INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

October 2024

The total **zero-day vulnerabilities** count for October month: 248

Command Injection	CSRF	SQL Injection	Local File Inclusion	Malicious File Upload	Cross-Site Scripting
21	9	93	13	11	101

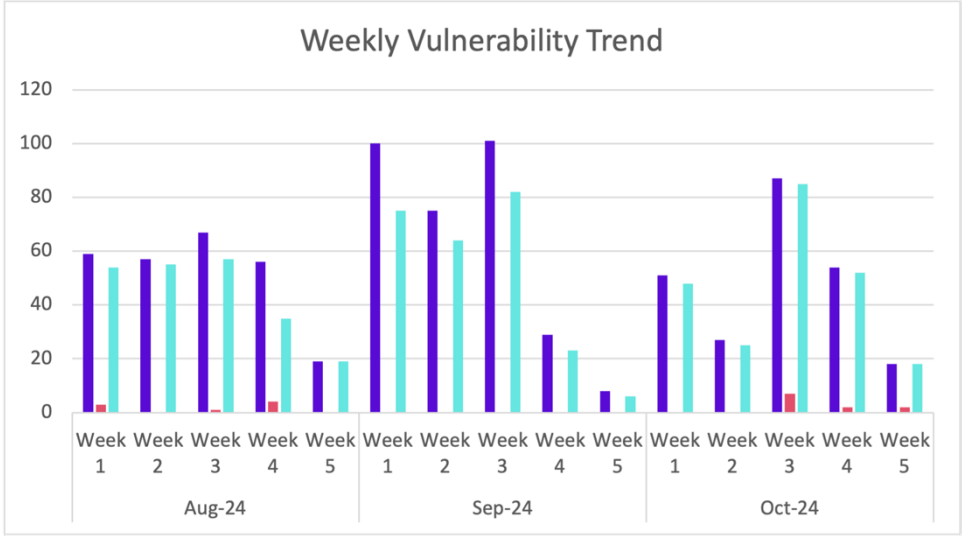
Zero-day vulnerabilities protected through core rules	237
Zero-day vulnerabilities protected through custom rules	11
Zero-day vulnerabilities found by Indusface WAS	228

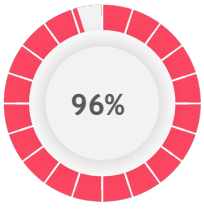
- To enable custom rules, please contact support@indusface.com
- Learn more about zero-day vulnerabilities, detection, and prevention, here

Vulnerability Trend:

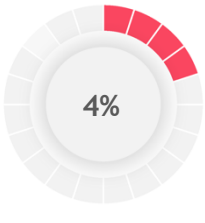
The weekly trend displays the total number of vulnerabilities discovered and the type of protection provided for the last quarter.

Weekly Vulnerability Trend

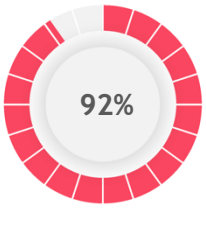




of the zero-day vulnerabilities were protected by the core rules in the last month

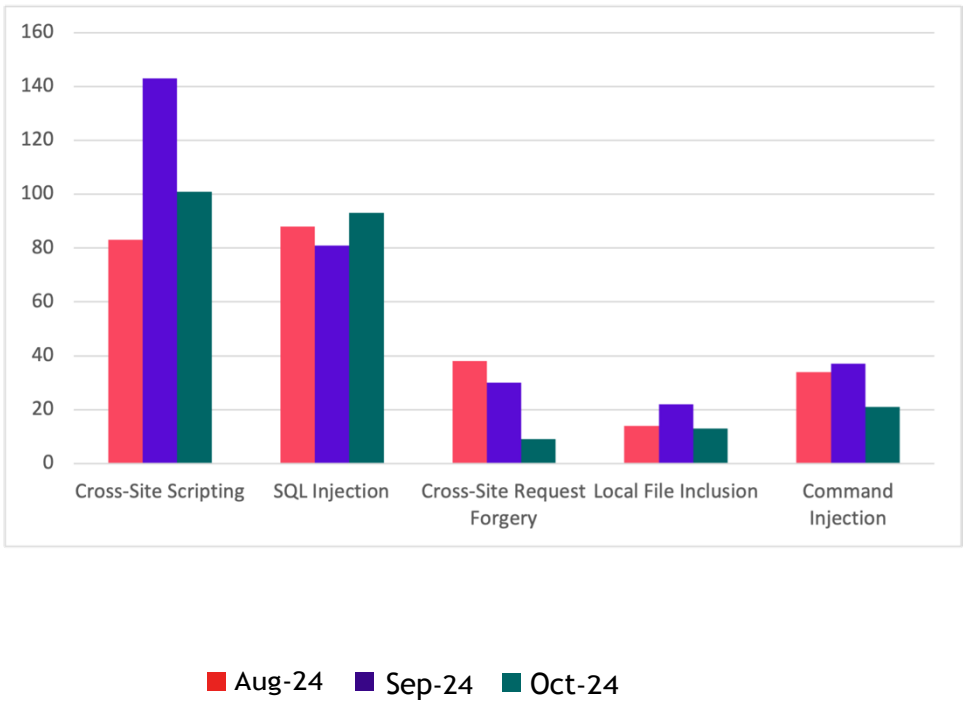


of the zero-day vulnerabilities were protected by the custom rules in the last month



