INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

May 2024

The total **zero-day vulnerabilities** count for May month: 169

Command Injection	CSRF	Local File Inclusion	SQLi	Malicious File Upload	Cross-site Scripting
12	14	13	50	9	71

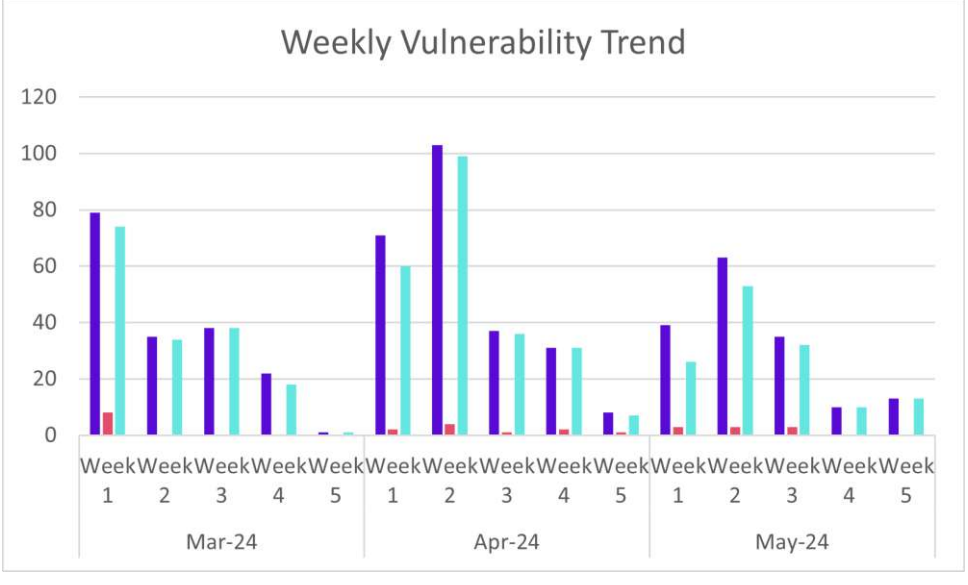
Zero-day vulnerabilities protected through core rules	160
Zero-day vulnerabilities protected through custom rules	9
Zero-day vulnerabilities for which protection cannot be done	0
Zero-day vulnerabilities found by Indusface WAS	134

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

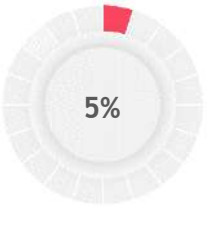
Vulnerability Trend:

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

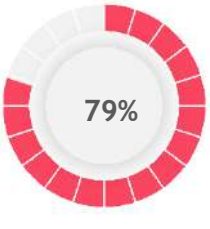
Weekly Vulnerability Trend



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

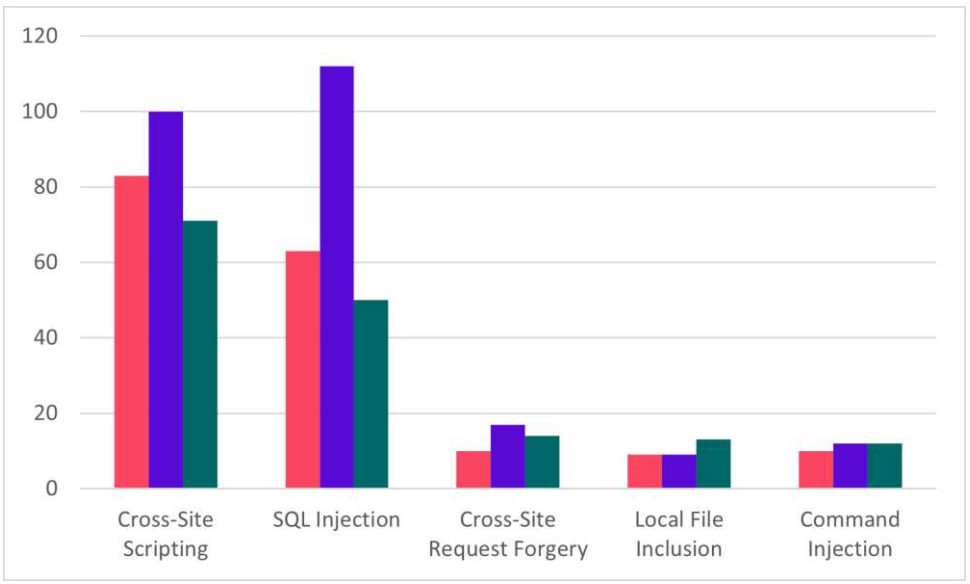


of the zero-day vulnerabilities were protected by the custom rules in the last month



