INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

August 2024

The total **zero-day vulnerabilities** count for August month: 266

Command Injection	CSRF	Local File Inclusion	SQLi	Malicious File Upload	Cross-Site Scripting	XXE
34	38	14	88	8	83	1

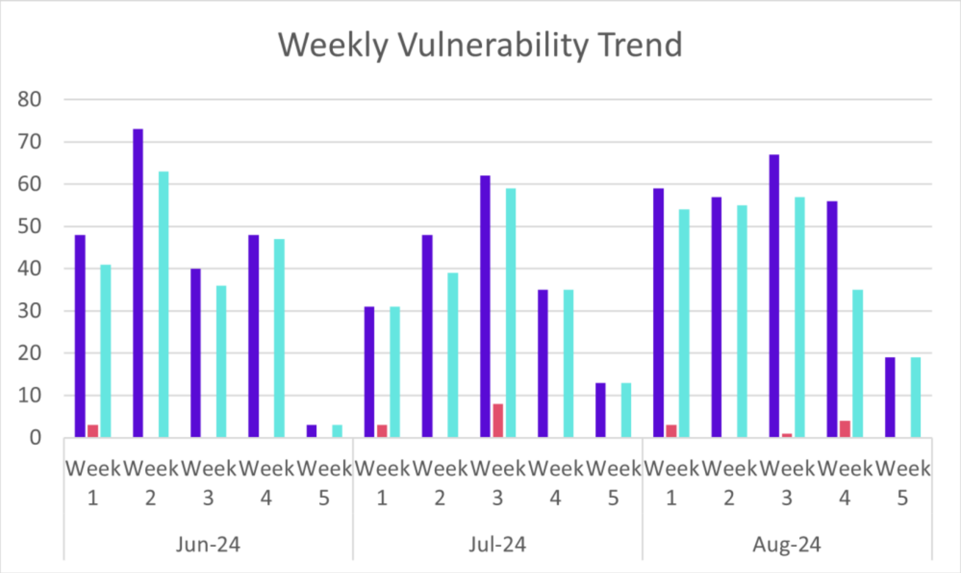
Zero-day vulnerabilities protected through core rules	258
Zero-day vulnerabilities protected through custom rules	8
Zero-day vulnerabilities for which protection cannot be done	0
Zero-day vulnerabilities found by Indusface WAS	220

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

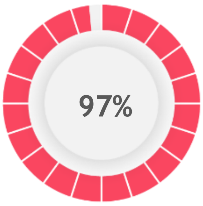
Vulnerability Trend:

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

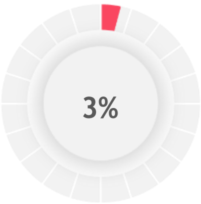
Weekly Vulnerability Trend



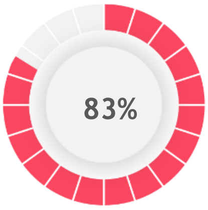
- 🟪 Total Blocked/Logged Web AppSec Zero-Day Vulnerabilities by Core Rules
- 🟩 Total Custom Patch Required for Web AppSec Zero-Day Vulnerabilities
- 🟦 Total Zero-Day Vulnerabilities found by Indusface Scanner



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

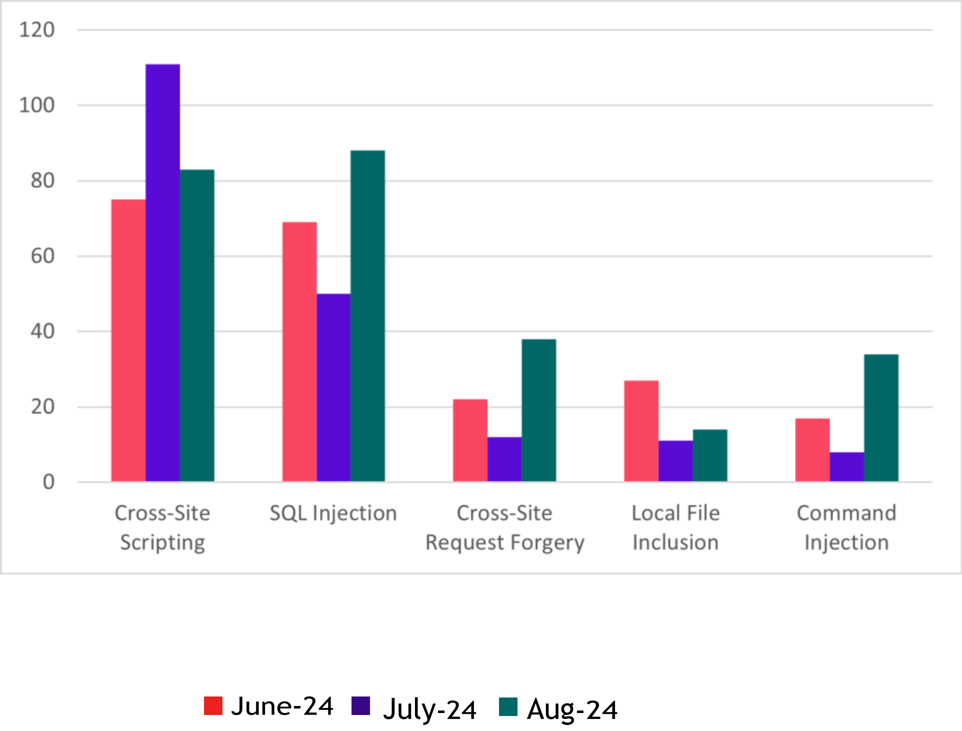


of the zero-day vulnerabilities were protected by the custom rules in the last month