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-2024-46256	NginxProxyManager 2.11.3 Add Lets Encrypt Certificate requestLetsEncryptSsl command injection	A vulnerability classified as critical has been found in NginxProxyManager 2.11.3. Affected is the function requestLetsEncryptSsl of the component Add Lets Encrypt Certificate. The manipulation leads to command injection. This vulnerability is traded as CVE-2024-46256. 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.	Patched by core rule	Y
CVE-2024-21531	git-shallow-clone gitShallowClone process os command injection (SNYK-JS-GITSHALLOWCLONE-3253853)	A vulnerability classified as critical was found in git-shallow-clone. Affected by this vulnerability is the function gitShallowClone. The manipulation of the argument process leads to os command injection. This vulnerability is known as CVE-2024-21531. It is possible to launch the attack on the local host. There is no exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-9054	Microchip TimeProvider 4100 up to 2.4.6 Configuration Module os command injection	A vulnerability which was classified as critical has been found in Microchip TimeProvider 4100 up to 2.4.6. Affected by this issue is some unknown functionality of the component Configuration Module. The manipulation leads to os command injection. This vulnerability is handled as CVE-2024-9054. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2022-30357	D-Link DI-8200 16.07.26A1 upgrade_filter.asp upgrade_filter_asp path command injection	A vulnerability has been found in D-Link DI-8200 16.07.26A1 and classified as critical. Affected by this vulnerability is the function upgrade_filter_asp of the file upgrade_filter.asp. The manipulation of the argument path leads to command injection. This vulnerability is known as CVE-2024-44413. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-10193	Web Tip SHIRASAGI up to 1.19.0 HTTP Request path traversal	A vulnerability has been found in Web Tip SHIRASAGI up to 1.19.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the component HTTP Request Handler. The manipulation leads to path traversal. This vulnerability is known as CVE-2024-46898. 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-2024-37844	D-Link DIR-878/DIR-882 POST SetVirtualServerSettings command	A vulnerability was found in D-Link DIR-878 and DIR-882. It has been declared as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	critical. Affected by this vulnerability is the function SetVirtualServerSettings of the component POST Handler. The manipulation of the argument ExternalPort/InternalPort/ProtocolNumber/LocalIPAddress leads to command injection. This vulnerability is known as CVE-2024-48633. The attack can be launched remotely. There is no exploit available.		
CVE-2024-41992	D-Link DIR-822/DIR-878 FW130 POST SetVLANSettings VID command injection	A vulnerability classified as critical has been found in D-Link DIR-822 and DIR-878 FW130. Affected is the function SetVLANSettings of the component POST Handler. The manipulation of the argument VID leads to command injection. This vulnerability is traded as CVE-2024-48637. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-46212	D-Link DIR-822/DIR-878 FW130 POST SetGuestZoneRouterSettings SubnetMask command injection	A vulnerability classified as critical was found in D-Link DIR-822 and DIR-878 FW130. Affected by this vulnerability is the function SetGuestZoneRouterSettings of the component POST Handler. The manipulation of the argument SubnetMask leads to command injection. This vulnerability is known as CVE-2024-48638. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-46240	D-Link DIR-822/DIR-878 FW130 POST SetWLanRadioSettings SSID command injection	A vulnerability was found in D-Link DIR-822 and DIR-878 FW130 and classified as critical. Affected by this issue is the function SetWLanRadioSettings of the component POST Handler. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument SSID leads to command injection. This vulnerability is handled as CVE-2024-48631. The attack may be launched remotely. There is no exploit available.		
CVE-2023-39593	MariaDB 10.5 sys_exec code injection	A vulnerability classified as critical has been found in MariaDB 10.5. This affects the function sys_exec. The manipulation leads to code injection. This vulnerability is uniquely identified as CVE-2023-39593. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-27766	MariaDB 11.1 lib_mysqludf_sys.so code injection	A vulnerability was found in MariaDB 11.1. It has been declared as critical. This vulnerability affects unknown code in the library lib_mysqludf_sys.so. The manipulation leads to code injection. This vulnerability was named CVE-2024-27766. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-26785	MariaDB 10.5 code injection	A vulnerability has been found in MariaDB 10.5 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to code injection. This vulnerability is known as CVE-2023-26785. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-48654	WAVLINK WN530H4/WN530HG4/WN572HG3 up to 20221028 internet.cgi ping_ddns DDNS command injection	A vulnerability was found in WAVLINK WN530H4 WN530HG4 and WN572HG3 up to 20221028 and classified as critical. This issue affects the function ping_ddns of the file internet.cgi. The manipulation of the argument DDNS leads to command injection. The identification of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		this vulnerability is CVE-2024-10193. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-48706	infiniflow ragflow up to 0.11.0 llm_app.py add_llm req['llm_factory']/req['llm_name'] command injection	A vulnerability classified as very critical has been found in infiniflow ragflow up to 0.11.0. Affected is the function add_llm of the file llm_app.py. The manipulation of the argument req[&039;llm_factory&039;]/req[&039;llm_name&039;] leads to command injection. This vulnerability is traded as CVE-2024-10131. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-48142	Butterfly Effect Limited Monica ChatGPT AI Assistant 2.4.0 Chatbox injection	A vulnerability classified as critical was found in Butterfly Effect Limited Monica ChatGPT AI Assistant 2.4.0. Affected by this vulnerability is an unknown functionality of the component Chatbox. The manipulation leads to injection. This vulnerability is known as CVE-2024-48142. The attack can only be done within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-48141	Zhipu AI CodeGeeX 2.17.0 Chatbox injection	A vulnerability was found in Zhipu AI CodeGeeX 2.17.0. It has been classified as problematic. Affected is an unknown function of the component Chatbox. The manipulation leads to injection. This vulnerability is traded as CVE-2024-48141. Access to the local network is required for this attack to succeed. There is no exploit available.	Patched by core rule	Y
CVE-2024-48140	Butterfly Effect	A vulnerability	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Limited Monica Your AI Copilot 6.3.0 Chatbox injection	classified as critical has been found in Butterfly Effect Limited Monica Your AI Copilot 6.3.0. Affected is an unknown function of the component Chatbox. The manipulation leads to injection. This vulnerability is traded as CVE-2024-48140. The attack needs to be approached within the local network. There is no exploit available.	core rule	
CVE-2024-48145	Netangular ChatNet AI 1.0 Chatbox injection	A vulnerability was found in Netangular ChatNet AI 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Chatbox. The manipulation leads to injection. This vulnerability is handled as CVE-2024-48145. The attack can only be done within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-48144	Fusion Chat Chat AI Assistant Ask Me Anything 1.2.4.0 Chatbox injection	A vulnerability was found in Fusion Chat Chat AI Assistant Ask Me Anything 1.2.4.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Chatbox. The manipulation leads to injection. This vulnerability is known as CVE-2024-48144. The attack needs to be approached within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-48139	Blackbox AI 1.3.95 Chatbox injection	A vulnerability was found in Blackbox AI 1.3.95 and classified as problematic. This issue affects some unknown processing of the component Chatbox. The manipulation leads to injection. The identification of this vulnerability is CVE-2024-48139. Access to the local network is required for	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		this attack. There is no exploit available.		
CVE-2024-37846	MangoOS up to 5.1.x Platform Management Edit Page injection	A vulnerability classified as problematic has been found in MangoOS up to 5.1.x. Affected is an unknown function of the component Platform Management Edit Page. The manipulation leads to injection. This vulnerability is traded as CVE-2024-37846. The attack can only be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-45987	projectworlds Online Voting System 1.0 voter.php cross-site request forgery	A vulnerability has been found in projectworlds Online Voting System 1.0 and classified as problematic. This vulnerability affects unknown code of the file voter.php. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2024-45987. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-9282	bg5sbk MiniCMS 1.11 page-edit.php cross-site request forgery	A vulnerability was found in bg5sbk MiniCMS 1.11. It has been classified as problematic. Affected is an unknown function of the file page-edit.php. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-9282. 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. The initial researcher advisory mentions confusing version and file name information.	Patched by core rule	N
CVE-2024-9281	bg5sbk MiniCMS up to 1.11 post-edit.php cross-site request forgery	A vulnerability was found in bg5sbk MiniCMS up to 1.11 and classified as problematic. This issue affects some unknown processing of the file post-edit.php. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-9281. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		not respond in any way. The initial researcher advisory mentions confusing version and file name information.		
CVE-2024-47846	Wikimedia Cargo Extension 3.6.0 on Mediawiki cross-site request forgery	A vulnerability was found in Wikimedia Cargo Extension 3.6.0 on Mediawiki 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-2024-47846. 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-2024-47828	ampache up to 6.6.0 Request cross-site request forgery (GHSA-p9cq-2qph-55f2)	A vulnerability was found in ampache up to 6.6.0. It has been rated as problematic. This issue affects some unknown processing of the component Request Handler. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-47828. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2020-36836	Gradio up to 4.x cross site scripting (GHSA-gvv6-33j7-884g)	A vulnerability classified as problematic has been found in Gradio up to 4.x. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-47872. 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-2024-10045	SourceCodester Online Eyewear Shop 1.0 Code cross site scripting	A vulnerability which was classified as problematic was found in SourceCodester Online Eyewear Shop 1.0. Affected is an unknown function of the	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		file /admin/pageinventory/view_inventory&id2. The manipulation of the argument Code leads to cross site scripting. This vulnerability is traded as CVE-2024-9906. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2024-48038	PHPGurukul Boat Booking System 1.0 BW Dates Report Page bwdates-report-details.php fdate/tdate sql injection	A vulnerability which was classified as critical has been found in PHPGurukul Boat Booking System 1.0. Affected by this issue is some unknown functionality of the file /admin/bwdates-report-details.php of the component BW Dates Report Page. The manipulation of the argument fdate/tdate leads to sql injection. This vulnerability is handled as CVE-2024-10160. The attack may be launched remotely. Furthermore there is an exploit available. The initial researcher advisory only mentions the parameter "fdate" to be affected. But it must be assumed "tdate" is affected as well.	Patched by core rule	N
CVE-2024-48048	PHPGurukul Boat Booking System 1.0 Edit Subdomain Details Page /admin/edit-subadmin.php sadminusername/fullname/emailid/mobilenumber sql injection	A vulnerability has been found in PHPGurukul Boat Booking System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/edit-subadmin.php of the component Edit Subdomain Details Page. The manipulation of the argument sadminusername/fullname/emailid/mobilenumber leads to sql injection. This vulnerability was named CVE-2024-10162. The attack can be initiated remotely. Furthermore there is an exploit available. The initial researcher advisory only mentions	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the parameter "mobilenumber" to be affected. But it must be assumed that other parameters are affected as well.		