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

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-32884	Byron gitoxide up to 0.34.x/0.41.x/0.61.x Username command injection (GHSA-98p4-xjmm-8mfh)	A vulnerability was found in Byron gitoxide up to 0.34.x/0.41.x/0.61.x. It has been rated as critical. Affected by this issue is some unknown functionality of the component Username Handler. The manipulation leads to command injection. This vulnerability is handled as CVE-2024-32884. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	N
CVE-2024-3191	MailCleaner up to 2023.03.14 Email os command injection (MZ-24-01)	A vulnerability which was classified as critical has been found in MailCleaner up to 2023.03.14. This issue affects some unknown processing of the component Email Handler. The manipulation leads to os command injection. The identification of this vulnerability is CVE-2024-3191. The attack may be initiated remotely. Furthermore there is an exploit	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		available. It is recommended to apply a patch to fix this issue.		
CVE-2024-3193	MailCleaner up to 2023.03.14 Admin Endpoints os command injection (MZ-24-01)	A vulnerability has been found in MailCleaner up to 2023.03.14 and classified as critical. Affected by this vulnerability is an unknown functionality of the component Admin Endpoints. The manipulation leads to os command injection. This vulnerability is known as CVE-2024-3193. The attack can be launched remotely. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue.	Patched by core rule	N
CVE-2024-3196	MailCleaner up to 2023.03.14 SOAP Service os command injection (MZ-24-01)	A vulnerability was found in MailCleaner up to 2023.03.14. It has been declared as critical. This vulnerability affects the function getStats/Services_silentDump/Services_stopStartMTA/Config_saveDateTime/Config_hostid/Logs_StartGetStat/dump Configuration of the component SOAP Service. The manipulation leads to os command injection. This vulnerability was named CVE-2024-3196. Local access is required to approach this attack. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue.	Patched by core rule	N
CVE-2024-33792	Netis MEX605 2.00.06 Tracert Page cross site scripting	A vulnerability which was classified as problematic was found in Netis MEX605 2.00.06. Affected is an unknown function of the component Tracert Page. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-33792. 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-2024-33789	Linksys E5600 1.1.0.26 /API/info ipurl command injection	A vulnerability classified as critical was found in Linksys E5600 1.1.0.26. This vulnerability affects unknown code of the file /API/info. The manipulation of the argument ipurl leads to command injection. This vulnerability was named CVE-2024-33789. Access to the local network is required for this attack. There is no exploit available.	Patched by core rule	N
CVE-2024-33793	Netis MEX605 2.00.06 Ping Test Page cross site scripting	A vulnerability was found in Netis MEX605 2.00.06 and classified as problematic. Affected by this issue is some unknown functionality of the component Ping Test Page. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-33793. The attack may be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-4507	Ruijie RG-UAC up to 20240428 static_route_add_ipv6.php text_prefixlen/text_gateway/devname os command injection	A vulnerability was found in Ruijie RG-UAC up to 20240428 and classified as critical. This issue affects some unknown processing of the file /view/IPV6/ipv6StaticRoute/static_route_add_ipv6.php. The manipulation of the argument text_prefixlen/text_gateway/devname leads to os command injection. The identification of this vulnerability is CVE-2024-4507. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	N
CVE-2024-2913	mintplex-labs	A vulnerability was	Patched by	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	anything-llm User Invite toctou	found in mintplex-labs anything-llm and classified as problematic. Affected by this issue is some unknown functionality of the component User Invite Handler. The manipulation leads to time-of-check time-of-use. This vulnerability is handled as CVE-2024-2913. The attack may be launched remotely. There is no exploit available.	core rule	
CVE-2024-34352	1Panel up to v1.10.2-lts command injection	A vulnerability which was classified as critical has been found in 1Panel up to v1.10.2-lts. This issue affects some unknown processing. The manipulation leads to command injection. The identification of this vulnerability is CVE-2024-34352. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	N
CVE-2024-4809	SourceCodester Open Source Clinic Management System 1.0 setting.php logo unrestricted upload	A vulnerability has been found in SourceCodester Open Source Clinic Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file setting.php. The manipulation of the argument logo leads to unrestricted upload. This vulnerability is known as CVE-2024-4809. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	N
CVE-2024-34697	freescout-helpdesk freescout up to 1.8.138 cross site scripting	A vulnerability was found in freescout-helpdesk freescout up to 1.8.138. It has been classified as problematic. This affects an unknown part. The manipulation leads to basic cross site scripting.	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is uniquely identified as CVE-2024-34697. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-3481	Counter Box Plugin up to 1.2.3 on WordPress cross-site request forgery	A vulnerability was found in Counter Box Plugin up to 1.2.3 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-2024-3481. 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-2024-2405	Float Menu Plugin up to 6.0.0 on WordPress cross-site request forgery	A vulnerability was found in Float Menu Plugin up to 6.0.0 on WordPress. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-2405. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	N
CVE-2024-3476	Side Menu Lite Plugin up to 4.2.0 on WordPress cross-site request forgery	A vulnerability has been found in Side Menu Lite Plugin up to 4.2.0 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2024-3476. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	N
CVE-2024-3471	Button Generator Plugin up to 2.x on WordPress cross-site request forgery	A vulnerability classified as problematic has been found in Button Generator Plugin up to 2.x on WordPress. This	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2024-3471. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-3477	Popup Box Plugin up to 2.2.6 on WordPress cross-site request forgery	A vulnerability was found in Popup Box Plugin up to 2.2.6 on WordPress and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2024-3477. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	N
CVE-2024-3474	Wow Skype Buttons Plugin up to 4.0.3 on WordPress cross-site request forgery	A vulnerability which was classified as problematic has been found in Wow Skype Buttons Plugin up to 4.0.3 on WordPress. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-3474. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	N
CVE-2024-3478	Herd Effects Plugin up to 5.2.6 on WordPress cross-site request forgery	A vulnerability was found in Herd Effects Plugin up to 5.2.6 on WordPress. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		uniquely identified as CVE-2024-3478. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-3472	Modal Window Plugin up to 5.3.9 on WordPress cross-site request forgery	A vulnerability classified as problematic was found in Modal Window Plugin up to 5.3.9 on WordPress. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2024-3472. 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-2024-3475	Sticky Buttons Plugin up to 3.2.3 on WordPress cross-site request forgery	A vulnerability which was classified as problematic was found in Sticky Buttons Plugin up to 3.2.3 on WordPress. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-3475. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	N
CVE-2024-1230	SimpleShop Plugin up to 2.10.0 on WordPress cross-site request forgery	A vulnerability was found in SimpleShop Plugin up to 2.10.0 on WordPress. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2024-1230. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-4592	DedeCMS 5.7 sys_group_edit.php cross-site request	A vulnerability classified as problematic was found in DedeCMS 5.7.	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	forgery	This vulnerability affects unknown code of the file /src/dede/sys_group_edit.php. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2024-4592. 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-2024-4594	DedeCMS 5.7 /src/dede/sys_safe.php cross-site request forgery	A vulnerability which was classified as problematic was found in DedeCMS 5.7. Affected is an unknown function of the file /src/dede/sys_safe.php. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-4594. It is possible to launch the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	N
CVE-2024-34351	vercel next.js up to 14.1.0 server-side request forgery	A vulnerability was found in vercel next.js up to 14.1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to server-side request forgery. This vulnerability is known as CVE-2024-34351. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	N
CVE-2024-3940	reCAPTCHA Jetpack Plugin up to 0.2.2 on WordPress Setting cross-site request forgery	A vulnerability was found in reCAPTCHA Jetpack Plugin up to 0.2.2 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2024-3940. The attack can be launched remotely. There is no exploit available.		