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

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-7160	TOTOLINK A3700R 9.1.2u.5822_B20200513 /cgi-bin/cstecgi.cgi setWanCfg hostName command injection	A vulnerability classified as critical has been found in TOTOLINK A3700R 9.1.2u.5822_B20200513. Affected is the function setWanCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument hostName leads to command injection. This vulnerability is traded as CVE-2024-7160. 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-2024-7158	TOTOLINK A3100R 4.1.2cu.5050_B20200504 HTTP POST Request /cgi-bin/cstecgi.cgi setTelnetCfg telnet_enabled command injection	A vulnerability was found in TOTOLINK A3100R 4.1.2cu.5050_B20200504. It has been declared as critical. This vulnerability affects the function setTelnetCfg of the file /cgi-bin/cstecgi.cgi of the component HTTP POST Request Handler. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument telnet_enabled leads to command injection. This vulnerability was named CVE-2024-7158. 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.		
CVE-2024-7181	TOTOLINK A3600R 4.1.2cu.5182_B20201102 /cgi-bin/cstecgi.cgi setTelnetCfg telnet_enabled command injection	A vulnerability classified as critical was found in TOTOLINK A3600R 4.1.2cu.5182_B20201102. This vulnerability affects the function setTelnetCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument telnet_enabled leads to command injection. This vulnerability was named CVE-2024-7181. 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	Y
CVE-2024-7175	TOTOLINK A3600R 4.1.2cu.5182_B20201102 /cgi-bin/cstecgi.cgi setDiagnosisCfg ipDoamin os command injection	A vulnerability has been found in TOTOLINK A3600R 4.1.2cu.5182_B20201102 and classified as critical. This vulnerability affects the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument ipDoamin leads to os command injection. This vulnerability was named CVE-2024-7175. 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	Y
CVE-2024-7171	TOTOLINK A3600R	A vulnerability	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	4.1.2cu.5182_B20201102 /cgi-bin/cstecgi.cgi NTPSyncWithHost hostTime os command injection	classified as critical has been found in TOTOLINK A3600R 4.1.2cu.5182_B20201102. Affected is the function NTPSyncWithHost of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument hostTime leads to os command injection. This vulnerability is traded as CVE-2024-7171. 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.	core rule	
CVE-2024-7215	TOTOLINK LR1200 9.3.1cu.2832 /cgi-bin/cstecgi.cgi NTPSyncWithHost host_time command injection	A vulnerability was found in TOTOLINK LR1200 9.3.1cu.2832 and classified as critical. Affected by this issue is the function NTPSyncWithHost of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument host_time leads to command injection. This vulnerability is handled as CVE-2024-7215. 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-2024-7214	TOTOLINK LR350 9.3.5u.6369_B20220309 /cgi-bin/cstecgi.cgi setWanCfg hostName command injection	A vulnerability has been found in TOTOLINK LR350 9.3.5u.6369_B20220309 and classified as critical. Affected by this vulnerability is the function setWanCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument hostName leads to command injection. This vulnerability is known as CVE-2024-7214. The attack can be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-7464	TOTOLINK CP900 6.3c.566 Telnet Service setTelnetCfg telnet_enabled command injection	A vulnerability which was classified as critical has been found in TOTOLINK CP900 6.3c.566. This issue affects the function setTelnetCfg of the component Telnet Service. The manipulation of the argument telnet_enabled leads to command injection. The identification of this vulnerability is CVE-2024-7464. 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-2024-7467	Raisecom MSG1200/MSG2100E/MSG2200/MSG2300 3.90 Web Interface /vpn/list_ip_network.php sslvpn_config_mod template/stylenum os command injection	A vulnerability was found in Raisecom MSG1200 MSG2100E MSG2200 and MSG2300 3.90 and classified as critical. Affected by this issue is the function sslvpn_config_mod of the file /vpn/list_ip_network.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. This vulnerability is handled as CVE-2024-7467. 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-2024-7468	Raisecom MSG1200/MSG2100E/MSG2200/MSG2300	A vulnerability was found in Raisecom MSG1200 MSG2100E	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	3.90 Web Interface list_service_manage.php sslvpn_config_mod template/stylenum os command injection	MSG2200 and MSG2300 3.90. It has been classified as critical. This affects the function sslvpn_config_mod of the file /vpn/list_service_manage.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. This vulnerability is uniquely identified as CVE-2024-7468. 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.		
CVE-2024-7469	Raisecom MSG1200/MSG2100E/MSG2200/MSG2300 3.90 Web Interface list_vpn_web_custom.php sslvpn_config_mod template/stylenum os command injection	A vulnerability was found in Raisecom MSG1200 MSG2100E MSG2200 and MSG2300 3.90. It has been declared as critical. This vulnerability affects the function sslvpn_config_mod of the file /vpn/list_vpn_web_custom.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. This vulnerability was named CVE-2024-7469. 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	Y
CVE-2024-7470	Raisecom MSG1200/MSG2100E/MSG2200/MSG2300 3.90 Web Interface vpn_template_style.php sslvpn_config_mod template/stylenum	A vulnerability was found in Raisecom MSG1200 MSG2100E MSG2200 and MSG2300 3.90. It has been rated as critical. This issue affects the function	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	os command injection	sslvpn_config_mod of the file /vpn/vpn_template_style.php of the component Web Interface. The manipulation of the argument template/stylenum leads to os command injection. The identification of this vulnerability is CVE-2024-7470. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-39228	gl-inet SF1200 check_config os command injection	A vulnerability was found in gl-inet AR750 AR750S AR300M AR300M16 MT300N-V2 B1300 MT1300 SFT1200 X750 MT3000 MT2500 AXT1800 AX1800 A1300 X300B XE300 E750 AP1300 S1300 XE3000 X3000 B2200 MV1000 MV1000W USB150 N300 and SF1200. It has been rated as critical. Affected by this issue is the function check_config. The manipulation leads to os command injection. This vulnerability is handled as CVE-2024-39228. The attack needs to be approached within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-39227	gl-inet X3000 check_ovpn_client_config os command injection	A vulnerability which was classified as critical has been found in gl-inet AR750 AR750S AR300M AR300M16 MT300N-V2 B1300 MT1300 SFT1200 X750 MT3000 MT2500 AXT1800 AX1800 A1300 X300B XE300 E750 AP1300 S1300 XE3000 and X3000. This issue affects the function check_ovpn_client_config. The manipulation leads to os command injection.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The identification of this vulnerability is CVE-2024-39227. The attack needs to be done within the local network. There is no exploit available.		
CVE-2024-7580	Alien Technology ALR-F800 up to 19.10.24.00 /admin/system.html uploadedFile os command injection	A vulnerability was found in Alien Technology ALR-F800 up to 19.10.24.00. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/system.html. The manipulation of the argument uploadedFile with the input ;whoami leads to os command injection. This vulnerability is handled as CVE-2024-7580. 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. It is recommended to apply restrictive firewalling.	Patched by core rule	Y
CVE-2024-7579	Alien Technology ALR-F800 up to 19.10.24.00 File Name upgrade.cgi popen uploadedFile os command injection	A vulnerability was found in Alien Technology ALR-F800 up to 19.10.24.00. It has been declared as critical. Affected by this vulnerability is the function popen of the file /var/www/cgi-bin/upgrade.cgi of the component File Name Handler. The manipulation of the argument uploadedFile leads to os command injection. This vulnerability is known as CVE-2024-7579. 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. It is recommended to apply restrictive firewalling.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-42741	TOTOLINK X5000r 9.1.0cu.2350_b20230313 /cgi-bin/cstecgi.cgi setL2tpServerCfg os command injection	A vulnerability was found in TOTOLINK X5000r 9.1.0cu.2350_b20230313. It has been rated as critical. Affected by this issue is the function setL2tpServerCfg of the file /cgi-bin/cstecgi.cgi. The manipulation leads to os command injection. This vulnerability is handled as CVE-2024-42741. The attack can only be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-42743	TOTOLINK X5000r 9.1.0cu.2350_b20230313 /cgi-bin/cstecgi.cgi setSyslogCfg os command injection	A vulnerability was found in TOTOLINK X5000r 9.1.0cu.2350_b20230313 and classified as critical. Affected by this issue is the function setSyslogCfg of the file /cgi-bin/cstecgi.cgi. The manipulation leads to os command injection. This vulnerability is handled as CVE-2024-42743. The attack needs to be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-42747	TOTOLINK X5000r 9.1.0cu.2350_b20230313 /cgi-bin/cstecgi.cgi setWanIeCfg os command injection	A vulnerability was found in TOTOLINK X5000r 9.1.0cu.2350_b20230313. It has been rated as critical. This issue affects the function setWanIeCfg of the file /cgi-bin/cstecgi.cgi. The manipulation leads to os command injection. The identification of this vulnerability is CVE-2024-42747. The attack needs to be approached within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-42742	TOTOLINK X5000r 9.1.0cu.2350_b20230313 /cgi-bin/cstecgi.cgi setUrlFilterRules os command injection	A vulnerability was found in TOTOLINK X5000r 9.1.0cu.2350_b20230313. It has been classified as critical. Affected is the function setUrlFilterRules of the file /cgi-bin/cstecgi.cgi. The manipulation leads to os command injection.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is traded as CVE-2024-42742. The attack needs to be approached within the local network. There is no exploit available.		
CVE-2024-42745	TOTOLINK X5000r 9.1.0cu.2350_b20230313 /cgi-bin/cstecgi.cgi setUPnPCfg os command injection	A vulnerability was found in TOTOLINK X5000r 9.1.0cu.2350_b20230313. It has been declared as critical. This vulnerability affects the function setUPnPCfg of the file /cgi-bin/cstecgi.cgi. The manipulation leads to os command injection. This vulnerability was named CVE-2024-42745. Access to the local network is required for this attack to succeed. There is no exploit available.	Patched by core rule	Y
CVE-2024-42744	TOTOLINK X5000r 9.1.0cu.2350_b20230313 /cgi-bin/cstecgi.cgi setModifyVpnUser os command injection	A vulnerability was found in TOTOLINK X5000r 9.1.0cu.2350_b20230313. It has been classified as critical. This affects the function setModifyVpnUser of the file /cgi-bin/cstecgi.cgi. The manipulation leads to os command injection. This vulnerability is uniquely identified as CVE-2024-42744. Access to the local network is required for this attack. There is no exploit available.	Patched by core rule	Y
CVE-2024-42748	TOTOLINK X5000r 9.1.0cu.2350_b20230313 /cgi-bin/cstecgi.cgi setWiFiWpsCfg os command injection	A vulnerability classified as critical has been found in TOTOLINK X5000r 9.1.0cu.2350_b20230313. Affected is the function setWiFiWpsCfg of the file /cgi-bin/cstecgi.cgi. The manipulation leads to os command injection. This vulnerability is traded as CVE-2024-42748. The attack can only be done within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-42738	TOTOLINK X5000r 9.1.0cu.2350_b20230	A vulnerability classified as critical was	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	313 /cgi-bin/cstecgi.cgi setDmzCfg os command injection	found in TOTOLINK X5000r 9.1.0cu.2350_b20230313. Affected by this vulnerability is the function setDmzCfg of the file /cgi-bin/cstecgi.cgi. The manipulation leads to os command injection. This vulnerability is known as CVE-2024-42738. The attack can be launched remotely. There is no exploit available.		
CVE-2024-42737	TOTOLINK X5000r 9.1.0cu.2350_b20230313 /cgi-bin/cstecgi.cgi delBlacklist os command injection	A vulnerability classified as critical has been found in TOTOLINK X5000r 9.1.0cu.2350_b20230313. Affected is the function delBlacklist of the file /cgi-bin/cstecgi.cgi. The manipulation leads to os command injection. This vulnerability is traded as CVE-2024-42737. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-42739	TOTOLINK X5000r 9.1.0cu.2350_b20230313 /cgi-bin/cstecgi.cgi setAccessDeviceCfg os command injection	A vulnerability was found in TOTOLINK X5000r 9.1.0cu.2350_b20230313 and classified as critical. Affected by this issue is the function setAccessDeviceCfg of the file /cgi-bin/cstecgi.cgi. The manipulation leads to os command injection. This vulnerability is handled as CVE-2024-42739. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-42947	Tenda FH1201 1.2.0.14(408) HTTP /goform/telnet handler command injection	A vulnerability which was classified as critical was found in Tenda FH1201 1.2.0.14. This affects the function handler of the file /goform/telnet of the component HTTP Handler. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2024-42947. It is possible to initiate the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack remotely. There is no exploit available.		