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-47170	agnaistic agnai up to 1.0.329 Configuration File path traversal (GHSA-h355-hm5h-cm8h)	A vulnerability was found in agnaistic agnai up to 1.0.329. It has been classified as problematic. This affects an unknown part of the component Configuration File Handler. The manipulation leads to path traversal: &039;.../...//&039;. This vulnerability is uniquely identified as CVE-2024-47170. 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-2024-41922	Veertu Anka Build 1.42.0 Log File Download path traversal (TALOS-2024-2061)	A vulnerability which was classified as critical was found in Veertu Anka Build 1.42.0. Affected is an unknown function of the component Log File Download Handler. The manipulation leads to path traversal. This vulnerability is traded as CVE-2024-41922. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-41163	Veertu Anka Build 1.42.0 HTTP Request path traversal (TALOS-2024-2059)	A vulnerability which was classified as critical has been found in Veertu Anka Build 1.42.0. This issue affects some unknown processing of the component HTTP Request Handler. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation leads to path traversal. The identification of this vulnerability is CVE-2024-41163. The attack may be initiated remotely. There is no exploit available.		
CVE-2024-47841	Wikimedia CSS Extension up to 1.39.8/1.41.2/1.42.1 on Mediawiki path traversal	A vulnerability was found in Wikimedia CSS Extension up to 1.39.8/1.41.2/1.42.1 on Mediawiki. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2024-47841. 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-2024-45290	PHPOffice PhpSpreadsheet up to 1.29.1/2.1.0 XLSX File absolute path traversal	A vulnerability was found in PHPOffice PhpSpreadsheet up to 1.29.1/2.1.0. It has been declared as problematic. This vulnerability affects unknown code of the component XLSX File Handler. The manipulation leads to absolute path traversal. This vulnerability was named CVE-2024-45290. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-46446	Mecha CMS up to 3.0.0 path traversal	A vulnerability was found in Mecha CMS up to 3.0.0. It has been classified as critical. This affects an unknown part. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2024-46446. Access to the local network is required for this attack. There is no exploit available.	Patched by core rule	Y
CVE-2024-45291	PHPOffice PhpSpreadsheet up to 1.29.1/2.1.0 XLSX File setEmbedImages absolute path traversal	A vulnerability was found in PHPOffice PhpSpreadsheet up to 1.29.1/2.1.0. It has been rated as problematic. This issue affects the function setEmbedImages of the component XLSX File Handler. The manipulation leads to absolute path traversal. The identification of this vulnerability is CVE-2024-45291. 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-2024-7037	open-webui up to 0.3.8 /api/pipelines/upload path traversal	A vulnerability which was classified as problematic was found in open-webui up to 0.3.8. Affected is an unknown function of the file /api/pipelines/upload. The manipulation leads to path traversal. This vulnerability is traded as CVE-2024-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		7037. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2024-47868	Gradio up to 4.x information disclosure (GHSA-4q3c-cj7g-jcwf)	A vulnerability was found in Gradio up to 4.x. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to information disclosure. This vulnerability is known as CVE-2024-47868. 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-2024-10313	code-projects Pharmacy Management System 1.0 manage_medicine_stock.php name/packing/generic_name/suppliers_name sql injection	A vulnerability which was classified as critical has been found in code-projects Pharmacy Management System 1.0. This issue affects some unknown processing of the file /php/manage_medicine_stock.php. The manipulation of the argument name/packing/generic_name/suppliers_name leads to sql injection. The identification of this vulnerability is CVE-2024-10024. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-10379	Sajid Javed Top Bar Plugin up to 2.0.1 on WordPress path traversal	A vulnerability was found in Sajid Javed Top Bar Plugin up to 2.0.1 on WordPress. It has been rated as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		critical. This issue affects some unknown processing. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2024-47645. The attack may be initiated remotely. There is no exploit available.		
CVE-2024-48931	code-projects Pharmacy Management System 1.0 Manage Medicines Page /manage_medicine.php name/address/doctor_address/suppliers_name cross site scripting	A vulnerability was found in code-projects Pharmacy Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /manage_medicine.php of the component Manage Medicines Page. The manipulation of the argument name/address/doctor_address/suppliers_name leads to cross site scripting. This vulnerability is handled as CVE-2024-10199. The attack may be launched remotely. Furthermore there is an exploit available. The initial researcher advisory mentions contradicting files to be affected.	Patched by core rule	Y
CVE-2024-49285	Collabtive 3.1 managemilestone.php name cross site scripting	A vulnerability was found in Collabtive 3.1. It has been classified as problematic. This affects an unknown part of the file managemilestone.php. The manipulation of the argument	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		name leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-48707. It is possible to initiate the attack remotely. There is no exploit available.		