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-33350	taoCMS 3.0.2 include/model/file.php path traversal	A vulnerability was found in taoCMS 3.0.2. It has been rated as critical. Affected by this issue is some unknown functionality of the file include/model/file.php. The manipulation leads to path traversal. This vulnerability is handled as CVE-2024-33350. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-3195	MailCleaner up to 2023.03.14 Admin Endpoints path traversal (MZ-24-01)	A vulnerability was found in MailCleaner up to 2023.03.14. It has been classified as critical. This affects an unknown part of the component Admin Endpoints. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2024-3195. It is possible to initiate the attack remotely. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y
CVE-2024-30851	codesiddhant Jasmin Ransomware 1.0.1 download_file.php path traversal	A vulnerability classified as problematic has been found in codesiddhant Jasmin Ransomware 1.0.1. This affects an unknown part of the file download_file.php. The manipulation leads to path traversal. This vulnerability is uniquely identified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2024-30851. The attack needs to be initiated within the local network. There is no exploit available.		
CVE-2024-32982	litestar up to 1.51.14/2.8.2 base.py path traversal (GHSA-83pv-qr33-2vcf)	A vulnerability classified as critical has been found in litestar up to 1.51.14/2.8.2. This affects an unknown part of the file litestar/static_files/base.py. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2024-32982. 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-2024-34471	HSC Mailinspector 5.2.17-3 mliRealtimeEmails.php filename path traversal	A vulnerability was found in HSC Mailinspector 5.2.17-3. It has been classified as critical. Affected is an unknown function of the file mliRealtimeEmails.php. The manipulation of the argument filename leads to path traversal. This vulnerability is traded as CVE-2024-34471. The attack can only be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-34315	CmsEasy 7.7.7.9 template_admin.php file_get_contents file inclusion	A vulnerability has been found in CmsEasy 7.7.7.9 and classified as problematic. This vulnerability affects the function file_get_contents of the file /admin/template_ad	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		min.php. The manipulation leads to file inclusion. This vulnerability was named CVE-2024-34315. The attack can only be initiated within the local network. There is no exploit available.		
CVE-2024-1076	SSL Zen Plugin up to 4.5.x on WordPress access control	A vulnerability has been found in SSL Zen Plugin up to 4.5.x on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to improper access controls. This vulnerability is known as CVE-2024-1076. 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-2024-34245	DedeCMS 5.7.114 makehtml_js_action.php path traversal	A vulnerability which was classified as problematic has been found in DedeCMS 5.7.114. This issue affects some unknown processing of the file makehtml_js_action.php. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2024-34245. The attack can only be done within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2023-40297	Stakater Forecastle up to 1.0.139 Website path traversal	A vulnerability was found in Stakater Forecastle up to 1.0.139. It has been rated as critical. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		issue affects some unknown processing of the component Website. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2023-40297. The attack can only be done within the local network. There is no exploit available.		
CVE-2024-4322	parisneo lollms-webui /list_personalities category path traversal	A vulnerability was found in parisneo lollms-webui. It has been declared as problematic. This vulnerability affects the function list_personalities of the file /list_personalities. The manipulation of the argument category leads to path traversal: &039;\..\filename&039;. This vulnerability was named CVE-2024-4322. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-3403	imartinez privategpt 0.2.0 File Upload path traversal	A vulnerability which was classified as critical has been found in imartinez privategpt 0.2.0. This issue affects some unknown processing of the component File Upload. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2024-3403. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-34193	smanga 3.2.7 file path traversal	A vulnerability was found in smanga 3.2.7. It has been	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		classified as problematic. This affects an unknown part. The manipulation of the argument file leads to path traversal. This vulnerability is uniquely identified as CVE-2024-34193. Access to the local network is required for this attack to succeed. There is no exploit available.		
CVE-2024-4388	cas Plugin up to 1.0.0 on WordPress path traversal	A vulnerability was found in cas Plugin up to 1.0.0 on WordPress and classified as critical. Affected by this issue is some unknown functionality. The manipulation leads to path traversal. This vulnerability is handled as CVE-2024-4388. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-33438	CubeCart up to 6.5.4 Phar File unrestricted upload	A vulnerability which was classified as critical was found in CubeCart up to 6.5.4. Affected is an unknown function of the component Phar File Handler. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2024-33438. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by custom rule	N
CVE-2024-4349	SourceCodester Pisay Online E-Learning System 1.0 /lesson/controller.php file unrestricted upload	A vulnerability has been found in SourceCodester Pisay Online E-Learning System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /lesson/controller.php. The manipulation of the argument file leads to unrestricted upload. This vulnerability is known as CVE-2024-4349. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by custom rule	N
CVE-2024-33103	DokuWiki 2024-02-06a Media Manager unrestricted upload (Issue 4267)	A vulnerability was found in DokuWiki 2024-02-06a. It has been classified as critical. Affected is an unknown function of the component Media Manager. The manipulation leads to unrestricted upload. This vulnerability is	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		traded as CVE-2024-33103. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2024-33786	Zhongcheng Kexin Ticketing Management Platform 20.04 File unrestricted upload	A vulnerability which was classified as critical was found in Zhongcheng Kexin Ticketing Management Platform 20.04. This affects an unknown part of the component File Handler. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2024-33786. It is possible to initiate the attack remotely. There is no exploit available.	Patched by custom rule	N
CVE-2024-4500	SourceCodester Prison Management System 1.0 /Employee/edit-photo.php userImage unrestricted upload	A vulnerability was found in SourceCodester Prison Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /Employee/edit-photo.php. The manipulation of the argument userImage leads to unrestricted upload. This vulnerability was named CVE-2024-4500. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by custom rule	N
CVE-2024-33294	SourceCodester Library System 1.0 student_edit_photo.php photo unrestricted upload	A vulnerability has been found in SourceCodester Library System 1.0 and classified as critical. This vulnerability affects unknown code of the file student_edit_photo.php. The manipulation	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the argument photo leads to unrestricted upload. This vulnerability was named CVE-2024-33294. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-34909	KYKMS up to 1.0.1 PDF File unrestricted upload	A vulnerability was found in KYKMS up to 1.0.1 and classified as critical. Affected by this issue is some unknown functionality of the component PDF File Handler. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2024-34909. The attack may be launched remotely. There is no exploit available.	Patched by custom rule	N
CVE-2024-34913	r-pan-scaffolding up to 5.0 PDF File unrestricted upload	A vulnerability was found in r-pan-scaffolding up to 5.0. It has been classified as critical. This affects an unknown part of the component PDF File Handler. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2024-34913. It is possible to initiate the attack remotely. There is no exploit available.	Patched by custom rule	N
CVE-2024-34906	dootask 0.30.13 PDF File unrestricted upload	A vulnerability has been found in dootask 0.30.13 and classified as critical. Affected by this vulnerability is an unknown functionality of the component PDF File Handler. The manipulation leads to unrestricted upload.	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is known as CVE-2024-34906. 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-2024-4257	BlueNet Technology Clinical Browsing System 1.2.1 /xds/deleteStudy.php documentUniqueId sql injection	A vulnerability was found in BlueNet Technology Clinical Browsing System 1.2.1. It has been classified as critical. This affects an unknown part of the file /xds/deleteStudy.php. The manipulation of the argument documentUniqueId leads to sql injection. This vulnerability is uniquely identified as CVE-2024-4257. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-33444	onethink 1.1 ModelModel.class.php sql injection (Issue 39)	A vulnerability was found in onethink 1.1. It has been rated as critical. Affected by this issue is some unknown functionality of the file ModelModel.class.php. The manipulation leads to sql injection. This vulnerability is handled as CVE-2024-33444. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-31821	SQL Ecommerce-CodeIgniter-Bootstrap Orders_model.php manageQuantitiesAndProcurement sql injection	A vulnerability which was classified as critical was found in SQL Ecommerce-CodeIgniter-Bootstrap. This affects the function manageQuantitiesAndProcurement of the file Orders_model.php. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2024-31821. 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. It is recommended to apply a patch to fix this issue.		