CVE-2024-42978	Tenda FH1206 02.03.01.35 HTTP /goform/telnet handler command injection	A vulnerability which was classified as critical has been found in Tenda FH1206 02.03.01.35. This issue affects the function handler of the file /goform/telnet of the component HTTP Handler. The manipulation leads to command injection. The identification of this vulnerability is CVE-2024-42978. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-7907	TOTOLINK X6000R 9.4.0cu.852_20230719 /cgi-bin/cstecgi.cgi setSyslogCfg rtLogServer command injection	A vulnerability which was classified as critical has been found in TOTOLINK X6000R 9.4.0cu.852_20230719. This issue affects the function setSyslogCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument rtLogServer leads to command injection. The identification of this vulnerability is CVE-2024-7907. 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-2024-42633	Linksys E1500 1.0.06.001 do_upgrade_post os command injection	A vulnerability has been found in Linksys E1500 1.0.06.001 and classified as critical. Affected by this vulnerability is the function do_upgrade_post. The manipulation leads to os command injection. This vulnerability is known as CVE-2024-42633. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-7922	D-Link DNS-1550-04 up to 20240814 /cgi-bin/myMusic.cgi command injection	A vulnerability was found in D-Link DNS-120 DNR-202L DNS-315L DNS-320 DNS-320L DNS-320LW DNS-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		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 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability is handled as CVE-2024-7922. The attack may 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-2024-43027	Draytek Vigor 3900/Vigor 2960/Vigor 300B prior 1.5.1.5_Beta cgi-bin/mainfunction.cgi action command injection	A vulnerability which was classified as critical was found in Draytek Vigor 3900 Vigor 2960 and Vigor 300B. This affects an unknown part of the file cgi-bin/mainfunction.cgi. The manipulation of the argument action leads to command injection. This vulnerability is uniquely identified as CVE-2024-43027. 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-44382	D-Link DI_8004W 16.07.26A1 jhttpd upgrade_filter_asp command injection	A vulnerability was found in D-Link DI_8004W 16.07.26A1. It has been declared as critical. This vulnerability affects the function upgrade_filter_asp of the component jhttpd. The manipulation leads to command injection. This vulnerability was named CVE-2024-44382. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-44381	D-Link DI_8004W 16.07.26A1 jhttpd msp_info_htm command injection	A vulnerability which was classified as critical was found in D-Link DI_8004W 16.07.26A1. Affected is the function msp_info_htm of the component jhttpd. The manipulation leads to command injection. This vulnerability is traded as CVE-2024-44381. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-6490	Master Slider Plugin up to 3.9.10 on WordPress cross-site request forgery	A vulnerability was found in Master Slider Plugin up to 3.9.10 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-2024-6490. The attack may be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-7169	SourceCodester School Fees Payment System 1.0 /ajax.php cross-site request forgery	A vulnerability classified as problematic has been found in SourceCodester School Fees Payment System 1.0. This affects an unknown part of the file /ajax.php. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2024-7169. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	N
CVE-2024-6412	HTML Forms Plugin up to 1.3.33 on WordPress cross-site request forgery	A vulnerability was found in HTML Forms Plugin up to 1.3.33 on WordPress. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2024-6412. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	N
CVE-2024-3983	WooCommerce Customers Manager Plugin up to 30.0 on WordPress cross-site request forgery	A vulnerability which was classified as problematic has been found in WooCommerce Customers Manager Plugin up to 30.0 on WordPress. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		forgery. This vulnerability is handled as CVE-2024-3983. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-6496	Light Poll Plugin up to 1.0.0 on WordPress cross-site request forgery	A vulnerability which was classified as problematic was found in Light Poll Plugin up to 1.0.0 on WordPress. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2024-6496. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-7460	OSWAPP Warehouse Inventory System 1.0/2.0 /change_password.php cross-site request forgery	A vulnerability was found in OSWAPP Warehouse Inventory System 1.0/2.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /change_password.php. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2024-7460. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	N
CVE-2024-7459	OSWAPP Warehouse Inventory System 1.0/2.0 /edit_account.php cross-site request forgery	A vulnerability was found in OSWAPP Warehouse Inventory System 1.0/2.0. It has been classified as problematic. Affected is an unknown function of the file /edit_account.php. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-7459. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	N
CVE-2024-42626	FrogCMS 0.9.5 /admin/ cross-site	A vulnerability which was classified as	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	request forgery	problematic has been found in FrogCMS 0.9.5. Affected by this issue is some unknown functionality of the file /admin//snippet/add. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2024-42626. The attack may be launched remotely. There is no exploit available.		
CVE-2024-42632	FrogCMS 0.9.5 /admin/ cross-site request forgery	A vulnerability which was classified as problematic was found in FrogCMS 0.9.5. This affects an unknown part of the file /admin//page/add. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2024-42632. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-42629	FrogCMS 0.9.5 /admin/ cross-site request forgery	A vulnerability which was classified as problematic has been found in FrogCMS 0.9.5. This issue affects some unknown processing of the file /admin//page/edit/10. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-42629. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-42623	FrogCMS 0.9.5 /admin/ cross-site request forgery	A vulnerability classified as problematic was found in FrogCMS 0.9.5. Affected by this vulnerability is an unknown functionality of the file /admin//layout/delete/1. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2024-42623. The attack can be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-42628	FrogCMS 0.9.5	A vulnerability classified	Patched by	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	/admin/ cross-site request forgery	as problematic was found in FrogCMS 0.9.5. This vulnerability affects unknown code of the file /admin//snippet/edit/3. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2024-42628. The attack can be initiated remotely. There is no exploit available.	core rule	
CVE-2024-42625	FrogCMS 0.9.5 /admin/ cross-site request forgery	A vulnerability which was classified as problematic was found in FrogCMS 0.9.5. This affects an unknown part of the file /admin//layout/add. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2024-42625. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-42627	FrogCMS 0.9.5 cross-site request forgery	A vulnerability was found in FrogCMS 0.9.5. It has been declared as problematic. This vulnerability affects unknown code of the file /admin//snippet/delete/3. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2024-42627. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-42624	FrogCMS 0.9.5 /admin/ cross-site request forgery	A vulnerability classified as problematic has been found in FrogCMS 0.9.5. Affected is an unknown function of the file /admin//page/delete/10. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-42624. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-42631	FrogCMS 0.9.5 /admin/ cross-site request forgery	A vulnerability has been found in FrogCMS 0.9.5 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/admin//layout/edit/1. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2024-42631. The attack can be launched remotely. There is no exploit available.		
CVE-2024-42630	FrogCMS 0.9.5 cross-site request forgery	A vulnerability which was classified as problematic was found in FrogCMS 0.9.5. Affected is an unknown function of the file /admin//plugin/file_manager/create_file. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-42630. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-42579	Warehouse Inventory System 2.0 add_group.php cross-site request forgery	A vulnerability was found in Warehouse Inventory System 2.0. It has been classified as problematic. Affected is an unknown function of the file add_group.php. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-42579. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	N
CVE-2024-42580	Warehouse Inventory System 2.0 edit_group.php cross-site request forgery	A vulnerability was found in Warehouse Inventory System 2.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file edit_group.php. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2024-42580. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	N
CVE-2024-42577	Warehouse Inventory System 2.0 add_product.php	A vulnerability has been found in Warehouse Inventory System 2.0 and classified as	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	cross-site request forgery	problematic. This vulnerability affects unknown code of the file add_product.php. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2024-42577. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-42582	Warehouse Inventory System 2.0 delete_categorie.php cross-site request forgery	A vulnerability classified as problematic has been found in Warehouse Inventory System 2.0. This affects an unknown part of the file delete_categorie.php. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2024-42582. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	N
CVE-2024-42581	Warehouse Inventory System 2.0 delete_group.php cross-site request forgery	A vulnerability was found in Warehouse Inventory System 2.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file delete_group.php. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2024-42581. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	N
CVE-2024-42583	Warehouse Inventory System 2.0 delete_user.php cross-site request forgery	A vulnerability classified as problematic was found in Warehouse Inventory System 2.0. This vulnerability affects unknown code of the file delete_user.php. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2024-42583. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	N
CVE-2024-42584	Warehouse Inventory System	A vulnerability which was classified as	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	2.0 delete_product.php cross-site request forgery	problematic has been found in Warehouse Inventory System 2.0. This issue affects some unknown processing of the file delete_product.php. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-42584. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-42611	Pligg CMS 2.0.2 cross-site request forgery	A vulnerability was found in Pligg CMS 2.0.2. It has been rated as problematic. Affected by this issue is some unknown functionality of the file admin/admin_page.phplink_id1/modedelete. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2024-42611. The attack may be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-42618	Pligg CMS 2.0.2 /module.php cross-site request forgery	A vulnerability classified as problematic was found in Pligg CMS 2.0.2. Affected by this vulnerability is an unknown functionality of the file /module.phpmodulekarma. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2024-42618. The attack can be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-42605	Pligg CMS 2.0.2 edit_page.php cross-site request forgery	A vulnerability was found in Pligg CMS 2.0.2. It has been classified as problematic. Affected is an unknown function of the file /admin/edit_page.phplink_id1. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-42605. It is possible to	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		launch the attack remotely. There is no exploit available.		
CVE-2024-42604	Pligg CMS 2.0.2 cross-site request forgery	A vulnerability has been found in Pligg CMS 2.0.2 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/admin_group.phpmodedelete/group_id3. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2024-42604. The attack can be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-42621	Pligg CMS 2.0.2 /admin/admin_editor.php cross-site request forgery	A vulnerability which was classified as problematic has been found in Pligg CMS 2.0.2. This issue affects some unknown processing of the file /admin/admin_editor.php. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-42621. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-42616	Pligg CMS 2.0.2 cross-site request forgery	A vulnerability which was classified as problematic was found in Pligg CMS 2.0.2. Affected is an unknown function of the file /admin/admin_widgets.phpactionremove/widgetStatistics. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-42616. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-42606	Pligg CMS 2.0.2 admin_log.php cross-site request forgery	A vulnerability was found in Pligg CMS 2.0.2 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/admin_log.phpclear1. The manipulation leads to cross-site request forgery.	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is handled as CVE-2024-42606. The attack may be launched remotely. There is no exploit available.		
CVE-2024-42617	Pligg CMS 2.0.2 cross-site request forgery	A vulnerability classified as problematic was found in Pligg CMS 2.0.2. This vulnerability affects unknown code of the file /admin/admin_config.phpactionsave/var_id32. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2024-42617. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-42613	Pligg CMS 2.0.2 cross-site request forgery	A vulnerability classified as problematic has been found in Pligg CMS 2.0.2. This affects an unknown part of the file /admin/admin_widgets.phpactioninstall/widgetakismet. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2024-42613. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-42603	Pligg CMS 2.0.2 admin_backup.php cross-site request forgery	A vulnerability was found in Pligg CMS 2.0.2 and classified as problematic. This issue affects some unknown processing of the file /admin/admin_backup.phpdobackupclearall. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-42603. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-42607	Pligg CMS 2.0.2 admin_backup.php cross-site request forgery	A vulnerability was found in Pligg CMS 2.0.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/admin_backup.phpdobackupdatabase. The manipulation leads to cross-site request	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		forgery. This vulnerability is known as CVE-2024-42607. The attack can be launched remotely. There is no exploit available.		
CVE-2024-42608	Pligg CMS 2.0.2 /admin/submit_page.php cross-site request forgery	A vulnerability was found in Pligg CMS 2.0.2 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/submit_page.php. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2024-42608. The attack may be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-42610	Pligg CMS 2.0.2 admin_backup.php cross-site request forgery	A vulnerability classified as problematic has been found in Pligg CMS 2.0.2. Affected is an unknown function of the file /admin/admin_backup.phpdobackupfiles. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-42610. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-42609	Pligg CMS 2.0.2 admin_backup.php cross-site request forgery	A vulnerability was found in Pligg CMS 2.0.2. It has been rated as problematic. This issue affects some unknown processing of the file /admin/admin_backup.phpdobackupavatars. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-42609. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	N