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-46472	CodeAstro Membership Management System 1.0 Login Page email sql injection	A vulnerability which was classified as critical has been found in dingfanzu CMS up to 29d67d9044f6f93378e6eb6ff92272217ff7225c. Affected by this issue is some unknown functionality of the file saveNewPwd.php. The manipulation of the argument username leads to sql injection. This vulnerability is handled as CVE-2024-9294. The attack may be launched remotely. Furthermore there is an exploit available. Continious delivery with rolling releases is used by this product. Therefore no version details of affected nor updated releases are available.	Patched by core rule	Y
CVE-2024-9294	dingfanzu CMS up to 29d67d9044f6f93378e6eb6ff92272217ff7225c saveNewPwd.php username sql injection	A vulnerability classified as critical was found in skyselang yylAdmin up to 3.0. Affected by this vulnerability is the function list of the file /app/admin/controller/file/File.php of the component Backend. The manipulation of the argument is_disable leads to sql injection. This vulnerability is known as CVE-2024-9293. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9293	skyselang yylAdmin up to 3.0 Backend File.php list is_disable sql injection	A vulnerability was found in SourceCodester Advocate Office Management System	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		1.0 and classified as critical. This issue affects some unknown processing of the file /control/login.php. The manipulation of the argument username leads to sql injection. The identification of this vulnerability is CVE-2024-9295. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-9295	SourceCodester Advocate Office Management System 1.0 /control/login.php username sql injection	A vulnerability was found in SourceCodester Advocate Office Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /control/forgot_pass.php. The manipulation of the argument username leads to sql injection. This vulnerability is traded as CVE-2024-9296. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9296	SourceCodester Advocate Office Management System 1.0 /control/forgot_pass.php username sql injection	A vulnerability classified as critical was found in PHPGurukul Online Shopping Portal 2.0. This vulnerability affects unknown code of the file /shopping/admin/index.php of the component Admin Panel. The manipulation of the argument username leads to sql injection. This vulnerability was named CVE-2024-9326. The attack can be initiated remotely. Furthermore there is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		an exploit available.		
CVE-2024-9326	PHPGurukul Online Shopping Portal 2.0 Admin Panel index.php username sql injection	A vulnerability which was classified as critical was found in SourceCodester Online Timesheet App 1.0. This affects an unknown part of the file /endpoint/delete-timesheet.php. The manipulation of the argument timesheet leads to sql injection. This vulnerability is uniquely identified as CVE-2024-9319. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9319	SourceCodester Online Timesheet App 1.0 delete-timesheet.php timesheet sql injection	A vulnerability which was classified as critical has been found in SourceCodester Advocate Office Management System 1.0. Affected by this issue is some unknown functionality of the file /control/activate.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-9318. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9318	SourceCodester Advocate Office Management System 1.0 /control/activate.php id sql injection	A vulnerability classified as critical was found in SourceCodester Online Eyewear Shop 1.0. Affected by this vulnerability is the function delete_category of the file /classes/Master.phpfdelete_category. The manipulation of the argument id leads to sql injection.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is known as CVE-2024-9317. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2024-9317	SourceCodester Online Eyewear Shop 1.0 Master.php delete_category id sql injection	A vulnerability classified as critical has been found in code-projects Blood Bank Management System 1.0. Affected is an unknown function of the file /admin/blood/update/B+.php. The manipulation of the argument Bloodname leads to sql injection. This vulnerability is traded as CVE-2024-9316. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9316	code-projects Blood Bank Management System 1.0 B+.php Bloodname sql injection	A vulnerability was found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/maintenance/manage_department.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-9315. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9315	SourceCodester Employee and Visitor Gate Pass Logging System 1.0 manage_departmen	A vulnerability was found in SourceCodester Advocate Office Management System	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	t.php id sql injection	1.0. It has been rated as critical. This issue affects some unknown processing of the file /control/edit_client.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-9328. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-9328	SourceCodester Advocate Office Management System 1.0 /control/edit_client.php id sql injection	A vulnerability was found in code-projects Blood Bank System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /forgot.php. The manipulation of the argument useremail leads to sql injection. This vulnerability was named CVE-2024-9327. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9327	code-projects Blood Bank System 1.0 /forgot.php useremail sql injection	A vulnerability classified as critical has been found in Cost Calculator Builder Plugin up to 3.2.28 on WordPress. Affected is an unknown function. The manipulation leads to sql injection. This vulnerability is traded as CVE-2024-8379. 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-2024-8379	Cost Calculator Builder Plugin up to	A vulnerability was found in code-projects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	3.2.28 on WordPress sql injection	Restaurant Reservation System 1.0. It has been classified as critical. This affects an unknown part of the file /updatebal.php. The manipulation of the argument company leads to sql injection. This vulnerability is uniquely identified as CVE-2024-9360. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-9360	code-projects Restaurant Reservation System 1.0 /updatebal.php company sql injection	A vulnerability was found in code-projects Restaurant Reservation System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /addcompany.php. The manipulation of the argument company leads to sql injection. This vulnerability is handled as CVE-2024-9359. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9359	code-projects Restaurant Reservation System 1.0 /addcompany.php company sql injection	A vulnerability which was classified as critical has been found in OS4Ed openSIS-Classic 9.1. Affected by this issue is some unknown functionality. The manipulation leads to sql injection. This vulnerability is handled as CVE-2024-46626. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-46626	OS4Ed openSIS-Classic 9.1 sql injection	A vulnerability has been found in code-projects Restaurant Reservation System 1.0	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and classified as critical. Affected by this vulnerability is an unknown functionality of the file /filter2.php. The manipulation of the argument from/to leads to sql injection. This vulnerability is known as CVE-2024-9429. The attack can be launched remotely. Furthermore there is an exploit available. The initial researcher advisory only mentions the parameter "from" to be affected. But it must be assumed that parameter "to" is affected as well.		
CVE-2024-9429	code-projects Restaurant Reservation System 1.0 /filter2.php from/to sql injection	A vulnerability which was classified as critical was found in itsourcecode Sports Management System 1.0. Affected is the function delete_category of the file sports_scheduling/player.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-46078. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-46078	itsourcecode Sports Management System 1.0 player.php delete_category id sql injection	A vulnerability which was classified as critical was found in Microchip TimeProvider 4100 up to 2.4.6. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2024-7801. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-7801	Microchip TimeProvider 4100 up to 2.4.6 sql injection	A vulnerability was found in Wikimedia Cargo Extension 3.6.0 on Mediawiki and classified as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2024-47849. 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-2024-47849	Wikimedia Cargo Extension 3.6.0 on Mediawiki sql injection	A vulnerability was found in ESAFENET CDG V5. It has been rated as critical. Affected by this issue is the function delCatelogs of the file /CDGServer3/document/Catelogs;logindojojscommandDelCatelogs. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-9560. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9560	ESAFENET CDG V5 Catelogs;logindojojs delCatelogs id sql injection	A vulnerability which was classified as critical was found in TS Poll Plugin up to 2.3.9 on WordPress. Affected is an unknown function. The manipulation of the argument orderby	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		leads to sql injection. This vulnerability is traded as CVE-2024-9022. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2024-9022	TS Poll Plugin up to 2.3.9 on WordPress orderby sql injection	A vulnerability classified as critical was found in code-projects Crud Operation System 1.0. This vulnerability affects unknown code of the file delete.php. The manipulation of the argument sid leads to sql injection. This vulnerability was named CVE-2024-9812. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9812	code-projects Crud Operation System 1.0 delete.php sid sql injection	A vulnerability classified as critical has been found in code-projects Restaurant Reservation System 1.0. This affects an unknown part of the file filter3.php. The manipulation of the argument company leads to sql injection. This vulnerability is uniquely identified as CVE-2024-9811. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9811	code-projects Restaurant Reservation System 1.0 filter3.php company sql injection	A vulnerability has been found in LyLme_spage 1.9.5 and classified as critical. This vulnerability affects unknown code of the file /admin/tag.php. The manipulation of the argument id leads to sql injection.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability was named CVE-2024-9788. 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-2024-9788	LyLme_spage 1.9.5 /admin/tag.php id sql injection	A vulnerability which was classified as critical was found in code-projects Blood Bank System 1.0. Affected is an unknown function of the file register.php. The manipulation of the argument user leads to sql injection. This vulnerability is traded as CVE-2024-9797. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9797	code-projects Blood Bank System 1.0 register.php user sql injection	A vulnerability was found in code-projects Blood Bank System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/campsdetails.php. The manipulation of the argument hospital leads to sql injection. This vulnerability was named CVE-2024-9804. The attack can be initiated remotely. Furthermore there is an exploit available. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2024-9804	code-projects Blood Bank System 1.0	A vulnerability was found in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	/admin/campsdetails.php hospital sql injection	SourceCodester Online Eyewear Shop 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/pageproducts/view_product. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-9808. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2024-9808	SourceCodester Online Eyewear Shop 1.0 id sql injection	A vulnerability classified as critical has been found in WP-Advanced-Search Plugin up to 3.3.9.1 on WordPress. Affected is an unknown function. The manipulation of the argument t leads to sql injection. This vulnerability is traded as CVE-2024-9796. 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-2024-9796	WP-Advanced-Search Plugin up to 3.3.9.1 on WordPress t sql injection	A vulnerability was found in TI WooCommerce Wishlist Plugin up to 2.8.2 on WordPress. It has been classified as critical. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2024-9156. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-9156	TI WooCommerce Wishlist Plugin up to 2.8.2 on WordPress sql injection	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0. It has been declared as critical. Affected by this vulnerability is the function delete_product of the file /classes/Master.phpfdelete_product. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2024-9809. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9809	SourceCodester Online Eyewear Shop 1.0 Master.php delete_product id sql injection	A vulnerability was found in LyLme_spage 1.9.5 and classified as critical. This issue affects some unknown processing of the file /admin/apply.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-9789. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-9789	LyLme_spage 1.9.5 /admin/apply.php id sql injection	A vulnerability classified as critical has been found in SourceCodester Online Veterinary Appointment System 1.0. Affected is an unknown function of the file /admin/categories/ma	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		nage_category.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-9818. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2024-9818	SourceCodester Online Veterinary Appointment System 1.0 manage_category.php id sql injection	A vulnerability which was classified as critical has been found in Codezips Pharmacy Management System 1.0. This issue affects some unknown processing of the file product/register.php. The manipulation of the argument category leads to sql injection. The identification of this vulnerability is CVE-2024-9813. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9813	Codezips Pharmacy Management System 1.0 product/register.php category sql injection	A vulnerability was found in code-projects Blood Bank System 1.0. It has been classified as critical. This affects an unknown part of the file /update.php. The manipulation of the argument name leads to sql injection. This vulnerability is uniquely identified as CVE-2024-9817. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9817	code-projects Blood Bank System 1.0 /update.php name sql injection	A vulnerability was found in LyLme_spage 1.9.5. It has been classified as critical. Affected is an unknown function of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/admin/sou.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-9790. It is possible to launch the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-9790	LyLme_spage 1.9.5 /admin/sou.php id sql injection	A vulnerability which was classified as critical was found in Codezips Pharmacy Management System 1.0. Affected is an unknown function of the file product/update.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-9814. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9814	Codezips Pharmacy Management System 1.0 product/update.php id sql injection	A vulnerability was found in taskmatic 1.0. It has been classified as critical. Affected is an unknown function of the file /update-employee.php. The manipulation of the argument admin_id leads to sql injection. This vulnerability is traded as CVE-2024-48813. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-10021	taskmatic 1.0	A vulnerability which	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	/update-employee.php admin_id sql injection	was classified as critical was found in code-projects Blood Bank System 1.0. Affected is an unknown function of the file reset.php. The manipulation of the argument useremail leads to sql injection. This vulnerability is traded as CVE-2024-9894. It is possible to launch the attack remotely. Furthermore there is an exploit available.	core rule	
CVE-2024-10022	code-projects Blood Bank System 1.0 reset.php useremail sql injection	A vulnerability has been found in HuangDou UTCMS V9 and classified as critical. This vulnerability affects the function RunSql of the file app/modules/ut-data/admin/sql.php. The manipulation of the argument sql leads to sql injection. This vulnerability was named CVE-2024-9918. The attack can be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-10023	HuangDou UTCMS V9 sql.php RunSql sql sql injection	A vulnerability which was classified as critical has been found in HuangDou UTCMS V9. Affected by this issue is some unknown functionality of the file app/modules/ut-cac/admin/cli.php. The manipulation of the argument o leads to os command injection. This vulnerability is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		handled as CVE-2024-9916. The attack may be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-10069	HuangDou UTCMS V9 cli.php o os command injection	A vulnerability which was classified as critical has been found in SourceCodester Online Eyewear Shop 1.0. This issue affects some unknown processing of the file /admin/pageinventory/view_inventory&id2. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-9905. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-10070	SourceCodester Online Eyewear Shop 1.0 id sql injection	A vulnerability was found in Centreon BI Server up to 22.10.10/23.04.10/23.10.7/24.04.2. It has been declared as critical. This vulnerability affects unknown code of the component centreon-bi-server. The manipulation leads to sql injection. This vulnerability was named CVE-2024-45754. 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-2024-10071	Centreon BI Server	A vulnerability has	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	up to 22.10.10/23.04.10/23.10.7/24.04.2 centreon-bi-server sql injection	been found in Cloudlog 2.6.15 and classified as critical. This vulnerability affects unknown code of the file Oqrs.php. The manipulation of the argument station_id/callsign leads to sql injection. This vulnerability was named CVE-2024-48259. Access to the local network is required for this attack. There is no exploit available.	core rule	
CVE-2024-10129	Cloudlog 2.6.15 Oqrs.php station_id/callsign sql injection	A vulnerability which was classified as critical has been found in netease-youdao QAnything up to 1.4.1. This issue affects the function get_knowledge_base_name/from_status_to_status/delete_files/get_file_by_status. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2024-7099. 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-2024-10131	netease-youdao QAnything up to 1.4.1 sql injection	A vulnerability classified as problematic has been found in Teamplus Technology Team+ 13.5.x. This affects an unknown part of the component System Files Handler. The manipulation leads to relative path traversal. This vulnerability is uniquely identified as CVE-2024-9922. It is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-10133	Teamplus Technology Team+ 13.5.x System Files path traversal	A vulnerability which was classified as critical has been found in DrayTek Vigor3900 1.5.1.3. Affected by this issue is the function get_subconfig of the file mainfunction.cgi. The manipulation leads to command injection. This vulnerability is handled as CVE-2024-48153. The attack needs to be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-10134	DrayTek Vigor3900 1.5.1.3 mainfunction.cgi get_subconfig command injection	A vulnerability was found in Moxa EDR-8010 EDR-G9004 EDR-G9010 EDF-G1002-BP NAT-102 OnCell G4302-LTE4 and TN-4900. It has been classified as critical. This affects an unknown part. The manipulation leads to os command injection. This vulnerability is uniquely identified as CVE-2024-9139. 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-2024-10135	Moxa TN-4900 prior 3.12.1 os command injection	A vulnerability was found in Cloudlog 2.6.15 and classified as critical. This issue affects the function get_station_info of the file Oqrs.php. The manipulation of the argument station_id leads to sql injection. The identification of this vulnerability is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2024-48255. Access to the local network is required for this attack to succeed. There is no exploit available.		