CVE-2024-29320	Wallos up to 1.15.2 /subscriptions/get.php category/payment sql injection	A vulnerability was found in Wallos up to 1.15.2 and classified as critical. Affected by this issue is some unknown functionality of the file /subscriptions/get.php. The manipulation of the argument category/payment leads to sql injection. This vulnerability is handled as CVE-2024-29320. 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-2024-33332	SpringBlade 3.7.1 GET Request api/blade-system/tenant information disclosure	A vulnerability was found in SpringBlade 3.7.1. It has been classified as problematic. Affected is an unknown function of the file api/blade-system/tenant of the component GET Request Handler. The manipulation leads to information disclosure. This vulnerability is traded as CVE-2024-33332. The attack can only be done within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-31673	Kliqqi CMS 2.0.2 load_data.php userid sql injection	A vulnerability was found in Kliqqi CMS 2.0.2. It has been rated as critical. This issue affects some unknown processing of the file load_data.php. The manipulation of the argument userid leads to sql injection.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The identification of this vulnerability is CVE-2024-31673. The attack may be initiated remotely. There is no exploit available.		
CVE-2024-33787	Hengan Weighing Management Information Query Platform 2019-2021 53.25 search_user.aspx tuser_Number sql injection	A vulnerability which was classified as critical has been found in Hengan Weighing Management Information Query Platform 2019-2021 53.25. Affected by this issue is some unknown functionality of the file search_user.aspx. The manipulation of the argument tuser_Number leads to sql injection. This vulnerability is handled as CVE-2024-33787. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-34533	izi_data up to 17.0.2 query_execute sql injection	A vulnerability was found in izi_data up to 17.0.2 and classified as critical. Affected by this issue is the function IZITools::query_check/IZITools::query_fetch/IZITools::query_execute. The manipulation leads to sql injection. This vulnerability is handled as CVE-2024-34533. 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-2024-34532	Yvan Dotet PostgreSQL Query Deluxe module up to 17.0.0.3 models/querydeluxe.py get_result_from_qu	A vulnerability has been found in Yvan Dotet PostgreSQL Query Deluxe module up to 17.0.0.3 and classified as critical. Affected by this	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	ery sql injection	vulnerability is the function QueryDeluxe::get_result_from_query of the file models/querydeluxe.py. The manipulation of the argument query leads to sql injection. This vulnerability is known as CVE-2024-34532. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-34534	Cybrosys Text Commander Module up to 16.0.1 models/ir_model.py IrModel::chech_model data sql injection	A vulnerability was found in Cybrosys Text Commander Module up to 16.0.1. It has been classified as critical. This affects the function IrModel::chech_model of the file models/ir_model.py. The manipulation of the argument data leads to sql injection. This vulnerability is uniquely identified as CVE-2024-34534. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-33121	Roothub 2.6 searchs sql injection	A vulnerability classified as critical was found in Roothub 2.6. This vulnerability affects the function search. The manipulation of the argument s leads to sql injection. This vulnerability was named CVE-2024-33121. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-33403	Campcodes	A vulnerability was	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Complete Web-Based School Management System 1.0 /model/get_events.php event_id sql injection	found in Campcodes Complete Web-Based School Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /model/get_events.php. The manipulation of the argument event_id leads to sql injection. This vulnerability is handled as CVE-2024-33403. The attack may be launched remotely. Furthermore there is an exploit available.	core rule	
CVE-2024-33410	Campcodes Complete Web-Based School Management System 1.0 delete_range_grade.php id sql injection	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /model/delete_range_grade.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-33410. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-33405	Campcodes Complete Web-Based School Management System 1.0 add_friends.php friend_index sql injection	A vulnerability has been found in Campcodes Complete Web-Based School Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file add_friends.php. The manipulation of the argument friend_index 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
		33405. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2024-33407	Campcodes Complete Web-Based School Management System 1.0 /model/delete_record.php id sql injection	A vulnerability classified as critical was found in Campcodes Complete Web-Based School Management System 1.0. This vulnerability affects unknown code of the file /model/delete_record.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-33407. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-33406	Campcodes Complete Web-Based School Management System 1.0 delete_student_grade_subject.php index sql injection	A vulnerability classified as critical has been found in Campcodes Complete Web-Based School Management System 1.0. This affects an unknown part of the file /model/delete_student_grade_subject.php. The manipulation of the argument index leads to sql injection. This vulnerability is uniquely identified as CVE-2024-33406. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-33408	Campcodes Complete Web-Based School Management System 1.0 /model/get_classroom.php id sql injection	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /model/get_classroom.php. The manipulation	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-33408. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-33409	Campcodes Complete Web-Based School Management System 1.0 index.php name sql injection	A vulnerability which was classified as critical has been found in Campcodes Complete Web-Based School Management System 1.0. This issue affects some unknown processing of the file index.php. The manipulation of the argument name leads to sql injection. The identification of this vulnerability is CVE-2024-33409. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-33411	Campcodes Complete Web-Based School Management System 1.0 get_admin_profile.php my_index sql injection	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /model/get_admin_profile.php. The manipulation of the argument my_index leads to sql injection. This vulnerability is known as CVE-2024-33411. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-33404	Campcodes Complete Web-Based School Management	A vulnerability which was classified as critical was found in Campcodes Complete	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	System 1.0 add_student_first_payment.php index sql injection	Web-Based School Management System 1.0. Affected is an unknown function of the file /model/add_student_first_payment.php. The manipulation of the argument index leads to sql injection. This vulnerability is traded as CVE-2024-33404. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2024-33164	J2EEFAST 2.7.0 authUserList sql_filter sql injection	A vulnerability has been found in J2EEFAST 2.7.0 and classified as critical. Affected by this vulnerability is the function authUserList. The manipulation of the argument sql_filter leads to sql injection. This vulnerability is known as CVE-2024-33164. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-4595	SEMCMS up to 4.8 function.php locate sql injection	A vulnerability has been found in SEMCMS up to 4.8 and classified as critical. Affected by this vulnerability is the function locate of the file function.php. The manipulation leads to sql injection. This vulnerability is known as CVE-2024-4595. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-33147	J2EEFAST 2.7.0 authRoleList sql_filter sql injection	A vulnerability has been found in J2EEFAST 2.7.0 and classified as critical. This vulnerability affects the function authRoleList. The manipulation of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the argument sql_filter leads to sql injection. This vulnerability was named CVE-2024-33147. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-33148	J2EEFAST 2.7.0 list sql_filter sql injection	A vulnerability which was classified as critical was found in J2EEFAST 2.7.0. This affects the function list. The manipulation of the argument sql_filter leads to sql injection. This vulnerability is uniquely identified as CVE-2024-33148. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-33155	J2EEFAST 2.7.0 getDeptList sql_filter sql injection	A vulnerability was found in J2EEFAST 2.7.0 and classified as critical. This issue affects the function getDeptList. The manipulation of the argument sql_filter leads to sql injection. The identification of this vulnerability is CVE-2024-33155. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-33161	J2EEFAST 2.7.0 unallocatedList sql_filter sql injection	A vulnerability was found in J2EEFAST 2.7.0. It has been classified as critical. Affected is the function unallocatedList. The manipulation of the argument sql_filter leads to sql injection. This vulnerability is traded as CVE-2024-33161. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-33153	J2EEFAST 2.7.0 commentList sql_filter sql injection	A vulnerability classified as critical has been found in J2EEFAST 2.7.0. Affected is the function commentList. The manipulation of the argument sql_filter leads to sql injection. This vulnerability is traded as CVE-2024-33153. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-33149	J2EEFAST 2.7.0 myProcessList sql_filter sql injection	A vulnerability which was classified as critical was found in J2EEFAST 2.7.0. Affected is the function myProcessList. The manipulation of the argument sql_filter leads to sql injection. This vulnerability is traded as CVE-2024-33149. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-34314	CmsEasy 7.7.7.9 template_admin.php file_get_contents file inclusion	A vulnerability which was classified as problematic was found in CmsEasy 7.7.7.9. This affects the function file_get_contents of the file /admin/template_admin.php. The manipulation leads to file inclusion. This vulnerability is uniquely identified as CVE-2024-34314. The attack can only be done within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-4654	BlueNet Technology Clinical Browsing System 1.2.1 /xds/cloudInterface.php INSTI_CODE sql injection	A vulnerability was found in BlueNet Technology Clinical Browsing System 1.2.1. It has been classified as critical. This affects an unknown part of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		file /xds/cloudInterface.php. The manipulation of the argument INSTI_CODE leads to sql injection. This vulnerability is uniquely identified as CVE-2024-4654. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-4653	BlueNet Technology Clinical Browsing System 1.2.1 /xds/outIndex.php name sql injection	A vulnerability was found in BlueNet Technology Clinical Browsing System 1.2.1 and classified as critical. Affected by this issue is some unknown functionality of the file /xds/outIndex.php. The manipulation of the argument name leads to sql injection. This vulnerability is handled as CVE-2024-4653. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-32655	Npgsql up to 8.0.2 NpgsqlConnector.FrontendMessages.cs WriteBind integer overflow	A vulnerability classified as critical was found in Npgsql up to 8.0.2. This vulnerability affects the function WriteBind of the file src/Npgsql/Internal/NpgsqlConnector.FrontendMessages.cs. The manipulation leads to integer overflow. This vulnerability was named CVE-2024-32655. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-34220	SourceCodester Human Resource Management System 1.0 leave sql injection	A vulnerability classified as critical was found in SourceCodester Human Resource Management System 1.0. Affected by	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		this vulnerability is an unknown functionality. The manipulation of the argument leave leads to sql injection. This vulnerability is known as CVE-2024-34220. The attack can be launched remotely. There is no exploit available.		
CVE-2024-34310	Jin Fang Times Content Management System 3.2.3 id sql injection	A vulnerability was found in Jin Fang Times Content Management System 3.2.3. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-34310. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-30801	Cloud Based Customer Service Management Platform 1.0.0 Login.asp sql injection	A vulnerability classified as critical has been found in Cloud Based Customer Service Management Platform 1.0.0. Affected is an unknown function of the file Login.asp. The manipulation leads to sql injection. This vulnerability is traded as CVE-2024-30801. Local access is required to approach this attack. There is no exploit available.	Patched by core rule	Y
CVE-2024-4798	SourceCodester Online Computer and Laptop Store 1.0 manage_brand.php id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Online Computer and Laptop Store 1.0. Affected by this issue is some unknown functionality of the file /admin/maintenance/	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manage_brand.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-4798. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-4802	Kashipara College Management System 1.0 submit_extracurricular_activity.php activity_datetime sql injection	A vulnerability was found in Kashipara College Management System 1.0. It has been classified as critical. Affected is an unknown function of the file submit_extracurricular_activity.php. The manipulation of the argument activity_datetime leads to sql injection. This vulnerability is traded as CVE-2024-4802. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-4806	Kashipara College Management System 1.0 each_extracurricula_activities.php id sql injection	A vulnerability classified as critical was found in Kashipara College Management System 1.0. This vulnerability affects unknown code of the file each_extracurricula_activities.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-4806. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-4807	Kashipara College Management System 1.0 delete_user.php id sql injection	A vulnerability which was classified as critical has been found in Kashipara College Management System	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		1.0. This issue affects some unknown processing of the file delete_user.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-4807. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-34222	SourceCodester Human Resource Management System 1.0 searccountry sql injection	A vulnerability was found in SourceCodester Human Resource Management System 1.0. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument searccountry leads to sql injection. The identification of this vulnerability is CVE-2024-34222. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-50718	NocoDB up to 0.202.9 table_name sql injection	A vulnerability was found in NocoDB up to 0.202.9. It has been rated as critical. This issue affects some unknown processing. The manipulation of the argument table_name leads to sql injection. The identification of this vulnerability is CVE-2023-50718. 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-2024-34226	SourceCodester Visitor Management	A vulnerability was found in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	System 1.0 id sql injection	SourceCodester Visitor Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /php-sqlite-vms/pagemanage_visitor&id1. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-34226. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2024-4973	code-projects Simple Chat System 1.0 /register.php name/number/address sql injection	A vulnerability classified as critical was found in code-projects Simple Chat System 1.0. This vulnerability affects unknown code of the file /register.php. The manipulation of the argument name/number/address leads to sql injection. This vulnerability was named CVE-2024-4973. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-35409	WeBid 1.1.2 admin/tax.php sql injection	A vulnerability was found in WeBid 1.1.2. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file admin/tax.php. The manipulation leads to sql injection. This vulnerability is known as CVE-2024-35409. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-3552	Web Directory Free Plugin up to 1.6.9 on	A vulnerability classified as critical was	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	WordPress sql injection	found in Web Directory Free Plugin up to 1.6.9 on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2024-3552. The attack can be launched remotely. There is no exploit available.		
CVE-2024-5365	SourceCodester Best House Rental Management System up to 1.0 manage_payment.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Best House Rental Management System up to 1.0. This affects an unknown part of the file manage_payment.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-5365. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-5366	SourceCodester Best House Rental Management System up to 1.0 edit-cate.php id sql injection	A vulnerability has been found in SourceCodester Best House Rental Management System up to 1.0 and classified as critical. This vulnerability affects unknown code of the file edit-cate.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-5366. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-5378	SourceCodester	A vulnerability was	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	School Intramurals Student Attendance Management System /manage_sy.php sql injection	found in SourceCodester School Intramurals Student Attendance Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /manage_sy.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-5378. The attack can be initiated remotely. Furthermore there is an exploit available.	core rule	
CVE-2024-5364	SourceCodester Best House Rental Management System up to 1.0 manage_tenant.php id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Best House Rental Management System up to 1.0. Affected by this issue is some unknown functionality of the file manage_tenant.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-5364. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-5363	SourceCodester Best House Rental Management System up to 1.0 manage_user.php id sql injection	A vulnerability classified as critical was found in SourceCodester Best House Rental Management System up to 1.0. Affected by this vulnerability is an unknown functionality of the file manage_user.php. The manipulation of the argument id leads to sql injection. This vulnerability is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		known as CVE-2024-5363. The attack can be launched remotely. Furthermore there is an exploit available.		