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-41628	Severalnines Cluster Control prior 1.9.8-9778/2.0.0-9779/2.1.0-9780 CMON API path traversal	A vulnerability has been found in Severalnines Cluster Control and classified as critical. Affected by this vulnerability is an unknown functionality of the component CMON API. The manipulation leads to path traversal. This vulnerability is known as CVE-2024-41628. 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-2024-6255	gaizhenbiao ChuanhuChatGPT up to 20240410 JSON File config.json file inclusion	A vulnerability was found in gaizhenbiao ChuanhuChatGPT up to 20240410 and classified as critical. This issue affects some unknown processing of the file config.json of the component JSON File Handler. The manipulation leads to file inclusion. The identification of this vulnerability is CVE-2024-6255. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-6459	News Element Elementor Blog Magazine Plugin up to 1.0.5 on WordPress file inclusion	A vulnerability was found in News Element Elementor Blog Magazine Plugin up to 1.0.5 on WordPress. It has been rated as critical. Affected by this issue is some unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		functionality. The manipulation leads to file inclusion. This vulnerability is handled as CVE-2024-6459. The attack needs to be approached within the local network. There is no exploit available.		
CVE-2024-6331	stitionai devika up to 1.0 Google Gimini file inclusion	A vulnerability has been found in stitionai devika up to 1.0 and classified as problematic. This vulnerability affects unknown code of the component Google Gimini. The manipulation leads to file inclusion. This vulnerability was named CVE-2024-6331. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-7458	elunez eladmin up to 2.7 Database Management/Deployment Management upload file path traversal (Issue 851)	A vulnerability was found in elunez eladmin up to 2.7 and classified as critical. This issue affects some unknown processing of the file /api/deploy/upload /api/database/upload of the component Database Management/Deployment Management. The manipulation of the argument file leads to path traversal: &039;dir/../../filename&039;. The identification of this vulnerability is CVE-2024-7458. Access to the local network is required for this attack. Furthermore there is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		an exploit available.		
CVE-2024-7497	itsourcecode Airline Reservation System 1.0 /admin/index.php page file inclusion	A vulnerability was found in itsourcecode Airline Reservation System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/index.php. The manipulation of the argument page leads to file inclusion. The identification of this vulnerability is CVE-2024-7497. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7496	itsourcecode Airline Reservation System 1.0 /index.php page file inclusion	A vulnerability has been found in itsourcecode Airline Reservation System 1.0 and classified as critical. This vulnerability affects unknown code of the file /index.php. The manipulation of the argument page leads to file inclusion. This vulnerability was named CVE-2024-7496. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-39226	gl-inet X3000 /cgi-bin/glc path traversal	A vulnerability was found in gl-inet AR750 AR750S AR300M AR300M16 MT300N-V2 B1300 MT1300 SFT1200 X750 MT3000 MT2500 AXT1800 AX1800 A1300 X300B XE300 E750 AP1300 S1300 XE3000 and X3000. It has been declared as critical. Affected by this	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability is an unknown functionality of the file /cgi-bin/glc. The manipulation leads to path traversal. This vulnerability is known as CVE-2024-39226. Access to the local network is required for this attack to succeed. There is no exploit available.		
CVE-2024-7551	juzaweb CMS up to 3.4.2 Theme Editor default path traversal	A vulnerability was found in juzaweb CMS up to 3.4.2. It has been classified as problematic. Affected is an unknown function of the file /admin-cp/theme/editor/default of the component Theme Editor. The manipulation leads to path traversal. This vulnerability is traded as CVE-2024-7551. 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-2024-6707	Open WebUI 0.1.105 path traversal	A vulnerability which was classified as critical has been found in Open WebUI 0.1.105. This issue affects some unknown processing. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2024-6707. The attack needs to be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		initiated within the local network. There is no exploit available.		
CVE-2024-7741	wanglongcn ltcms 1.0.20 API Endpoint /api/file/downloadfile downloadFile path traversal	A vulnerability was found in wanglongcn ltcms 1.0.20 and classified as critical. This issue affects the function downloadFile of the file /api/file/downloadfile of the component API Endpoint. The manipulation of the argument file leads to path traversal. The identification of this vulnerability is CVE-2024-7741. 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-2024-42680	Super Easy Enterprise Management System up to 1.0.0 Single Quotation Mark path traversal	A vulnerability has been found in Super Easy Enterprise Management System up to 1.0.0 and classified as problematic. This vulnerability affects unknown code of the component Single Quotation Mark Handler. The manipulation leads to path traversal. This vulnerability was named CVE-2024-42680. Attacking locally is a requirement. There is no exploit available.	Patched by core rule	Y
CVE-2024-6460	Tradedoubler Grow Plugin up to 2.0.21 on WordPress component path	A vulnerability classified as critical was found in Tradedoubler Grow	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	traversal	Plugin up to 2.0.21 on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation of the argument component leads to path traversal. This vulnerability is known as CVE-2024-6460. The attack can only be done within the local network. There is no exploit available.		
CVE-2024-7924	ZZCMS 2023 /I/list.php skin path traversal	A vulnerability was found in ZZCMS 2023. It has been declared as critical. This vulnerability affects unknown code of the file /I/list.php. The manipulation of the argument skin leads to path traversal. This vulnerability was named CVE-2024-7924. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-7189	itsourcecode Online Food Ordering System 1.0 editproduct.php photo unrestricted upload	A vulnerability classified as critical has been found in itsourcecode Online Food Ordering System 1.0. Affected is an unknown function of the file editproduct.php. The manipulation of the argument photo leads to unrestricted upload. This vulnerability is traded as CVE-2024-7189. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by custom rule	N
CVE-2024-7329	YouDianCMS 7 image_upload.php files unrestricted upload	A vulnerability which was classified as critical was found in YouDianCMS 7. Affected is an unknown function of the file /Public/ckeditor/plugins/multiimage/dialogs/image_upload.php. The manipulation of the argument files leads to unrestricted upload. This vulnerability is traded as CVE-2024-7329. 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 custom rule	N
CVE-2024-7342	Baidu UEditor 1.4.3.3 controller.php upfile unrestricted upload	A vulnerability was found in Baidu UEditor 1.4.3.3. It has been classified as problematic. This	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects an unknown part of the file /ueditor/php/controller.phpactionuploadfile&amp;encodeutf-8. The manipulation of the argument upfile leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2024-7342. 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.		
CVE-2024-42676	Huizhi Enterprise Resource Management System up to 1.0 DNPageAjaxPostBack /nssys/common/Upload unrestricted upload	A vulnerability classified as critical was found in Huizhi Enterprise Resource Management System up to 1.0. Affected by this vulnerability is an unknown functionality of the file /nssys/common/Upload of the component DNPageAjaxPostBack. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2024-42676. The attack can be launched remotely. There is no exploit available.	Patched by custom rule	N
CVE-2024-42778	Kashipara Music Management System 1.0 ajax.php unrestricted upload	A vulnerability has been found in Kashipara Music Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /music/ajax.phpactionsave_playlist. The	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation leads to unrestricted upload. This vulnerability was named CVE-2024-42778. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-42777	Kashipara Music Management System 1.0 ajax.php unrestricted upload	A vulnerability which was classified as critical has been found in Kashipara Music Management System 1.0. Affected by this issue is some unknown functionality of the file /music/ajax.phpactionsignup. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2024-42777. The attack may be launched remotely. There is no exploit available.	Patched by custom rule	N
CVE-2024-42779	Kashipara Music Management System 1.0 ajax.php unrestricted upload	A vulnerability which was classified as critical was found in Kashipara Music Management System 1.0. Affected is an unknown function of the file /music/ajax.phpactionsave_music. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2024-42779. It is possible to launch the attack remotely. There is no exploit available.	Patched by custom rule	N
CVE-2024-42780	Kashipara Music Management System 1.0 ajax.php unrestricted upload	A vulnerability has been found in Kashipara Music Management System 1.0 and classified as critical. Affected by this vulnerability is an	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown functionality of the file /music/ajax.phpactionsave_genre. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2024-42780. The attack can be launched remotely. There is no exploit available.		