CVE-2024-10138	Cloudlog 2.6.15 Oqrs.php get_station_info station_id sql injection	A vulnerability classified as problematic has been found in Schweizerische Steuerkonferenz Library taxstatement.jar 2.2.2/2.2.4 on Windows. Affected is the function DocumentBuilder of the component PDF Handler. The manipulation leads to xml external entity reference. This vulnerability is traded as CVE-2024-8602. The attack can only be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2024-10139	Schweizerische Steuerkonferenz Library taxstatement.jar 2.2.2/2.2.4 on Windows PDF DocumentBuilder xml external entity reference	A vulnerability classified as critical was found in Jepaas 7.2.8. This vulnerability affects unknown code of the file /homePortal/loadUserMsg. The manipulation of the argument orderSQL leads to sql injection. This vulnerability was named CVE-2024-46535. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-10140	Jepaas 7.2.8 /homePortal/loadUserMsg orderSQL sql injection	A vulnerability was found in Splunk Enterprise and Cloud Platform and classified	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		as problematic. This issue affects some unknown processing of the component KVStore. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-45737. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-10153	Splunk Enterprise/Cloud Platform prior 9.1.6/9.2.3/9.3.1 KVStore cross-site request forgery (SVD-2024-1007 / Nessus ID 208939)	A vulnerability which was classified as critical was found in Cloudlog 2.6.15. This affects the function delete_oqrs_line of the file Oqrs.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-48253. The attack needs to be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-10156	Cloudlog 2.6.15 Oqrs.php delete_oqrs_line id sql injection	A vulnerability was found in Wavelog 1.8.5. It has been classified as critical. Affected is the function get_band_confirmed of the file Activated_gridmap_model.php. The manipulation of the argument band/sat/propagation/mode leads to sql injection. This vulnerability is traded as CVE-2024-48251. The attack needs to be approached within the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		local network. There is no exploit available.		
CVE-2024-10160	Wavelog 1.8.5 Activated_gridmap_model.php get_band_confirmed band/sat/propagation/mode sql injection	A vulnerability was found in Splunk Enterprise up to 9.1.5/9.2.2/9.3.0 on Windows. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to relative path traversal. This vulnerability was named CVE-2024-45731. 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-2024-10163	Splunk Enterprise up to 9.1.5/9.2.2/9.3.0 on Windows path traversal (SVD-2024-1001)	A vulnerability which was classified as critical has been found in Netgear R7000 1.0.11.136. Affected by this issue is some unknown functionality of the file RMT_invite.cgi. The manipulation of the argument device_name2 leads to command injection. This vulnerability is handled as CVE-2024-35520. Access to the local network is required for this attack. There is no exploit available.	Patched by core rule	Y
CVE-2024-10171	Netgear R7000 1.0.11.136 RMT_invite.cgi device_name2 command injection (PSV-2023-0154)	A vulnerability which was classified as critical was found in MitraStar GPT-2541GNAC BR_g5.6_1.11b26. Affected is an unknown function of the file /cgi-bin/settings-firewall.cgi of the component Firewall Settings Page. The manipulation of the argument	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		SrcInterface leads to os command injection. This vulnerability is traded as CVE-2024-9977. It is possible to launch the attack remotely. Furthermore there is an exploit available. We tried to contact the vendor early about the disclosure but the official mail address was not working properly.		
CVE-2024-10196	MitraStar GPT-2541GNAC BR_g5.6_1.11(WVK.0)b26 Firewall Settings Page settings-firewall.cgi SrcInterface os command injection	A vulnerability was found in PHPGurukul User Registration & Login and User Management System 3.2. It has been classified as critical. Affected is an unknown function of the file /admin/search-result.php. The manipulation of the argument searchkey leads to sql injection. This vulnerability is traded as CVE-2024-48283. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-10277	PHPGurukul User Registration & Login and User Management System /admin/search-result.php sql injection	A vulnerability was found in Netgear EX6120 EX6100 and EX3700. It has been rated as critical. This issue affects some unknown processing of the file operating_mode.cgi. The manipulation of the argument ap_mode leads to command injection. The identification of this vulnerability is CVE-2024-35519. The attack can only be initiated within the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		local network. There is no exploit available.		
CVE-2024-10279	Netgear EX6120/EX6100/EX3700 operating_mode.cgi ap_mode command injection	A vulnerability which was classified as problematic was found in Forminator Forms Plugin up to 1.35.1 on WordPress. Affected is an unknown function of the component Draft Quiz Creation. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-9351. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-10349	Forminator Forms Plugin up to 1.35.1 on WordPress Draft Quiz Creation cross-site request forgery	A vulnerability was found in LiteSpeed Technologies LiteSpeed Cache Plugin up to 6.4.1 on WordPress and classified as critical. Affected by this issue is some unknown functionality. The manipulation leads to relative path traversal. This vulnerability is handled as CVE-2024-47637. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-10350	LiteSpeed Technologies LiteSpeed Cache Plugin up to 6.4.1 on WordPress path traversal	A vulnerability was found in James Park Analyse Uploads Plugin up to 0.5 on WordPress. It has been classified as problematic. This affects an unknown part. The manipulation leads to relative path traversal. This vulnerability is uniquely identified as CVE-2024-49253. It is possible to initiate the attack remotely. There	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		is no exploit available.		
CVE-2024-10354	James Park Analyse Uploads Plugin up to 0.5 on WordPress path traversal	A vulnerability was found in Limb Gallery Plugin up to 1.5.7 on WordPress. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to path traversal: &039;.../...//&039;. The identification of this vulnerability is CVE-2024-49258. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-10376	Limb Gallery Plugin up to 1.5.7 on WordPress path traversal	A vulnerability which was classified as critical has been found in Ahime Image Printer Plugin up to 1.0.0 on WordPress. Affected by this issue is some unknown functionality. The manipulation leads to path traversal. This vulnerability is handled as CVE-2024-49245. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-10377	Ahime Image Printer Plugin up to 1.0.0 on WordPress path traversal	A vulnerability classified as critical has been found in ESAFENET CDG 5. This affects the function actionPolicyPush of the file /com/esafenet/policy/action/PolicyPushControlAction.java. The manipulation of the argument policyId leads to sql injection. This vulnerability is uniquely identified as CVE-2024-10070. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-30160	ESAFENET CDG 5 PolicyPushControlAction.java actionPolicyPush policyId sql injection	A vulnerability classified as critical was found in ESAFENET CDG 5. This vulnerability affects the function actionUpdateEncryptPolicyEdit of the file /com/esafenet/servlet/policy/EncryptPolicyService.java. The manipulation of the argument encryptPolicyId leads to sql injection. This vulnerability was named CVE-2024-10071. The attack can be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-35517	ESAFENET CDG 5 EncryptPolicyService.java actionUpdateEncryptPolicyEdit encryptPolicyId sql injection	A vulnerability was found in ESAFENET CDG 5. It has been rated as critical. Affected by this issue is the function actionPassMainApplication of the file /com/esafenet/servlet/client/MailDecryptApplicationService.java. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-10069. The attack may be launched remotely. Furthermore there is an exploit available. The vendor was	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		contacted early about this disclosure but did not respond in any way.		
CVE-2024-44414	ESAFENET CDG 5 MailDecryptApplicationService.java actionPassMainApplication id sql injection	A vulnerability which was classified as critical has been found in ESAFENET CDG 5. This issue affects the function actionAddEncryptPolicyGroup of the file /com/esafenet/servlet/policy/EncryptPolicyService.java. The manipulation of the argument checklist leads to sql injection. The identification of this vulnerability is CVE-2024-10072. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-46535	ESAFENET CDG 5 EncryptPolicyService.java actionAddEncryptPolicyGroup checklist sql injection	A vulnerability was found in ESAFENET CDG 5 and classified as critical. Affected by this issue is the function connectLogout of the file /com/esafenet/servlet/ajax/MultiServerAjax.java. The manipulation of the argument servername leads to sql injection. This vulnerability is handled as CVE-2024-10134. The attack may be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		way.		