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-32887	Sidekiq up to 7.2.3 substr cross site scripting (GHSA-q655-3pj8-9fxq)	A vulnerability was found in Sidekiq up to 7.2.3. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument substr leads to cross site scripting. This vulnerability is handled as CVE-2024-32887. 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-2024-31741	MiniCMS 1.11 cross site scripting (Issue 49)	A vulnerability was found in MiniCMS 1.11 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-31741. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-4293	PHPGurukul Doctor Appointment Management System 1.0 appointment-bwdates-reports-details.php fromdate/todate cross site scripting	A vulnerability classified as problematic was found in PHPGurukul Doctor Appointment Management System 1.0. Affected by this vulnerability is an unknown functionality of the file appointment-bwdates-reports-details.php. The manipulation of the argument fromdate/todate 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-2024-4293. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2023-51254	JFinalCMS 5.0.0 Friendship Link cross site scripting	A vulnerability was found in JFinalCMS 5.0.0 and classified as problematic. Affected by this issue is some unknown functionality of the component Friendship Link Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-51254. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-1905	Smart Forms Plugin up to 2.6.95 on WordPress Setting cross site scripting	A vulnerability was found in Smart Forms Plugin up to 2.6.95 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-1905. 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-2024-3192	MailCleaner up to 2023.03.14 Admin Interface Mail Message cross site scripting (MZ-24-01)	A vulnerability which was classified as problematic was found in MailCleaner up to 2023.03.14. Affected is an unknown function of the component Admin Interface. The manipulation as part of Mail Message leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is traded as CVE-2024-3192. It is possible to launch the attack remotely. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue.		
CVE-2024-3194	MailCleaner up to 2023.03.14 Log File Endpoint cross site scripting (MZ-24-01)	A vulnerability was found in MailCleaner up to 2023.03.14 and classified as problematic. Affected by this issue is some unknown functionality of the component Log File Endpoint. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-3194. The attack may be launched remotely. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y
CVE-2024-33905	Telegram WebK up to 1.x web_app_open_link cross site scripting	A vulnerability classified as problematic was found in Telegram WebK up to 1.x. This vulnerability affects the function web_app_open_link. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-33905. 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-2020-27478	Simplcommerce up to 3103357200c70b476	A vulnerability was found in Simplcommerce up to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	7986544e01b19dbf11505a7 Search Bar cross site scripting	3103357200c70b4767986544e01b19dbf11505a7. It has been classified as problematic. This affects an unknown part of the component Search Bar. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2020-27478. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-33102	ThinkSAAS 3.7.0 /pubs/counter.php code cross site scripting (Issue 35)	A vulnerability was found in ThinkSAAS 3.7.0. It has been rated as problematic. This issue affects some unknown processing of the file /pubs/counter.php. The manipulation of the argument code leads to cross site scripting. The identification of this vulnerability is CVE-2024-33102. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-33101	ThinkSAAS 3.7.0 /action/anti.php word cross site scripting (Issue 34)	A vulnerability classified as problematic was found in ThinkSAAS 3.7.0. This vulnerability affects unknown code of the file /action/anti.php. The manipulation of the argument word leads to cross site scripting. This vulnerability was named CVE-2024-33101. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-33831	yapi 1.10.2 Advanced Expectation	A vulnerability classified as problematic has been	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Response module body cross site scripting (Issue 2745)	found in yapi 1.10.2. This affects an unknown part of the component Advanced Expectation Response module. The manipulation of the argument body leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-33831. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-33424	CMSimple 5.15 Settings Menu Downloads cross site scripting	A vulnerability which was classified as problematic has been found in CMSimple 5.15. This issue affects some unknown processing of the component Settings Menu. The manipulation of the argument Downloads leads to cross site scripting. The identification of this vulnerability is CVE-2024-33424. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-33300	Typora up to 1.7 Markdown Editor cross site scripting	A vulnerability was found in Typora up to 1.7. It has been classified as problematic. This affects an unknown part of the component Markdown Editor. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-33300. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-33423	CMSimple 5.15 Settings Menu Logout cross site scripting	A vulnerability which was classified as problematic was found in CMSimple 5.15.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Affected is an unknown function of the component Settings Menu. The manipulation of the argument Logout leads to cross site scripting. This vulnerability is traded as CVE-2024-33423. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2024-32890	librespeed speedtest up to 5.3.0 processedString cross site scripting	A vulnerability was found in librespeed speedtest up to 5.3.0. It has been rated as problematic. This issue affects some unknown processing. The manipulation of the argument processedString leads to cross site scripting. The identification of this vulnerability is CVE-2024-32890. 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-2024-32970	phlex up to 1.9.2/1.10.1 cross site scripting	A vulnerability was found in phlex up to 1.9.2/1.10.1. 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-2024-32970. 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-2024-34061	dgtlmoon	A vulnerability was	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	changedetection.io up to 0.45.21 notification_urls cross site scripting (GHSA-pwgc-w4x9-gw67)	found in dgtlmoon changedetection.io up to 0.45.21. It has been rated as problematic. This issue affects the function notification_urls. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-34061. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	core rule	
CVE-2024-4216	pgAdmin up to 8.5 API /settings/store cross site scripting	A vulnerability which was classified as problematic has been found in pgAdmin up to 8.5. This issue affects some unknown processing of the file /settings/store of the component API. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-4216. 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-2024-34067	Pterodactyl Panel up to 1.11.5 cross site scripting	A vulnerability was found in Pterodactyl Panel up to 1.11.5. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument Name/Environment variable/Default value/Description/Validation rules leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is known as CVE-2024-34067. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-3637	Responsive Contact Form Builder & Lead Generation Plugin Setting cross site scripting	A vulnerability which was classified as problematic has been found in Responsive Contact Form Builder & Lead Generation Plugin up to 1.8.9 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-2024-3637. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-3692	Gutenverse Plugin up to 1.9.0 on WordPress htmlTag cross site scripting	A vulnerability which was classified as problematic was found in Gutenverse Plugin up to 1.9.0 on WordPress. Affected is an unknown function. The manipulation of the argument htmlTag leads to cross site scripting. This vulnerability is traded as CVE-2024-3692. 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-2024-33791	Netis MEX605 2.00.06 getTimeZone cross	A vulnerability has been found in Netis MEX605 2.00.06 and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	site scripting	classified as problematic. Affected by this vulnerability is the function getTimeZone. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-33791. The attack can be launched remotely. There is no exploit available.		
CVE-2024-34449	vanessa219 Vditor 3.10.3 Element Attribute cross site scripting	A vulnerability was found in vanessa219 Vditor 3.10.3. It has been classified as problematic. Affected is an unknown function of the component Element Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-34449. It is possible to launch the attack remotely. There is no exploit available. The real existence of this vulnerability is still doubted at the moment. It is recommended to change the configuration settings.	Patched by core rule	Y