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-7164	SourceCodester School Fees Payment System 1.0 /ajax.php username sql injection	A vulnerability has been found in SourceCodester School Fees Payment System 1.0 and classified as critical. This vulnerability affects unknown code of the file /ajax.phpactionlogin. The manipulation of the argument username leads to sql injection. This vulnerability was named CVE-2024-7164. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7165	SourceCodester School Fees Payment System 1.0 /view_payment.php ef_id sql injection	A vulnerability was found in SourceCodester School Fees Payment System 1.0 and classified as critical. This issue affects some unknown processing of the file /view_payment.php. The manipulation of the argument ef_id leads to sql injection. The identification of this vulnerability is CVE-2024-7165. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7166	SourceCodester School Fees Payment System 1.0 /receipt.php ef_id sql injection	A vulnerability was found in SourceCodester School Fees Payment System 1.0. It has been classified as critical. Affected is an unknown function of the file /receipt.php. The manipulation of the argument ef_id 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-2024-7166. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2024-7167	SourceCodester School Fees Payment System 1.0 /manage_course.php id sql injection	A vulnerability was found in SourceCodester School Fees Payment System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /manage_course.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2024-7167. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7168	SourceCodester School Fees Payment System 1.0 /manage_user.php id sql injection	A vulnerability was found in SourceCodester School Fees Payment System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /manage_user.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-7168. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7191	itsourcecode Society Management System 1.0 /admin/get_balance.php student_id sql injection	A vulnerability which was classified as critical has been found in itsourcecode Society Management System 1.0. Affected by this issue is some unknown functionality of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/admin/get_balance.php. The manipulation of the argument student_id leads to sql injection. This vulnerability is handled as CVE-2024-7191. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-7199	SourceCodester Complaints Report Management System 1.0 /admin/manage_user.php id sql injection	A vulnerability classified as critical was found in SourceCodester Complaints Report Management System 1.0. This vulnerability affects unknown code of the file /admin/manage_user.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-7199. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7190	itsourcecode Society Management System 1.0 /admin/get_price.php expenses_id sql injection	A vulnerability classified as critical was found in itsourcecode Society Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/get_price.php. The manipulation of the argument expenses_id leads to sql injection. This vulnerability is known as CVE-2024-7190. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7194	itsourcecode Society Management System 1.0	A vulnerability was found in itsourcecode Society Management System 1.0 and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	check_student.php student_id sql injection	classified as critical. This issue affects some unknown processing of the file check_student.php. The manipulation of the argument student_id leads to sql injection. The identification of this vulnerability is CVE-2024-7194. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-7198	SourceCodester Complaints Report Management System 1.0 manage_station.php id sql injection	A vulnerability classified as critical has been found in SourceCodester Complaints Report Management System 1.0. This affects an unknown part of the file /admin/manage_station.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-7198. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7195	itsourcecode Society Management System 1.0 /admin/check_admin.php username sql injection	A vulnerability was found in itsourcecode Society Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/check_admin.php. The manipulation of the argument username leads to sql injection. This vulnerability is traded as CVE-2024-7195. It is possible to launch the attack remotely. Furthermore	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		there is an exploit available.		
CVE-2024-7311	code-projects Online Bus Reservation Site 1.0 register.php Email sql injection	A vulnerability was found in code-projects Online Bus Reservation Site 1.0. It has been rated as critical. This issue affects some unknown processing of the file register.php. The manipulation of the argument Email leads to sql injection. The identification of this vulnerability is CVE-2024-7311. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7273	itsourcecode Alton Management System 1.0 search.php rcode sql injection	A vulnerability classified as critical was found in itsourcecode Alton Management System 1.0. This vulnerability affects unknown code of the file search.php. The manipulation of the argument rcode leads to sql injection. This vulnerability was named CVE-2024-7273. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7278	itsourcecode Alton Management System 1.0 /admin/team_save.php team sql injection	A vulnerability was found in itsourcecode Alton Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/team_save.php. The manipulation of the argument team leads to sql injection. This vulnerability is uniquely identified as CVE-2024-7278. 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-2024-7275	itsourcecode Alton Management System 1.0 /admin/category_save.php category sql injection	A vulnerability which was classified as critical was found in itsourcecode Alton Management System 1.0. Affected is an unknown function of the file /admin/category_save.php. The manipulation of the argument category leads to sql injection. This vulnerability is traded as CVE-2024-7275. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7274	itsourcecode Alton Management System 1.0 /reservation_status.php rcode sql injection	A vulnerability which was classified as critical has been found in itsourcecode Alton Management System 1.0. This issue affects some unknown processing of the file /reservation_status.php. The manipulation of the argument rcode leads to sql injection. The identification of this vulnerability is CVE-2024-7274. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7276	itsourcecode Alton Management System 1.0 /admin/member_save.php last/first sql injection	A vulnerability has been found in itsourcecode Alton Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/member_save.php. The manipulation of the argument	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		last/first leads to sql injection. This vulnerability is known as CVE-2024-7276. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2024-7327	Xinhu RockOA 2.6.2 openmodhetongAction.php dataAction nickName sql injection	A vulnerability classified as critical was found in Xinhu RockOA 2.6.2. This vulnerability affects the function dataAction of the file /webmain/task/openapi/openmodhetongAction.php. The manipulation of the argument nickName leads to sql injection. This vulnerability was named CVE-2024-7327. 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	Y
CVE-2024-7320	itsourcecode Online Blood Bank Management System 1.0 Admin Login /admin/index.php user sql injection	A vulnerability classified as critical has been found in itsourcecode Online Blood Bank Management System 1.0. This affects an unknown part of the file /admin/index.php of the component Admin Login. The manipulation of the argument user leads to sql injection. This vulnerability is uniquely identified as CVE-2024-7320. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-7374	SourceCodester Simple Realtime Quiz System 1.0 /manage_user.php id sql injection	A vulnerability classified as critical was found in SourceCodester Simple Realtime Quiz System 1.0. This vulnerability affects unknown code of the file /manage_user.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-7374. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7445	itsourcecode Ticket Reservation System 1.0 checkout_ticket_save.php data sql injection	A vulnerability which was classified as critical has been found in itsourcecode Ticket Reservation System 1.0. Affected by this issue is some unknown functionality of the file checkout_ticket_save.php. The manipulation of the argument data leads to sql injection. This vulnerability is handled as CVE-2024-7445. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7446	itsourcecode Ticket Reservation System 1.0 list_tickets.php prefSeat_id sql injection	A vulnerability which was classified as critical was found in itsourcecode Ticket Reservation System 1.0. This affects an unknown part of the file list_tickets.php. The manipulation of the argument prefSeat_id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-7446. It is possible to initiate the attack remotely. Furthermore there is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		an exploit available.		
CVE-2024-7444	itsourcecode Ticket Reservation System 1.0 Login Page login.php username sql injection	A vulnerability classified as critical was found in itsourcecode Ticket Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the file login.php of the component Login Page. The manipulation of the argument username leads to sql injection. This vulnerability is known as CVE-2024-7444. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7449	itsourcecode Placement Management System 1.0 login.php email sql injection	A vulnerability which was classified as critical was found in itsourcecode Placement Management System 1.0. Affected is an unknown function of the file login.php. The manipulation of the argument email leads to sql injection. This vulnerability is traded as CVE-2024-7449. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7451	itsourcecode Placement Management System 1.0 apply_now.php id sql injection	A vulnerability was found in itsourcecode Placement Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file apply_now.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		7451. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-7452	itsourcecode Placement Management System 1.0 view_company.php id sql injection	A vulnerability was found in itsourcecode Placement Management System 1.0. It has been classified as critical. This affects an unknown part of the file view_company.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-7452. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7499	itsourcecode Airline Reservation System 1.0 flights.php departure_airport_id sql injection	A vulnerability was found in itsourcecode Airline Reservation System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file flights.php. The manipulation of the argument departure_airport_id leads to sql injection. This vulnerability is known as CVE-2024-7499. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7498	itsourcecode Airline Reservation System 1.0 Admin Login Page /admin/login.php login/login2 username sql injection	A vulnerability was found in itsourcecode Airline Reservation System 1.0. It has been classified as critical. Affected is the function login/login2 of the file /admin/login.php of the component Admin Login Page. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument username leads to sql injection. This vulnerability is traded as CVE-2024-7498. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2024-7009	Calibre up to 7.15.0 SQLite Database sql injection	A vulnerability was found in Calibre up to 7.15.0. It has been rated as critical. Affected by this issue is some unknown functionality of the component SQLite Database. The manipulation leads to sql injection. This vulnerability is handled as CVE-2024-7009. The attack may be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y
CVE-2024-34480	SourceCodester Laboratory Management System 1.0 view_category.php sql injection	A vulnerability was found in SourceCodester Laboratory Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file admin/category/view_category.php. The manipulation leads to sql injection. This vulnerability is handled as CVE-2024-34480. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-34479	SourceCodester Computer Laboratory	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
	Management System 1.0 classes/Master.php sql injection	SourceCodester Computer Laboratory Management System 1.0. This affects an unknown part of the file classes/Master.php. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2024-34479. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-41237	Kashipara Responsive School Management System 1.0 /smsa/teacher_login.php username sql injection	A vulnerability which was classified as critical was found in Kashipara Responsive School Management System 1.0. This affects an unknown part of the file /smsa/teacher_login.php. The manipulation of the argument username leads to sql injection. This vulnerability is uniquely identified as CVE-2024-41237. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40472	SourceCodester Daily Calories Monitoring Tool 1.0 delete-calorie.php sql injection	A vulnerability which was classified as critical was found in SourceCodester Daily Calories Monitoring Tool 1.0. Affected is an unknown function of the file delete-calorie.php. The manipulation leads to sql injection. This vulnerability is traded as CVE-2024-40472. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-7640	SourceCodester Kortex Lite Advocate Office Management	A vulnerability which was 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 delete_register.php case_register_id sql injection	SourceCodester Kortex Lite Advocate Office Management System 1.0. This issue affects some unknown processing of the file delete_register.php. The manipulation of the argument case_register_id leads to sql injection. The identification of this vulnerability is CVE-2024-7640. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-7639	SourceCodester Kortex Lite Advocate Office Management System 1.0 delete_act.php id sql injection	A vulnerability classified as critical was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. This vulnerability affects unknown code of the file delete_act.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-7639. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7636	code-projects Simple Ticket Booking 1.0 Login authenticate.php email/password sql injection	A vulnerability was found in code-projects Simple Ticket Booking 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file authenticate.php of the component Login. The manipulation of the argument email/password leads to sql injection. This vulnerability is known as CVE-2024-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		7636. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2024-7635	code-projects Simple Ticket Booking 1.0 Registration register_insert.php name/email/dob/password/Gender/phone sql injection	A vulnerability was found in code-projects Simple Ticket Booking 1.0. It has been classified as critical. Affected is an unknown function of the file register_insert.php of the component Registration Handler. The manipulation of the argument name/email/dob/password/Gender/phone leads to sql injection. This vulnerability is traded as CVE-2024-7635. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7642	SourceCodester Kortex Lite Advocate Office Management System 1.0 activate_act.php id sql injection	A vulnerability has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file activate_act.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2024-7642. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7638	SourceCodester Kortex Lite Advocate Office Management System 1.0 delete_client.php id sql injection	A vulnerability classified as critical has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0. This affects an unknown part of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		file delete_client.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-7638. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-7643	SourceCodester Leads Manager Tool 1.0 Delete Leads delete-leads.php leads sql injection	A vulnerability was found in SourceCodester Leads Manager Tool 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /endpoint/delete-leads.php of the component Delete Leads Handler. The manipulation of the argument leads leads to sql injection. This vulnerability is handled as CVE-2024-7643. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7641	SourceCodester Kortex Lite Advocate Office Management System 1.0 deactivate_act.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. Affected is an unknown function of the file deactivate_act.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-7641. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7637	code-projects	A vulnerability was	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Online Polling 1.0 Registration registeracc.php email sql injection	found in code-projects Online Polling 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file registeracc.php of the component Registration. The manipulation of the argument email leads to sql injection. This vulnerability is handled as CVE-2024-7637. The attack may be launched remotely. Furthermore there is an exploit available.	core rule	
CVE-2024-7665	SourceCodester Car Driving School Management System 1.0 manage_package.php id sql injection	A vulnerability classified as critical was found in SourceCodester Car Driving School Management System 1.0. Affected by this vulnerability is an unknown functionality of the file manage_package.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2024-7665. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7666	SourceCodester Car Driving School Management System 1.0 view_package.php id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Car Driving School Management System 1.0. Affected by this issue is some unknown functionality of the file view_package.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-7666. The attack may	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		be launched remotely. Furthermore there is an exploit available.		
