulnerability which was classified as problematic was found in Concrete CMS up to 9.3.3. Affected is an unknown function of the component Top Navigator Bar. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-8660. It is possible to launch the attack	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-8051	Special Feed Items Plugin up to 1.0.1 on WordPress cross site scripting	A vulnerability was found in Special Feed Items Plugin up to 1.0.1 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-2024-8051. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-8092	Accordion Image Menu Plugin up to 3.1.3 on WordPress cross site scripting	A vulnerability was found in Accordion Image Menu Plugin up to 3.1.3 on WordPress. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-8092. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-5170	Logo Manager for Enamad Plugin up to 0.7.1 on WordPress Setting cross site scripting	A vulnerability has been found in Logo Manager for Enamad Plugin up to 0.7.1 on WordPress and classified as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-5170.	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.		
CVE-2024-9007	jeanmarc77 123solar 1.8.4.5 /detailed.php date1 cross site scripting (Issue 73)	A vulnerability classified as problematic has been found in jeanmarc77 123solar 1.8.4.5. This affects an unknown part of the file /detailed.php. The manipulation of the argument date1 leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-9007. 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.	Patched by core rule	Y
CVE-2024-9033	SourceCodester Best House Rental Management System 1.0 ajax.php name cross site scripting	A vulnerability has been found in SourceCodester Best House Rental Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /ajax.phpactionsave_category. The manipulation of the argument name leads to cross site scripting. This vulnerability is known as CVE-2024-9033. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9030	CodeCanyon CRMGo SaaS 7.2 /deal/{note_id}/note notes cross site scripting	A vulnerability classified as problematic was found in CodeCanyon CRMGo SaaS 7.2. This vulnerability affects unknown code of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		file /deal/{note_id}/note. The manipulation of the argument notes leads to cross site scripting. This vulnerability was named CVE-2024-9030. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-9041	SourceCodester Best House Rental Management System 1.0 ajax.php firstname/lastname/ email sql injection	A vulnerability has been found in SourceCodester Best House Rental Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /ajax.phpactionupdate_account. The manipulation of the argument firstname/lastname/email leads to sql injection. This vulnerability was named CVE-2024-9041. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9039	SourceCodester Best House Rental Management System 1.0 /ajax.php firstname/lastname/ email sql injection	A vulnerability which was classified as critical has been found in SourceCodester Best House Rental Management System 1.0. Affected by this issue is some unknown functionality of the file /ajax.phpactionsignup. The manipulation of the argument firstname/lastname/email leads to sql injection. This vulnerability is handled as CVE-2024-9039. The attack may 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-2024-9092	SourceCodester Profile Registration without Reload Refresh 1.0 Registration Form add.php full_name cross site scripting	A vulnerability was found in SourceCodester Profile Registration without Reload Refresh 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file add.php of the component Registration Form. The manipulation of the argument full_name leads to cross site scripting. This vulnerability is handled as CVE-2024-9092. The attack may be launched remotely. Furthermore there is an exploit available. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2024-7846	YITH WooCommerce Ajax Search Plugin up to 2.7.0 on WordPress Block Attribute cross site scripting	A vulnerability was found in YITH WooCommerce Ajax Search Plugin up to 2.7.0 on WordPress. It has been declared as problematic. This vulnerability affects unknown code of the component Block Attribute Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-7846. 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-2024-47068	Rollup up to 3.29.4/4.22.3 cross site scripting (GHSA-	A vulnerability was found in Rollup up to 3.29.4/4.22.3. It has	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	gcx4-mw62-g8wm)	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-2024-47068. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-46639	HelpDeskZ 2.0.2 Name cross site scripting	A vulnerability was found in HelpDeskZ 2.0.2. It has been classified as problematic. Affected is an unknown function. The manipulation of the argument Name leads to cross site scripting. This vulnerability is traded as CVE-2024-46639. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-7878	WP ULike Plugin up to 4.7.3 on WordPress Setting cross site scripting	A vulnerability classified as problematic was found in WP ULike Plugin up to 4.7.3 on WordPress. 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-2024-7878. The attack can be launched 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.

Indusface, an institutionally funded firm, is the only vendor to receive 100% customer recommendation rating four years in a row and is a global customer choice in the 2024 Gartner Peer Insights™ Web Application and API Protection (WAAP) Report. Indusface is also a “Great Place to Work” 2024 certified and is PCI, ISO27001, SOC 2, GDPR certified and has been the recipient of many prestigious start-up awards.

Indusface is the only cloud WAAP (WAF) vendor with 100% customer recommendation for 4 consecutive years

A Customers' Choice from 2022 to 2024 Gartner® Peer Insights™