CVE-2024-48120	ESAFENET CDG 5 MultiServerAjax.java connectLogout servername sql injection	A vulnerability was found in Codezips Sales Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file deletecustcom.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2024-10165. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-48213	Codezips Sales Management System 1.0 deletecustcom.php id sql injection	A vulnerability classified as critical was found in PHPGurukul Boat Booking System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/profile.php of the component My Profile Page. The manipulation of the argument sadminusername/fullname/emailid/mobilenumber leads to sql injection. This vulnerability is known as CVE-2024-10159. The attack can be launched remotely. Furthermore there is an exploit available. The initial researcher advisory only mentions the parameter "mobilenumber" to be affected. But it must be assumed that other parameters are affected as well.	Patched by core rule	Y
CVE-2024-48222	PHPGurukul Boat Booking System 1.0	A vulnerability was found in ESAFENET	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	My Profile Page /admin/profile.php sadminusername/fullname/emailid/mobilenumber sql injection	CDG 5. It has been classified as critical. This affects the function actionDelNetSecConfig of the file /com/esafenet/servlet/netSec/NetSecConfigService.java. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-10135. It is possible to initiate the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-48233	ESAFENET CDG 5 NetSecConfigService.java actionDelNetSecConfig id sql injection	A vulnerability has been found in ESAFENET CDG 5 and classified as critical. Affected by this vulnerability is the function updateNetSecPolicyPriority of the file /com/esafenet/servlet/ajax/NetSecPolicyAjax.java. The manipulation of the argument id/frontId leads to sql injection. This vulnerability is known as CVE-2024-10133. The attack can be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-48249	ESAFENET CDG 5 NetSecPolicyAjax.java	A vulnerability was found in code-projects Pharmacy	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	updateNetSecPolicy Priority id/frontId sql injection	Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /manage_medicine.phpactiondelete. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-10137. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-48278	code-projects Pharmacy Management System 1.0 manage_medicine.php?action=delete id sql injection	A vulnerability classified as critical has been found in code-projects Pharmacy Management System 1.0. Affected is an unknown function of the file /add_new_purchase.phpactionis_supplier. The manipulation of the argument name leads to sql injection. This vulnerability is traded as CVE-2024-10138. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-48280	code-projects Pharmacy Management System 1.0 add_new_purchase.php?action=is_supplier name sql injection	A vulnerability was found in Codezips Sales Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file checkuser.php. The manipulation of the argument name leads to sql injection. This vulnerability is handled as CVE-2024-10166. The attack may be launched remotely. Furthermore there is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		an exploit available.		
CVE-2024-48282	Codezips Sales Management System 1.0 checkuser.php name sql injection	A vulnerability which was classified as critical has been found in code-projects Pharmacy Management System 1.0. Affected by this issue is some unknown functionality of the file /manage_supplier.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-10140. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-48343	code-projects Pharmacy Management System 1.0 /manage_supplier.php id sql injection	A vulnerability classified as critical was found in code-projects Pharmacy Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /add_new_supplier.php. The manipulation of the argument name leads to sql injection. This vulnerability is known as CVE-2024-10139. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-48396	code-projects Pharmacy Management System 1.0 /add_new_supplier.php name sql injection	A vulnerability was found in PHPGurukul Boat Booking System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/password-recovery.php of the component Reset Your Password Page. The manipulation of the argument username leads to sql injection.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The identification of this vulnerability is CVE-2024-10157. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-48570	PHPGurukul Boat Booking System 1.0 Reset Your Password Page password-recovery.php username sql injection	A vulnerability was found in PHPGurukul Boat Booking System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file status.php of the component Check Booking Status Page. The manipulation of the argument emailid leads to sql injection. This vulnerability is handled as CVE-2024-10154. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-48579	PHPGurukul Boat Booking System 1.0 Check Booking Status Page status.php emailid sql injection	A vulnerability which was classified as critical was found in code-projects Blood Bank System up to 1.0. Affected is an unknown function of the file /admin/massage.php. The manipulation of the argument bid leads to sql injection. This vulnerability is traded as CVE-2024-10171. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-48630	code-projects Blood Bank System up to 1.0 /admin/massage.php bid sql injection	A vulnerability classified as critical was found in code-projects Hospital Management System 1.0. This vulnerability affects unknown code of the file change-password.php. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument cpass leads to sql injection. This vulnerability was named CVE-2024-10169. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-48631	code-projects Hospital Management System 1.0 change-password.php cpass sql injection	A vulnerability has been found in PHPGurukul Boat Booking System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file book-boat.phpbid1 of the component Book a Boat Page. The manipulation of the argument nopeople leads to sql injection. This vulnerability is known as CVE-2024-10153. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-48632	PHPGurukul Boat Booking System 1.0 Book a Boat Page book-boat.php?bid=1 nopeople sql injection	A vulnerability was found in PHPGurukul Boat Booking System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/index.php of the component Sign In Page. The manipulation of the argument username leads to sql injection. This vulnerability was named CVE-2024-10156. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-48635	PHPGurukul Boat Booking System 1.0 Sign In Page /admin/index.php username sql	A vulnerability was found in code-projects Pharmacy Management System 1.0. It has been	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	declared as critical. This vulnerability affects unknown code of the file /manage_invoice.php. The manipulation of the argument invoice_number leads to sql injection. This vulnerability was named CVE-2024-10136. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-48638	code-projects Pharmacy Management System 1.0 /manage_invoice.php invoice_number sql injection	A vulnerability classified as critical has been found in Codezips Sales Management System 1.0. This affects an unknown part of the file deletecustind.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-10167. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-48652	Codezips Sales Management System 1.0 deletecustind.php id sql injection	A vulnerability was found in code-projects Pharmacy Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /add_new_invoice.php. The manipulation of the argument text leads to sql injection. The identification of this vulnerability is CVE-2024-10196. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-49244	code-projects Pharmacy	A vulnerability classified as critical was	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Management System 1.0 /add_new_invoice.php text sql injection	found in PHPGurukul Medical Card Generation System 1.0. This vulnerability affects unknown code of the file /admin/view-card-detail.php of the component Managecard View Detail Page. The manipulation of the argument viewid leads to sql injection. This vulnerability was named CVE-2024-10299. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-5429	PHPGurukul Medical Card Generation System 1.0 Managecard View Detail Page view-card-detail.php viewid sql injection	A vulnerability classified as critical has been found in funadmin 5.0.2. This affects the function index of the file \backend\controller\auth\Auth.php. The manipulation of the argument parentField leads to sql injection. This vulnerability is uniquely identified as CVE-2024-48230. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-9894	funadmin 5.0.2 Auth.php index parentField sql injection	A vulnerability has been found in funadmin 5.0.2 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /curd/table/edit. The manipulation leads to sql injection. This vulnerability is known as CVE-2024-48222. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-9918	funadmin 5.0.2 /curd/table/edit sql injection	A vulnerability was found in funadmin 5.0.2. It has been classified as critical. This affects an unknown part of the component Curd One Click Command Mode Plugin. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2024-48229. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-9952	funadmin 5.0.2 Curd One Click Command Mode Plugin sql injection	A vulnerability was found in ESAFENET CDG 5 and classified as critical. This issue affects some unknown processing of the file dataSearch.jsp. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-48343. The attack can only be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-9986	ESAFENET CDG 5 dataSearch.jsp id sql injection	A vulnerability was found in ESAFENET CDG 5 and classified as critical. This issue affects some unknown processing of the file dataSearch.jsp. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-48343. The attack can only be initiated within the local network. There is no exploit available.	Patched by core rule	Y