CVE-2024-7664	SourceCodester Car Driving School Management System 1.0 view_details.php id sql injection	A vulnerability classified as critical has been found in SourceCodester Car Driving School Management System 1.0. Affected is an unknown function of the file view_details.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-7664. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7663	SourceCodester Car Driving School Management System 1.0 manage_user.php id sql injection	A vulnerability was found in SourceCodester Car Driving School Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file manage_user.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-7663. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7667	SourceCodester Car Driving School Management System 1.0 User.php delete_users id sql injection	A vulnerability which was classified as critical was found in SourceCodester Car Driving School Management System 1.0. This affects the function delete_users of the file User.php. The manipulation of the argument id leads	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to sql injection. This vulnerability is uniquely identified as CVE-2024-7667. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-7668	SourceCodester Car Driving School Management System 1.0 Master.php delete_package id sql injection	A vulnerability has been found in SourceCodester Car Driving School Management System 1.0 and classified as critical. This vulnerability affects the function delete_package of the file Master.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-7668. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7669	SourceCodester Car Driving School Management System 1.0 Master.php delete_enrollment id sql injection	A vulnerability was found in SourceCodester Car Driving School Management System 1.0 and classified as critical. This issue affects the function delete_enrollment of the file Master.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-7669. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7676	Sourcecodester Car Driving School Management System 1.0 Master.php	A vulnerability was found in Sourcecodester Car Driving School Management System	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	save_package id sql injection	1.0. It has been classified as critical. Affected is the function save_package of the file /classes/Master.phpfsave_package. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-7676. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2024-7681	code-projects College Management System 1.0 Login Page login.php email/password sql injection	A vulnerability was found in code-projects College Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file login.php of the component Login Page. The manipulation of the argument email/password leads to sql injection. This vulnerability was named CVE-2024-7681. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7682	code-projects Job Portal 1.0 rw_i_nat.php id sql injection	A vulnerability was found in code-projects Job Portal 1.0. It has been rated as critical. This issue affects some unknown processing of the file rw_i_nat.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-7682. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-7680	itsourcecode Tailoring Management System 1.0 /incedit.php id/inccat/desc/date/amount sql injection	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been classified as critical. This affects an unknown part of the file /incedit.phpid4. The manipulation of the argument id/inccat/desc/date/amount leads to sql injection. This vulnerability is uniquely identified as CVE-2024-7680. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7808	code-projects Job Portal 1.0 logindbc.php email sql injection	A vulnerability was found in code-projects Job Portal 1.0. It has been classified as critical. Affected is an unknown function of the file logindbc.php. The manipulation of the argument email leads to sql injection. This vulnerability is traded as CVE-2024-7808. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7811	SourceCodester Daily Expenses Monitoring App 1.0 delete-expense.php expense sql injection	A vulnerability classified as critical has been found in SourceCodester Daily Expenses Monitoring App 1.0. This affects an unknown part of the file /endpoint/delete-expense.php. The manipulation of the argument expense leads to sql injection. This vulnerability is uniquely identified as CVE-2024-7811. 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-2024-7794	itsourcecode Vehicle Management System 1.0 mybill.php id sql injection	A vulnerability was found in itsourcecode Vehicle Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file mybill.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-7794. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-42843	projectworlds Online Examination System 1.0 feed.php subject sql injection	A vulnerability which was classified as critical was found in projectworlds Online Examination System 1.0. Affected is an unknown function of the file feed.php. The manipulation of the argument subject leads to sql injection. This vulnerability is traded as CVE-2024-42843. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-42679	Super Easy Enterprise Management System up to 1.0.0 the/ajax/Login.ashx sql injection	A vulnerability was found in Super Easy Enterprise Management System up to 1.0.0 and classified as critical. This issue affects some unknown processing of the file the/ajax/Login.ashx. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2024-42679. It is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		possible to launch the attack on the local host. There is no exploit available.		
CVE-2024-7839	itsourcecode Billing System 1.0 addbill.php owners_id sql injection	A vulnerability classified as critical has been found in itsourcecode Billing System 1.0. This affects an unknown part of the file addbill.php. The manipulation of the argument owners_id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-7839. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7838	itsourcecode Online Food Ordering System 1.0 /addcategory.php cname sql injection	A vulnerability was found in itsourcecode Online Food Ordering System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /addcategory.php. The manipulation of the argument cname leads to sql injection. This vulnerability is handled as CVE-2024-7838. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7913	itsourcecode Billing System 1.0 /addclient1.php lname/fname/mi/address/contact/meterReader sql injection	A vulnerability was found in itsourcecode Billing System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /addclient1.php. The manipulation of the argument lname/fname/mi/address/contact/meterReader 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-2024-7913. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-7937	itsourcecode Project Expense Monitoring System 1.0 printtransfer.php transfer_id sql injection	A vulnerability classified as critical was found in itsourcecode Project Expense Monitoring System 1.0. This vulnerability affects unknown code of the file printtransfer.php. The manipulation of the argument transfer_id leads to sql injection. This vulnerability was named CVE-2024-7937. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7936	itsourcecode Project Expense Monitoring System 1.0 transferred_report.php start/end/employee sql injection	A vulnerability classified as critical has been found in itsourcecode Project Expense Monitoring System 1.0. This affects an unknown part of the file transferred_report.php. The manipulation of the argument start/end/employee leads to sql injection. This vulnerability is uniquely identified as CVE-2024-7936. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7946	itsourcecode Online Blood Bank Management System 1.0 User Signup register.php user sql injection	A vulnerability was found in itsourcecode Online Blood Bank Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file register.php of the component User	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Signup. The manipulation of the argument user leads to sql injection. This vulnerability is handled as CVE-2024-7946. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-7933	itsourcecode Project Expense Monitoring System 1.0 Backend Login login1.php user sql injection	A vulnerability was found in itsourcecode Project Expense Monitoring System 1.0. It has been classified as critical. Affected is an unknown function of the file login1.php of the component Backend Login. The manipulation of the argument user leads to sql injection. This vulnerability is traded as CVE-2024-7933. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7935	itsourcecode Project Expense Monitoring System 1.0 print.php map_id sql injection	A vulnerability was found in itsourcecode Project Expense Monitoring System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file print.php. The manipulation of the argument map_id leads to sql injection. This vulnerability is handled as CVE-2024-7935. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7934	itsourcecode Project Expense Monitoring System 1.0 execute.php sql injection	A vulnerability was found in itsourcecode Project Expense Monitoring System 1.0. It has been declared as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		critical. Affected by this vulnerability is an unknown functionality of the file execute.php. The manipulation of the argument code leads to sql injection. This vulnerability is known as CVE-2024-7934. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2024-42570	School Management System bae5aa admininsert.php medium sql injection	A vulnerability has been found in School Management System bae5aa and classified as critical. Affected by this vulnerability is an unknown functionality of the file admininsert.php. The manipulation of the argument medium leads to sql injection. This vulnerability is known as CVE-2024-42570. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-42568	School Management System bae5aa vehicle.php transport sql injection	A vulnerability which was classified as critical has been found in School Management System bae5aa. This issue affects some unknown processing of the file vehicle.php. The manipulation of the argument transport leads to sql injection. The identification of this vulnerability is CVE-2024-42568. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-42567	School Management System bae5aa /search.php sid sql	A vulnerability classified as critical has been found in School Management System	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	bae5aa. This affects an unknown part of the file /search.phpaction2. The manipulation of the argument sid leads to sql injection. This vulnerability is uniquely identified as CVE-2024-42567. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-42566	School Management System login.php password sql injection	A vulnerability was found in School Management System. It has been rated as critical. Affected by this issue is some unknown functionality of the file login.php. The manipulation of the argument password leads to sql injection. This vulnerability is handled as CVE-2024-42566. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6847	Chatbot with ChatGPT Plugin up to 2.4.4 on WordPress sql injection	A vulnerability which was classified as critical was found in Chatbot with ChatGPT Plugin up to 2.4.4 on WordPress. Affected is an unknown function. The manipulation leads to sql injection. This vulnerability is traded as CVE-2024-6847. 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-2024-42572	School Management System bae5aa unitmarks.php	A vulnerability which was classified as critical was found in School Management System	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	medium sql injection	bae5aa. This affects an unknown part of the file unitmarks.php. The manipulation of the argument medium leads to sql injection. This vulnerability is uniquely identified as CVE-2024-42572. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-42575	School Management System bae5aa substaff.php medium sql injection	A vulnerability was found in School Management System bae5aa. It has been classified as critical. Affected is an unknown function of the file substaff.php. The manipulation of the argument medium leads to sql injection. This vulnerability is traded as CVE-2024-42575. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-42574	School Management System bae5aa attendance.php medium sql injection	A vulnerability was found in School Management System bae5aa and classified as critical. This issue affects some unknown processing of the file attendance.php. The manipulation of the argument medium leads to sql injection. The identification of this vulnerability is CVE-2024-42574. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-42573	School Management System bae5aa dtmarks.php	A vulnerability has been found in School Management System bae5aa and classified	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	medium sql injection	as critical. This vulnerability affects unknown code of the file dtmarks.php. The manipulation of the argument medium leads to sql injection. This vulnerability was named CVE-2024-42573. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-42782	Kashipara Music Management System 1.0 ajax.php search sql injection	A vulnerability which was classified as critical was found in Kashipara Music Management System 1.0. This affects an unknown part of the file /music/ajax.phpactionfind_music. The manipulation of the argument search leads to sql injection. This vulnerability is uniquely identified as CVE-2024-42782. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-42781	Kashipara Music Management System 1.0 Login ajax.php email sql injection	A vulnerability classified as critical has been found in Kashipara Music Management System 1.0. This affects an unknown part of the file /music/ajax.phpactionlogin of the component Login. The manipulation of the argument email leads to sql injection. This vulnerability is uniquely identified as CVE-2024-42781. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-42784	Kashipara Music Management	A vulnerability was found in Kashipara	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	System 1.0 controller.php id sql injection	Music Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /music/controller.phppageview_music. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-42784. The attack may be launched remotely. There is no exploit available.		
CVE-2024-42786	Kashipara Music Management System 1.0 View User Profile Page /music/view_user.php id sql injection	A vulnerability which was classified as critical has been found in Kashipara Music Management System 1.0. This issue affects some unknown processing of the file /music/view_user.php of the component View User Profile Page. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-42786. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-42785	Kashipara Music Management System 1.0 index.php id sql injection	A vulnerability classified as critical was found in Kashipara Music Management System 1.0. This vulnerability affects unknown code of the file /music/index.phppageview_playlist. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-42785. The attack can be initiated remotely.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		There is no exploit available.		
CVE-2024-8081	itsourcecode Payroll Management System 1.0 login.php username sql injection	A vulnerability classified as critical was found in itsourcecode Payroll Management System 1.0. Affected by this vulnerability is an unknown functionality of the file login.php. The manipulation of the argument username leads to sql injection. This vulnerability is known as CVE-2024-8081. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8139	itsourcecode E-Commerce Website 1.0 search_list.php user sql injection	A vulnerability has been found in itsourcecode E-Commerce Website 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file search_list.php. The manipulation of the argument user leads to sql injection. This vulnerability is known as CVE-2024-8139. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8147	code-projects Pharmacy Management System 1.0 index.php id sql injection	A vulnerability was found in code-projects Pharmacy Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /index.phpactioneditPharmacist. The manipulation of the argument id 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-2024-8147. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-8146	code-projects Pharmacy Management System 1.0 index.php id sql injection	A vulnerability has been found in code-projects Pharmacy Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /index.phpactioneditSalesman. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-8146. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8138	code-projects Pharmacy Management System 1.0 index.php id sql injection	A vulnerability which was classified as critical was found in code-projects Pharmacy Management System 1.0. Affected is an unknown function of the file /index.phpactioneditManager. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-8138. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8150	ContiNew Admin 3.2.0 user sort sql injection	A vulnerability was found in ContiNew Admin 3.2.0 and classified as critical. Affected by this issue is the function top.continew.starter.extension.crud.controller.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		BaseControllerpage of the file /api/system/userdeptId1&amp;page1&amp;size10. The manipulation of the argument sort leads to sql injection. This vulnerability is handled as CVE-2024-8150. The attack may be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-8155	ContiNew Admin 3.2.0 tree sort sql injection	A vulnerability classified as critical was found in ContiNew Admin 3.2.0. Affected by this vulnerability is the function top.continew.starter.extension.crud.controller.BaseControllertree of the file /api/system/dept/treesortparentId%2Casc&amp;sortsort%2Casc. The manipulation of the argument sort leads to sql injection. This vulnerability is known as CVE-2024-8155. 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