CVE-2024-34467	ThinkPHP 8.0.3 Cookie think_exception.tpl PHPSESSION information exposure (Issue 2996)	A vulnerability which was classified as problematic was found in ThinkPHP 8.0.3. This affects an unknown part of the file think_exception.tpl of the component Cookie Handler. The manipulation of the argument PHPSESSION leads to information exposure through error message. This vulnerability is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		uniquely identified as CVE-2024-34467. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-4512	SourceCodester Prison Management System 1.0 edit-profile.php cross site scripting	A vulnerability classified as problematic was found in SourceCodester Prison Management System 1.0. This vulnerability affects unknown code of the file /Employee/edit-profile.php. The manipulation of the argument txtfullname/txtdob/txtaddress/txtqualification/cmddept/cmdemployeetype/txtappointment leads to cross site scripting. This vulnerability was named CVE-2024-4512. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-4513	Campcodes Complete Web-Based School Management 1.0 timetable_update_form.php grade cross site scripting	A vulnerability which was classified as problematic has been found in Campcodes Complete Web-Based School Management 1.0. This issue affects some unknown processing of the file /view/timetable_update_form.php. The manipulation of the argument grade leads to cross site scripting. The identification of this vulnerability is CVE-2024-4513. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-4519	Campcodes Complete Web-Based School Management 1.0 teacher_salary_detai	A vulnerability was found in Campcodes Complete Web-Based School Management 1.0. It has been rated	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	ls3.php month cross site scripting	as problematic. This issue affects some unknown processing of the file /view/teacher_salary_details3.php. The manipulation of the argument month leads to cross site scripting. The identification of this vulnerability is CVE-2024-4519. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-4526	Campcodes Complete Web-Based School Management System 1.0 student_payment_details3.php month cross site scripting	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file /view/student_payment_details3.php. The manipulation of the argument month leads to cross site scripting. The identification of this vulnerability is CVE-2024-4526. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-4518	Campcodes Complete Web-Based School Management 1.0 teacher_salary_invoice.php desc cross site scripting	A vulnerability was found in Campcodes Complete Web-Based School Management 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /view/teacher_salary_invoice.php. The manipulation of the argument desc leads to cross site scripting. This vulnerability was named CVE-2024-4518.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-4527	Campcodes Complete Web-Based School Management System 1.0 student_payment_details2.php index cross site scripting	A vulnerability was found in Campcodes Complete Web-Based School Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file /view/student_payment_details2.php. The manipulation of the argument index leads to cross site scripting. This vulnerability is traded as CVE-2024-4527. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-33548	Asus RT-AC51U up to 3.0.0.4.380.8591 WPA Pre-Shared Key cross site scripting	A vulnerability which was classified as problematic has been found in Asus RT-AC51U up to 3.0.0.4.380.8591. This issue affects some unknown processing. The manipulation of the argument WPA Pre-Shared Key leads to cross site scripting. The identification of this vulnerability is CVE-2023-33548. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-28725	YzmCMS 7.0 cross site scripting	A vulnerability was found in YzmCMS 7.0 and classified as problematic. This issue affects some unknown processing of the component Ads Management/Carousel Management/System Settings. The manipulation leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The identification of this vulnerability is CVE-2024-28725. The attack may be initiated remotely. There is no exploit available.		
CVE-2024-3628	EasyEvent Plugin up to 1.0.0 on WordPress Setting cross site scripting	A vulnerability was found in EasyEvent Plugin up to 1.0.0 on WordPress. It has been declared as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-3628. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-34255	JIZHICMS 2.5.1 Message cross site scripting	A vulnerability was found in JIZHICMS 2.5.1. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Message Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-34255. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-4644	SourceCodester Prison Management System 1.0 changepassword.php cross site scripting	A vulnerability has been found in SourceCodester Prison Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /Employee/changepassword.php. The manipulation of the argument	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		txtold_password/txtnew_password/txtconfirm_password leads to cross site scripting. This vulnerability was named CVE-2024-4644. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-4645	SourceCodester Prison Management System 1.0 changepassword.php cross site scripting	A vulnerability was found in SourceCodester Prison Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file /Admin/changepassword.php. The manipulation of the argument txtold_password/txtnew_password/txtconfirm_password leads to cross site scripting. The identification of this vulnerability is CVE-2024-4645. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-29881	PHPOK 6.4.003 call_control.php index_f sql injection (Issue 15)	A vulnerability was found in PHPOK 6.4.003 and classified as critical. Affected by this issue is the function index_f of the file phpok64/framework/api/call_control.php. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-29881. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-24157	gnuboard g6 c2cc1f5069e00491ea48618d957332d90f6d40e4 board.py	A vulnerability was found in gnuboard g6 c2cc1f5069e00491ea48618d957332d90f6d40e	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	cross site scripting	4. It has been rated as problematic. This issue affects some unknown processing of the file board.py. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-24157. The attack may be initiated remotely. There is no exploit available.		
CVE-2024-34349	Sylius up to 1.12.15/1.13.0 Name cross site scripting (GHSA-v2f9-rv6w-vw8r)	A vulnerability was found in Sylius up to 1.12.15/1.13.0 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument Name leads to cross site scripting. This vulnerability is handled as CVE-2024-34349. 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-2024-34070	Froxlor up to 2.1.8 System Log loginname cross site scripting	A vulnerability was found in Froxlor up to 2.1.8. It has been classified as problematic. This affects an unknown part of the component System Log Handler. The manipulation of the argument loginname leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-34070. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		upgrade the affected component.		
CVE-2024-3941	reCAPTCHA Jetpack Plugin up to 0.2.2 on WordPress cross site scripting	A vulnerability was found in reCAPTCHA Jetpack Plugin up to 0.2.2 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-2024-3941. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-34231	SourceCodester Laboratory Management System 1.0 System Short Name cross site scripting	A vulnerability classified as problematic has been found in SourceCodester Laboratory Management System 1.0. Affected is an unknown function. The manipulation of the argument System Short Name leads to cross site scripting. This vulnerability is traded as CVE-2024-34231. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-2299	parisneo lollms-webui Profile Picture cross site scripting	A vulnerability was found in parisneo lollms-webui. It has been rated as problematic. This issue affects some unknown processing of the component Profile Picture Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-2299. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-34230	SourceCodester Laboratory Management System 1.0 System Information cross site scripting	A vulnerability has been found in SourceCodester Laboratory Management System 1.0 and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument System Information leads to cross site scripting. This vulnerability was named CVE-2024-34230. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-49781	NocoDB up to 0.202.8 Formula.vue replaceUrlsWithLink urls cross site scripting	A vulnerability was found in NocoDB up to 0.202.8 and classified as problematic. Affected by this issue is the function replaceUrlsWithLink of the file nc-gui/components/virtual-cell/Formula.vue. The manipulation of the argument urls leads to cross site scripting. This vulnerability is handled as CVE-2023-49781. 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-2024-34081	MantisBT up to 2.26.1 bug_change_status_page.php cross site scripting	A vulnerability which was classified as problematic has been found in MantisBT up to 2.26.1. This issue affects some unknown processing of the file bug_change_status_page.php. The manipulation leads to cross site scripting. The identification of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		this vulnerability is CVE-2024-34081. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-28866	GoCD up to 24.0.x redirect_to cross site scripting	A vulnerability which was classified as problematic was found in GoCD up to 24.0.x. Affected is an unknown function. The manipulation of the argument redirect_to leads to cross site scripting. This vulnerability is traded as CVE-2024-28866. 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-2024-34749	Aidin Phormer up to 3.34 cross site scripting	A vulnerability was found in Aidin Phormer up to 3.34. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability is known as CVE-2024-34749. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-34698	freescout-helpdesk freescout up to 1.8.138 /public/js/main.js getQueryParam prototype pollution	A vulnerability was found in freescout-helpdesk freescout up to 1.8.138. It has been declared as problematic. This vulnerability affects the function getQueryParam of the file /public/js/main.js. The manipulation leads to improperly controlled modification of object prototype attributes . This vulnerability was named CVE-2024-34698. 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-2024-32077	Apache Airflow up to 2.9.0 Task Instance Log cross site scripting	A vulnerability classified as problematic has been found in Apache Airflow up to 2.9.0. This affects an unknown part of the component Task Instance Log Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-32077. 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-2024-3241	Ultimate Blocks Plugin up to 3.1.6 on WordPress cross site scripting	A vulnerability classified as problematic has been found in Ultimate Blocks Plugin up to 3.1.6 on WordPress. Affected is an unknown function. The manipulation leads to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross site scripting. This vulnerability is traded as CVE-2024-3241. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-4974	code-projects Simple Chat System 1.0 /register.php name cross site scripting	A vulnerability which was classified as problematic was found in code-projects Simple Chat System 1.0. Affected is an unknown function of the file /register.php. The manipulation of the argument name leads to cross site scripting. This vulnerability is traded as CVE-2024-4974. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-4975	code-projects Simple Chat System 1.0 Message cross site scripting	A vulnerability which was classified as problematic has been found in code-projects Simple Chat System 1.0. This issue affects some unknown processing of the component Message Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-4975. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-4968	SourceCodester Interactive Map with Marker 1.0 Add Marker Marker Name cross site scripting	A vulnerability was found in SourceCodester Interactive Map with Marker 1.0. It has been rated as problematic.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Affected by this issue is some unknown functionality of the file Marker Name of the component Add Marker. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-4968. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-3644	Newsletter Popup Plugin up to 1.2 on WordPress Setting cross site scripting	A vulnerability was found in Newsletter Popup Plugin up to 1.2 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-3644. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-3641	Newsletter Popup Plugin up to 1.2 on WordPress cross site scripting	A vulnerability was found in Newsletter Popup Plugin up to 1.2 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-2024-3641. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-3288	Logo Slider Plugin up to 3.9.9 on WordPress cross site scripting	A vulnerability has been found in Logo Slider Plugin up to 3.9.9 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. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-3288. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-3368	All in One SEO Plugin up to 4.6.1.0 on WordPress Post Field cross site scripting	A vulnerability which was classified as problematic was found in All in One SEO Plugin up to 4.6.1.0 on WordPress. This affects an unknown part of the component Post Field Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-3368. 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-2024-3917	Pet Manager Plugin up to 1.4 on WordPress cross site scripting	A vulnerability was found in Pet Manager Plugin up to 1.4 on WordPress. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-3917. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-2220	Button Contact VR Plugin up to 4.7 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic has been found in Button Contact VR Plugin up to 4.7 on WordPress. This issue affects some unknown processing of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the component Setting Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-2220. The attack may be initiated remotely. There is no exploit available.		
CVE-2024-3918	Pet Manager Plugin up to 1.4 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic was found in Pet Manager Plugin up to 1.4 on WordPress. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-3918. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-3920	Flattr Plugin up to 1.2.2 on WordPress Setting cross site scripting	A vulnerability has been found in Flattr Plugin up to 1.2.2 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-3920. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-3594	IDonate Plugin up to 1.9.0 on WordPress Setting cross site scripting	A vulnerability classified as problematic was found in IDonate Plugin up to 1.9.0 on WordPress. This vulnerability affects unknown code of the component	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Setting Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-3594. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-5367	Kashipara College Management System 1.0 each_extracurricula_activities.php id cross site scripting	A vulnerability was found in Kashipara College Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file each_extracurricula_activities.php. The manipulation of the argument id leads to cross site scripting. The identification of this vulnerability is CVE-2024-5367. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-5375	Kashipara College Management System 1.0 submit_student.php address cross site scripting	A vulnerability has been found in Kashipara College Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file submit_student.php. The manipulation of the argument address leads to cross site scripting. This vulnerability is known as CVE-2024-5375. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-5370	Kashipara College Management System 1.0 submit_enroll_staff.php class_name	A vulnerability was found in Kashipara College Management System 1.0. It has been rated as problematic.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	cross site scripting	Affected by this issue is some unknown functionality of the file submit_enroll_staff.php. The manipulation of the argument class_name leads to cross site scripting. This vulnerability is handled as CVE-2024-5370. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-5376	Kashipara College Management System 1.0 view_each_faculty.php id cross site scripting	A vulnerability was found in Kashipara College Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file view_each_faculty.php. The manipulation of the argument id leads to cross site scripting. This vulnerability is handled as CVE-2024-5376. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-5383	lakernote EasyAdmin up to 20240324 /sys/file/upload file cross site scripting (I9B58I)	A vulnerability classified as problematic has been found in lakernote EasyAdmin up to 20240324. This affects an unknown part of the file /sys/file/upload. The manipulation of the argument file leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-5383. It is possible to initiate the attack remotely. Furthermore there is an exploit available. This product takes the approach of rolling	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		releases to provide continious delivery. Therefore version details for affected and updated releases are not available. It is recommended to apply a patch to fix this issue.		
CVE-2024-5380	jsy-1 short-url 1.0.0 admin.php cross site scripting (I8UP2A)	A vulnerability classified as problematic has been found in jsy-1 short-url 1.0.0. Affected is an unknown function of the file admin.php. The manipulation of the argument url leads to cross site scripting. This vulnerability is traded as CVE-2024-5380. 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-2024-5385	oretnom23 Online Car Wash Booking System 1.0 /admin/ First Name/Last Name cross site scripting	A vulnerability which was classified as problematic has been found in oretnom23 Online Car Wash Booking System 1.0. This issue affects some unknown processing of the file /admin/pageuser/list. The manipulation of the argument First Name/Last Name with the input <script>confirm </script> leads to cross site scripting. The identification of this vulnerability is CVE-2024-5385. The attack may be initiated remotely. Furthermore there is an 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.

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™