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-41354	phpipam 1.6 edit.php cross site scripting (Issue 4150)	A vulnerability was found in phpipam 1.6. It has been classified as problematic. Affected is an unknown function of the file /app/admin/widgets/edit.php. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-41354. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-41356	phpipam 1.6 zones-edit-network.php cross site scripting (Issue 4146)	A vulnerability was found in phpipam 1.6. It has been rated as problematic. Affected by this issue is some unknown functionality of the file app\admin\firewall-zones\zones-edit-network.php. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-41356. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-41374	ICEcoder 8.1 lib/settings-screen.php cross site scripting	A vulnerability which was classified as problematic was found in ICEcoder 8.1. This affects an unknown part in the library lib/settings-screen.php. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-41374. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-41375	ICEcoder 8.1	A vulnerability has	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	lib/terminal-xhr.php cross site scripting	been found in ICEcoder 8.1 and classified as problematic. This vulnerability affects unknown code in the library lib/terminal-xhr.php. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-41375. The attack can be initiated remotely. There is no exploit available.	core rule	
CVE-2024-41353	phpipam 1.6 edit-group.php cross site scripting (Issue 4147)	A vulnerability was found in phpipam 1.6 and classified as problematic. This issue affects some unknown processing of the file app\admin\groups\edit-group.php. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-41353. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-7200	SourceCodester Complaints Report Management System 1.0 ajax.php name cross site scripting	A vulnerability which was classified as problematic has been found in SourceCodester Complaints Report Management System 1.0. This issue affects some unknown processing of the file /admin/ajax.phpaction save_settings. The manipulation of the argument name leads to cross site scripting. The identification of this vulnerability is CVE-2024-7200. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-6362	Ultimate Blocks Plugin up to 3.1.x on WordPress post-grid Block Attribute cross site scripting	A vulnerability was found in Ultimate Blocks Plugin up to 3.1.x on WordPress and classified as problematic. This issue affects some unknown processing of the component post-grid Block Attribute Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-6362. 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-2024-6487	Inline Related Posts Plugin up to 3.7.x on WordPress Setting cross site scripting	A vulnerability was found in Inline Related Posts Plugin up to 3.7.x 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-2024-6487. 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-2024-4483	Email Encoder Plugin up to 2.2.1 on WordPress WP_Email_Encoder_Bundle_options[protection_text] cross site scripting	A vulnerability which was classified as problematic was found in Email Encoder Plugin up to 2.2.1 on WordPress. Affected is an unknown function. The manipulation of the argument WP_Email_Encoder_Bu	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		ndle_options[protection_text] leads to cross site scripting. This vulnerability is traded as CVE-2024-4483. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-6578	aimhubio aim up to 3.19.3 cross site scripting	A vulnerability classified as problematic has been found in aimhubio aim up to 3.19.3. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-6578. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-7225	SourceCodester Insurance Management System 1.0 Edit Insurance Policy Page update_policy pname cross site scripting	A vulnerability was found in SourceCodester Insurance Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /Script/admin/core/update_policy of the component Edit Insurance Policy Page. The manipulation of the argument pname leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-7225. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-5883	Ultimate Classified	A vulnerability has	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Listings Plugin up to 1.2 on WordPress cross site scripting	been found in Ultimate Classified Listings Plugin up to 1.2 on WordPress and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-5883. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	core rule	
CVE-2024-41640	AML Surety Eco up to 3.5 GET Request id cross site scripting	A vulnerability classified as problematic has been found in AML Surety Eco up to 3.5. Affected is an unknown function of the component GET Request Handler. The manipulation of the argument id leads to cross site scripting. This vulnerability is traded as CVE-2024-41640. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-7310	SourceCodester Record Management System 1.0 sort_user.php sort cross site scripting	A vulnerability was found in SourceCodester Record Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file sort_user.php. The manipulation of the argument sort leads to cross site scripting. This vulnerability was named CVE-2024-7310. The attack can be initiated remotely.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Furthermore there is an exploit available.		
CVE-2024-7303	itsourcecode Online Blood Bank Management System 1.0 Send Blood Request Page /request.php Address/bloodgroup cross site scripting	A vulnerability was found in itsourcecode Online Blood Bank Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /request.php of the component Send Blood Request Page. The manipulation of the argument Address/bloodgroup leads to cross site scripting. The identification of this vulnerability is CVE-2024-7303. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7321	itsourcecode Online Blood Bank Management System 1.0 User Registration signup.php user cross site scripting	A vulnerability classified as problematic was found in itsourcecode Online Blood Bank Management System 1.0. This vulnerability affects unknown code of the file signup.php of the component User Registration Handler. The manipulation of the argument user leads to cross site scripting. This vulnerability was named CVE-2024-7321. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6165	WANotifier Plugin up to 2.6.0 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic was found in WANotifier Plugin up to 2.6.0 on WordPress. Affected is an unknown function 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 traded as CVE-2024-6165. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-6272	SpiderContacts Plugin up to 1.1.7 on WordPress cross site scripting	A vulnerability has been found in SpiderContacts Plugin up to 1.1.7 on WordPress 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-2024-6272. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-6408	10Web Slider Plugin up to 1.2.56 on WordPress cross site scripting	A vulnerability was found in 10Web Slider Plugin up to 1.2.56 on WordPress 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-2024-6408. 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-2024-7343	Baidu UEditor 1.4.2 controller.php	A vulnerability was found in Baidu UEditor	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	source[] cross site scripting	1.4.2. It has been declared as problematic. This vulnerability affects unknown code of the file /ueditor142/php/controller.phpactioncatchimage. The manipulation of the argument source[] leads to cross site scripting. This vulnerability was named CVE-2024-7343. 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.		
CVE-2024-2872	WP-FeedStats socialdriver-framework Plugin 2024.0.0 on WordPress Setting cross site scripting	A vulnerability was found in WP-FeedStats socialdriver-framework Plugin 2024.0.0 on WordPress and classified as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-2872. 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-2024-1747	WooCommerce Customers Manager Plugin up to 30.1 on WordPress Metadata cross site scripting	A vulnerability has been found in WooCommerce Customers Manager Plugin up to 30.1 on WordPress and classified as problematic. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability affects unknown code of the component Metadata Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-1747. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-6529	Ultimate Classified Listings Plugin up to 1.3 on WordPress cross site scripting	A vulnerability was found in Ultimate Classified Listings Plugin up to 1.3 on WordPress. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-6529. 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-2024-4090	loating Notification Bar, Sticky Menu on Scroll, Announcement Banner, and Sticky Header for Any Plugin Setting cross site scripting	A vulnerability classified as problematic was found in loating Notification Bar Sticky Menu on Scroll Announcement Banner and Sticky Header for Any Plugin up to 2.7.1 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		known as CVE-2024-4090. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-5595	Essential Blocks Plugin up to 4.6.x on WordPress Page cross site scripting	A vulnerability was found in Essential Blocks Plugin up to 4.6.x on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Page Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-5595. 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-2024-7453	FastAdmin 1.5.0.20240328 Attachment Management Section 4 row[url]/row[imagewidth]/row[imageheight] cross site scripting	A vulnerability was found in FastAdmin 1.5.0.20240328. It has been declared as problematic. This vulnerability affects unknown code of the file /[admins_url].php/general/attachment/edit/ids/4dialog1 of the component Attachment Management Section. The manipulation of the argument row[url]/row[imagewidth]/row[imageheight] leads to cross site scripting. This vulnerability was named CVE-2024-7453. The attack can be initiated remotely.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Furthermore there is an exploit available.		
CVE-2024-6390	Quiz and Survey Master Plugin up to 9.0.x on WordPress Setting cross site scripting	A vulnerability classified as problematic has been found in Quiz and Survey Master Plugin up to 9.0.x 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-2024-6390. 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-2024-7466	PMWeb 7.2.00 Web Application Firewall cross site scripting	A vulnerability has been found in PMWeb 7.2.00 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Web Application Firewall. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-7466. 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-2024-6270	Community Events Plugin up to 1.5.0 on WordPress Setting cross site scripting	A vulnerability classified as problematic was found in Community Events Plugin up to 1.5.0 on WordPress. This vulnerability affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown code of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-6270. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-41380	microweber 2.0.16 add_tagging_tagged.php cross site scripting (Issue 1111)	A vulnerability has been found in microweber 2.0.16 and classified as problematic. This vulnerability affects unknown code of the file userfiles\modules\tags\add_tagging_tagged.php. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-41380. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-6710	Ditty Plugin up to 3.1.44 on WordPress cross site scripting	A vulnerability which was classified as problematic was found in Ditty Plugin up to 3.1.44 on WordPress. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-6710. 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-41381	microweber 2.0.16 admin.php cross site scripting (Issue 1110)	A vulnerability which was classified as problematic was found in microweber 2.0.16. This affects an unknown part of the file userfiles\modules\settings\admin.php. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-41381. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-6498	Collect.chat Chatbot Plugin up to 2.4.3 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic has been found in Collect.chat Chatbot Plugin up to 2.4.3 on WordPress. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-6498. 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-2024-3636	Pinpoint Booking System Plugin 2.9.9.2.9 on WordPress Setting cross site scripting	A vulnerability classified as problematic has been found in Pinpoint Booking System Plugin 2.9.9.2.9 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	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2024-3636. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-6766	WP-FeedStats shortcodes-ultimate-pro Plugin up to 7.2.0 on WordPress Shortcode Attribute cross site scripting	A vulnerability which was classified as problematic was found in WP-FeedStats shortcodes-ultimate-pro Plugin up to 7.2.0 on WordPress. This affects an unknown part of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-6766. 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-2024-7084	Ernest Marcinko Ajax Search Lite Plugin up to 4.12.0 on WordPress cross site scripting	A vulnerability was found in Ernest Marcinko Ajax Search Lite Plugin up to 4.12.0 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-2024-7084. 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-2024-6651	File Upload Plugin up to 4.24.7 on	A vulnerability which was classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	WordPress cross site scripting	problematic has been found in File Upload Plugin up to 4.24.7 on WordPress. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-6651. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-28740	Koha ILS up to 23.05 additonal-contents.pl cross site scripting	A vulnerability has been found in Koha ILS up to 23.05 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file additonal-contents.pl. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-28740. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-40819	ID4Portais prior 2022.837.002a Message Parameter cross site scripting	A vulnerability classified as problematic was found in ID4Portais. Affected by this vulnerability is an unknown functionality of the component Message Parameter Handler. The manipulation leads to basic cross site scripting. This vulnerability is known as CVE-2023-40819. 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
		It is recommended to upgrade the affected component.		
CVE-2024-7082	Easy Table of Contents Plugin up to 2.0.67 on WordPress cross site scripting	A vulnerability has been found in Easy Table of Contents Plugin up to 2.0.67 on WordPress and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-7082. 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-2024-41333	Phpgurukul Tourism Management System 2.0 uname cross site scripting (ID 179891)	A vulnerability classified as problematic was found in Phpgurukul Tourism Management System 2.0. This vulnerability affects unknown code. The manipulation of the argument uname leads to cross site scripting. This vulnerability was named CVE-2024-41333. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-41239	Kashipara Responsive School Management System 1.0 add_class_submit.php class_name cross site scripting	A vulnerability has been found in Kashipara Responsive School Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /smsa/add_class_submit.php. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument class_name leads to cross site scripting. This vulnerability was named CVE-2024-41239. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-41242	Kashipara Responsive School Management System 3.2.0 /smsa/student_login.php error cross site scripting	A vulnerability was found in Kashipara Responsive School Management System 3.2.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /smsa/student_login.php. The manipulation of the argument error leads to cross site scripting. This vulnerability is known as CVE-2024-41242. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-41240	Kashipara Responsive School Management System 3.2.0 /smsa/teacher_login.php error cross site scripting	A vulnerability was found in Kashipara Responsive School Management System 3.2.0. It has been classified as problematic. Affected is an unknown function of the file /smsa/teacher_login.php. The manipulation of the argument error leads to cross site scripting. This vulnerability is traded as CVE-2024-41240. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-41241	Kashipara Responsive School Management	A vulnerability was found in Kashipara Responsive School	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	System 3.2.0 /smsa/admin_login.php error cross site scripting	Management System 3.2.0 and classified as problematic. This issue affects some unknown processing of the file /smsa/admin_login.php. The manipulation of the argument error leads to cross site scripting. The identification of this vulnerability is CVE-2024-41241. The attack may be initiated remotely. There is no exploit available.		
CVE-2024-3973	House Manager Plugin up to 1.0.8.4 on WordPress cross site scripting	A vulnerability has been found in House Manager Plugin up to 1.0.8.4 on WordPress and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-3973. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-6494	File Upload Plugin up to 4.24.7 on WordPress cross site scripting	A vulnerability was found in File Upload Plugin up to 4.24.7 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-2024-6494. 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-2024-6884	Kadence Gutenberg	A vulnerability was	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Blocks with AI Plugin up to 3.2.38 on WordPress Post cross site scripting	found in Kadence Gutenberg Blocks with AI Plugin up to 3.2.38 on WordPress and classified as problematic. This issue affects some unknown processing of the component Post Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-6884. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	core rule	
CVE-2024-6706	Open WebUI 0.1.105 cross site scripting	A vulnerability was found in Open WebUI 0.1.105. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-6706. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-6481	Search & Filter Pro Plugin up to 2.5.17 on WordPress Setting cross site scripting	A vulnerability has been found in Search & Filter Pro Plugin up to 2.5.17 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-2024-6481. The attack can be initiated 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-2024-6158	Category Posts Widget Plugin up to 4.9.16 on WordPress Category Posts Widget Setting cross site scripting	A vulnerability was found in Category Posts Widget Plugin up to 4.9.16 on WordPress and classified as problematic. This issue affects some unknown processing of the component Category Posts Widget Setting Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-6158. 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-2024-6136	WP-FeedStats wp-cart-for-digital-products Plugin up to 8.5.5 on WordPress cross site scripting	A vulnerability has been found in WP-FeedStats wp-cart-for-digital-products Plugin up to 8.5.5 on WordPress and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-6136. 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-2024-6133	WP-FeedStats wp-cart-for-digital-products Plugin up to 8.5.5 on	A vulnerability which was classified as problematic was found in WP-FeedStats wp-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	WordPress cross site scripting	cart-for-digital-products Plugin up to 8.5.5 on WordPress. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-6133. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-6134	WP-FeedStats wp-cart-for-digital-products Plugin up to 8.5.5 on WordPress cross site scripting	A vulnerability was found in WP-FeedStats wp-cart-for-digital-products Plugin up to 8.5.5 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-2024-6134. 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-2024-40500	Martin Kucej i-librarian up to 5.11.0 Import search cross site scripting	A vulnerability classified as problematic was found in Martin Kucej i-librarian up to 5.11.0. This vulnerability affects the function search of the component Import. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-40500. The attack can be initiated remotely.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		There is no exploit available.		
CVE-2024-41613	Symphony CMS 2.7.10 Note cross site scripting	A vulnerability was found in Symphony CMS 2.7.10. It has been rated as problematic. This issue affects some unknown processing of the component Note Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-41613. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-41614	Symphony CMS up to 2.7.10 Comment Component cross site scripting	A vulnerability classified as problematic has been found in Symphony CMS up to 2.7.10. Affected is an unknown function of the component Comment Component. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-41614. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-7790	DevikaAI cross site scripting	A vulnerability has been found in DevikaAI and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-7790. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-7812	SourceCodester Best House Rental Management System 1.0 POST	A vulnerability classified as problematic was found in SourceCodester Best	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Parameter ajax.php lastname cross site scripting	House Rental Management System 1.0. This vulnerability affects unknown code of the file /rental_0/rental/ajax.phpactionsave_tenant of the component POST Parameter Handler. The manipulation of the argument lastname leads to cross site scripting. This vulnerability was named CVE-2024-7812. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-7815	CodeAstro Online Railway Reservation System 1.0 Update Employee Page admin-update-employee.php emp_fname /emp_lname /emp_nat_idno/emp_addr cross site scripting	A vulnerability has been found in CodeAstro Online Railway Reservation System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/admin-update-employee.php of the component Update Employee Page. The manipulation of the argument emp_fname /emp_lname /emp_nat_idno/emp_addr leads to cross site scripting. This vulnerability is known as CVE-2024-7815. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7793	SourceCodester Task Progress Tracker 1.0 /endpoint/add-task.php task_name cross site scripting	A vulnerability was found in SourceCodester Task Progress Tracker 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /endpoint/add-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		task.php. The manipulation of the argument task_name leads to cross site scripting. This vulnerability is known as CVE-2024-7793. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2024-7814	CodeAstro Online Railway Reservation System 1.0 Add Employee Page admin-add-employee.php emp_fname /emp_lname /emp_nat_idno/emp_addr cross site scripting	A vulnerability which was classified as problematic was found in CodeAstro Online Railway Reservation System 1.0. Affected is an unknown function of the file /admin/admin-add-employee.php of the component Add Employee Page. The manipulation of the argument emp_fname /emp_lname /emp_nat_idno/emp_addr leads to cross site scripting. This vulnerability is traded as CVE-2024-7814. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7852	SourceCodester Yoga Class Registration System 1.0 view_inquiry.php message cross site scripting	A vulnerability was found in SourceCodester Yoga Class Registration System 1.0 and classified as problematic. This issue affects some unknown processing of the file /admin/inquiries/view_inquiry.php. The manipulation of the argument message leads to cross site scripting. The identification of this vulnerability is CVE-2024-7852. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-6533	Directus 10.13.0 cross site scripting	A vulnerability classified as problematic has been found in Directus 10.13.0. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-6533. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-42678	Super Easy Enterprise Management System up to 1.0.0 /WebSet/DlgGridSet.html cross site scripting	A vulnerability which was classified as problematic has been found in Super Easy Enterprise Management System up to 1.0.0. Affected by this issue is some unknown functionality of the file /WebSet/DlgGridSet.html. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-42678. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-7900	xiaohe4966 TpMeCMS 1.3.3.2 Basic Configuration config cross site scripting	A vulnerability which was classified as problematic was found in xiaohe4966 TpMeCMS 1.3.3.2. Affected is an unknown function of the file /h.php/general/configrefaddtabs of the component Basic Configuration Handler. The manipulation of the argument Site Name/Beian/Contact address/copyright/technical support 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-2024-7900. It is possible to launch the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-7916	nafisulbari/itsourcecode Insurance Management System 1.0 Add Nominee Page addNominee.php Nominee-Client ID cross site scripting	A vulnerability classified as problematic was found in nafisulbari/itsourcecode Insurance Management System 1.0. Affected by this vulnerability is an unknown functionality of the file addNominee.php of the component Add Nominee Page. The manipulation of the argument Nominee-Client ID leads to cross site scripting. This vulnerability is known as CVE-2024-7916. 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-2024-23729	ColorOS Internet Browser 45.10.3.4.1 on Android com.android.browser.RealBrowserActivity cross site scripting	A vulnerability classified as problematic was found in ColorOS Internet Browser 45.10.3.4.1 on Android. This vulnerability affects unknown code of the component com.android.browser.RealBrowserActivity. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation leads to cross site scripting. This vulnerability was named CVE-2024-23729. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-6843	Chatbot with ChatGPT Plugin up to 2.4.4 on WordPress cross site scripting	A vulnerability which was classified as problematic has been found in Chatbot with ChatGPT Plugin up to 2.4.4 on WordPress. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-6843. 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-2024-7945	itsourcecode Laravel Property Management System 1.0 Notes Page /admin/notes/create Note text cross site scripting	A vulnerability was found in itsourcecode Laravel Property Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/notes/create of the component Notes Page. The manipulation of the argument Note text leads to cross site scripting. This vulnerability is known as CVE-2024-7945. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-39094	Friendica 2024.03 Setting homepage/xmpp/m	A vulnerability which was classified as problematic has been	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	atrix cross site scripting	found in Friendica 2024.03. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation of the argument homepage/xmpp/matrix leads to cross site scripting. This vulnerability is handled as CVE-2024-39094. The attack may be launched remotely. There is no exploit available.		
CVE-2024-35540	Typecho 1.3.0 cross site scripting	A vulnerability was found in Typecho 1.3.0. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-35540. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-0926	Custom Permalinks Plugin up to 2.6.0 on WordPress cross site scripting	A vulnerability was found in Custom Permalinks Plugin up to 2.6.0 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-0926. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-42852	AcuToWeb Server 10.5.0.7577C8b index.php cross site scripting	A vulnerability was found in AcuToWeb Server 10.5.0.7577C8b and classified as problematic. This issue affects some unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		processing of the file index.php. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-42852. The attack may be initiated remotely. There is no exploit available.		
CVE-2024-42918	itsourcecode Online Accreditation Management System controller.php cross site scripting	A vulnerability which was classified as problematic has been found in itsourcecode Online Accreditation Management System. Affected by this issue is some unknown functionality of the file controller.php. The manipulation of the argument SCHOOLNAME/EMAILADDRES/CONTACTNO/COMPANYNAME/COMPANYCONTACTNO leads to cross site scripting. This vulnerability is handled as CVE-2024-42918. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-6715	Ditty Plugin up to 3.1.45 on WordPress cross site scripting	A vulnerability was found in Ditty Plugin up to 3.1.45 on WordPress. 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-2024-6715. 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

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-3282	WP Table Builder Plugin up to 1.5.0 on WordPress cross site scripting	A vulnerability was found in WP Table Builder Plugin up to 1.5.0 on WordPress 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-2024-3282. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40111	flat file CMS 2.0.0-alpha.4 Template Body cross site scripting	A vulnerability was found in flat file CMS 2.0.0-alpha.4 and classified as problematic. This issue affects some unknown processing of the component Template Body Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-40111. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-8144	ClassCMS 4.8 Logo /index.php/admin cross site scripting	A vulnerability classified as problematic was found in ClassCMS 4.8. Affected by this vulnerability is an unknown functionality of the file /index.php/admin of the component Logo Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-8144. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8153	SourceCodester QR	A vulnerability was	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Code Bookmark System 1.0 delete-bookmark.php bookmark cross site scripting	found in SourceCodester QR Code Bookmark System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /endpoint/delete-bookmark.php. The manipulation of the argument bookmark leads to cross site scripting. The identification of this vulnerability is CVE-2024-8153. The attack may be initiated remotely. Furthermore there is an exploit available.	core rule	
CVE-2024-8154	SourceCodester QR Code Bookmark System 1.0 Parameter update-bookmark.php tbl_bookmark_id/name/url cross site scripting	A vulnerability classified as problematic has been found in SourceCodester QR Code Bookmark System 1.0. Affected is an unknown function of the file /endpoint/update-bookmark.php of the component Parameter Handler. The manipulation of the argument tbl_bookmark_id/name/url leads to cross site scripting. This vulnerability is traded as CVE-2024-8154. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-8152	SourceCodester QR Code Bookmark System 1.0 Parameter add-bookmark.php name/url cross site scripting	A vulnerability was found in SourceCodester QR Code Bookmark System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		file /endpoint/add-bookmark.php of the component Parameter Handler. The manipulation of the argument name/url leads to cross site scripting. This vulnerability was named CVE-2024-8152. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-8151	SourceCodester Interactive Map with Marker 1.0 delete-mark.php mark cross site scripting	A vulnerability was found in SourceCodester Interactive Map with Marker 1.0. It has been classified as problematic. This affects an unknown part of the file /endpoint/delete-mark.php. The manipulation of the argument mark leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-8151. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y

XML External Entity Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-6893	Journyx jtime 11.5.4 API soap_cgi.pyc xml external entity reference	A vulnerability classified as critical has been found in Journyx jtime 11.5.4. This affects an unknown part of the file soap_cgi.pyc of the component API Handler. The manipulation leads to xml external entity reference. This vulnerability is uniquely identified as CVE-2024-6893. The attack can only be initiated within the local network. There is no exploit available.	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.

Gartner
Peer Insights
Customers’
Choice 2024 ™

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™

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