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-47075	LayUI up to 2.9.16 img Tag name cross site scripting (GHSA-j827-6rgf-9629)	A vulnerability was found in LayUI up to 2.9.16. It has been rated as problematic. Affected by this issue is some unknown functionality of the component img Tag Handler. The manipulation of the argument name leads to cross site scripting. This vulnerability is handled as CVE-2024-47075. 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-2024-6517	Contact Form 7 Math Captcha Plugin up to 2.0.1 on WordPress cross site scripting	A vulnerability has been found in Contact Form 7 Math Captcha Plugin up to 2.0.1 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-6517. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40512	openPetra 2023.02 serverMReporting.asmx cross site scripting	A vulnerability was found in openPetra 2023.02. It has been classified as problematic. Affected is an unknown function of the file serverMReporting.asmx. The manipulation leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is traded as CVE-2024-40512. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2024-40511	openPetra 2023.02 serverMServerAdmin.asmx cross site scripting	A vulnerability was found in openPetra 2023.02 and classified as problematic. This issue affects some unknown processing of the file serverMServerAdmin.asmx. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-40511. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-46333	Piwigo 14.5.0 Add Album Album Name cross site scripting	A vulnerability was found in Piwigo 14.5.0. It has been classified as problematic. Affected is an unknown function of the component Add Album Handler. The manipulation of the argument Album Name leads to cross site scripting. This vulnerability is traded as CVE-2024-46333. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-9291	kalvinGit kvf-admin up to f12a94dc1ebb7d1c51ee978a85e4c7ed75c620ff XML File upfile cross site scripting	A vulnerability classified as problematic has been found in kalvinGit kvf-admin up to f12a94dc1ebb7d1c51ee978a85e4c7ed75c620ff. Affected is an unknown function of the file /ueditor/uploadconfigPathueditor/config.json &actionuploadfile	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the component XML File Handler. The manipulation of the argument upfile leads to cross site scripting. This vulnerability is traded as CVE-2024-9291. It is possible to launch the attack remotely. Furthermore there is an exploit available. The GitHub repository of the project did not receive an update for more than two years. This product is using a rolling release to provide continious delivery. Therefore no version details for affected nor updated releases are available.		
CVE-2024-9279	funnyzpc Mee-Admin up to 1.6 User Center /mee/index User Nickname cross site scripting	A vulnerability which was classified as problematic was found in funnyzpc Mee-Admin up to 1.6. This affects an unknown part of the file /mee/index of the component User Center. The manipulation of the argument User Nickname leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-9279. It is possible to initiate the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-40507	openPetra 2023.02 serverMPersonnel.asmx cross site	A vulnerability was found in openPetra 2023.02. It has been	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	scripting	classified as problematic. This affects an unknown part of the file serverMPersonnel.asmx. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-40507. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-45986	projectworlds Online Voting System 1.0 voter.php cross site scripting	A vulnerability classified as problematic was found in projectworlds Online Voting System 1.0. This vulnerability affects unknown code of the file voter.php. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-45986. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-25412	Flatpress 1.3 email cross site scripting	A vulnerability was found in Flatpress 1.3. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument email leads to cross site scripting. This vulnerability is known as CVE-2024-25412. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-25411	Flatpress 1.3 setup.php username cross site scripting	A vulnerability has been found in Flatpress 1.3 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		setup.php. The manipulation of the argument username leads to cross site scripting. This vulnerability is known as CVE-2024-25411. The attack can be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.		
CVE-2024-9300	SourceCodester Online Railway Reservation System 1.0 Message Us Form contact_us.php fullname/email/message cross site scripting	A vulnerability classified as problematic was found in SourceCodester Online Railway Reservation System 1.0. This vulnerability affects unknown code of the file contact_us.php of the component Message Us Form. The manipulation of the argument fullname/email/message leads to cross site scripting. This vulnerability was named CVE-2024-9300. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9299	SourceCodester Online Railway Reservation System 1.0 /?page=reserve First Name/Middle Name/Last Name cross site scripting	A vulnerability classified as problematic has been found in SourceCodester Online Railway Reservation System 1.0. This affects an unknown part of the file /pagereserve. The manipulation of the argument First Name/Middle Name/Last Name leads to cross site scripting. This vulnerability is uniquely identified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2024-9299. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-40508	openPetra 2023.02 serverMConference.asmx cross site scripting	A vulnerability was found in openPetra 2023.02. It has been rated as problematic. This issue affects some unknown processing of the file serverMConference.asmx. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-40508. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40506	openPetra 2023.02 serverMHospitality.asmx cross site scripting	A vulnerability was found in openPetra 2023.02. It has been declared as problematic. This vulnerability affects unknown code of the file serverMHospitality.asmx. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-40506. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40509	openPetra 2023.02 serverMFinDev.asmx cross site scripting	A vulnerability was found in openPetra 2023.02. It has been classified as problematic. This affects an unknown part of the file serverMFinDev.asmx. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-40509. It is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-9323	SourceCodester Inventory Management System 1.0 add_staff.php cross site scripting	A vulnerability was found in SourceCodester Inventory Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /app/action/add_staff.php. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-9323. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9320	SourceCodester Online Timesheet App 1.0 Add Timesheet Form add-timesheet.php day/task cross site scripting	A vulnerability has been found in SourceCodester Online Timesheet App 1.0 and classified as problematic. This vulnerability affects unknown code of the file /endpoint/add-timesheet.php of the component Add Timesheet Form. The manipulation of the argument day/task leads to cross site scripting. This vulnerability was named CVE-2024-9320. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-46453	iq3xcite up to 3.05 /test/ cross site scripting	A vulnerability which was classified as problematic was found in iq3xcite up to 3.05. Affected is an unknown function of the file /test/. The manipulation leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is traded as CVE-2024-46453. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2024-8283	10Web Slider Plugin up to 1.2.58 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic was found in 10Web Slider Plugin up to 1.2.58 on WordPress. This affects an unknown part of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-8283. 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-2024-3635	Post Grid Plugin up to 7.4.x on WordPress Setting cross site scripting	A vulnerability classified as problematic was found in Post Grid Plugin up to 7.4.x on WordPress. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-3635. 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-2024-47536	StarCitizenTools mediawiki-skins-Citizen up to 2.30.x Setting real name	A vulnerability has been found in StarCitizenTools mediawiki-skins-Citizen	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	cross site scripting (GHSA-62r2-gcxr-426x)	up to 2.30.x and classified as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation of the argument real name leads to basic cross site scripting. This vulnerability was named CVE-2024-47536. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-8536	Ultimate Blocks Plugin up to 3.2.1 on WordPress Block Attribute cross site scripting	A vulnerability has been found in Ultimate Blocks Plugin up to 3.2.1 on WordPress and classified as problematic. This vulnerability affects unknown code of the component Block Attribute Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-8536. 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-2024-8239	Starbox Plugin up to 3.5.2 on WordPress Shortcode cross site scripting	A vulnerability which was classified as problematic has been found in Starbox Plugin up to 3.5.2 on WordPress. Affected by this issue is some unknown functionality of the component Shortcode Handler. The manipulation leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is handled as CVE-2024-8239. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-33210	flatpress 1.3 cross site scripting	A vulnerability which was classified as problematic was found in flatpress 1.3. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-33210. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-33209	FlatPress 1.3 Add New Entry Section cross site scripting	A vulnerability which was classified as problematic has been found in FlatPress 1.3. This issue affects some unknown processing of the component Add New Entry Section. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-33209. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-31835	flatpress CMS 1.3 file name cross site scripting	A vulnerability classified as problematic was found in flatpress CMS 1.3. This vulnerability affects unknown code. The manipulation of the argument file name leads to cross site scripting. This vulnerability was named CVE-2024-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		31835. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-46077	itsourcecode Online Tours and Travels Management System 1.0 travellers.php cross site scripting	A vulnerability which was classified as problematic has been found in itsourcecode Online Tours and Travels Management System 1.0. This issue affects some unknown processing of the file travellers.php. The manipulation of the argument val-username/val-email/val-suggestions/val-digits/state_name leads to cross site scripting. The identification of this vulnerability is CVE-2024-46077. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-47840	Wikimedia Apex Skin Extension up to 1.39.8/1.41.2/1.42.1 on Mediawiki cross site scripting	A vulnerability has been found in Wikimedia Apex Skin Extension up to 1.39.8/1.41.2/1.42.1 on Mediawiki and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-47840. 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-2024-43687	Microchip TimeProvider 4100 up to 2.4.6 Banner	A vulnerability which was classified as problematic was found	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Config Module cross site scripting	in Microchip TimeProvider 4100 up to 2.4.6. Affected is an unknown function of the component Banner Config Module. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-43687. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-47847	Wikimedia Cargo Extension 3.6.0 on Mediawiki cross site scripting	A vulnerability was found in Wikimedia Cargo Extension 3.6.0 on Mediawiki. 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-2024-47847. 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-2024-45932	Krayin CRM 1.3.0 2 organization name cross site scripting	A vulnerability was found in Krayin CRM 1.3.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/contacts/organizations/edit/2. The manipulation of the argument organization name leads to cross site scripting. This vulnerability is handled as CVE-2024-45932. The attack may	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		be launched remotely. There is no exploit available.		
CVE-2024-46300	itsourcecode Placement Management System 1.0 registration.php Full Name cross site scripting	A vulnerability which was classified as problematic has been found in itsourcecode Placement Management System 1.0. Affected by this issue is some unknown functionality of the file registration.php. The manipulation of the argument Full Name leads to cross site scripting. This vulnerability is handled as CVE-2024-46300. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-43362	Cacti up to 1.2.27 HTTP POST Request links.php fileurl cross site scripting (GHSA-wh9c-v56x-v77c)	A vulnerability was found in Cacti up to 1.2.27. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file links.php of the component HTTP POST Request Handler. The manipulation of the argument fileurl leads to cross site scripting. This vulnerability is known as CVE-2024-43362. 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-2024-43365	Cacti up to 1.2.27 HTTP POST Request links.php consolenewsection cross site scripting (GHSA-49f2-hwx9-qffr)	A vulnerability classified as problematic has been found in Cacti up to 1.2.27. This affects an unknown part of the file links.php of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component HTTP POST Request Handler. The manipulation of the argument consolenewsection leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-43365. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-43364	Cacti up to 1.2.27 HTTP POST Request links.php title cross site scripting (GHSA-fgc6-g8gc-wcg5)	A vulnerability was found in Cacti up to 1.2.27. It has been rated as problematic. Affected by this issue is some unknown functionality of the file links.php of the component HTTP POST Request Handler. The manipulation of the argument title leads to cross site scripting. This vulnerability is handled as CVE-2024-43364. 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-2024-46410	PublicCMS 4.0.202406.d Category Management cross site scripting	A vulnerability classified as problematic has been found in PublicCMS 4.0.202406.d. Affected is an unknown function of the component Category Management. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-46410. It is possible to launch the attack	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remotely. There is no exploit available.		
CVE-2024-46237	PHPGurukul Hospital Management System 4.0 doctor/add-patient.php patname/pataddress cross site scripting	A vulnerability which was classified as problematic has been found in PHPGurukul Hospital Management System 4.0. This issue affects some unknown processing of the file doctor/add-patient.php. The manipulation of the argument patname/pataddress leads to cross site scripting. The identification of this vulnerability is CVE-2024-46237. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-8187	Smart Post Show Plugin up to 3.0.0 on WordPress Pagination Color cross site scripting	A vulnerability has been found in Smart Post Show Plugin up to 3.0.0 on WordPress and classified as problematic. This vulnerability affects unknown code of the component Pagination Color Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-8187. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-9807	Craig Rodway Classroombookings 2.8.7 Session Page /sessions Name cross site scripting	A vulnerability was found in Craig Rodway Classroombookings 2.8.7 and classified as problematic. This issue affects some unknown processing of the file /sessions of the component Session Page. The manipulation of the argument Name 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-2024-9807. The attack may be initiated remotely. There is no exploit available. The project maintainer was contacted early about the disclosure. He responded very quickly friendly and professional. It is recommended to upgrade the affected component.		
CVE-2024-9803	code-projects Blood Bank Management System 1.0 blooddetails.php Availibility cross site scripting	A vulnerability was found in code-projects Blood Bank Management System 1.0. It has been classified as problematic. This affects an unknown part of the file blooddetails.php. The manipulation of the argument Availibility leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-9803. It is possible to initiate the attack remotely. Furthermore there is an exploit available. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2024-9805	code-projects Blood Bank System 1.0 /admin/campsdetails.php hospital/address/city/contact cross site scripting	A vulnerability was found in code-projects Blood Bank System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/campsdetails.php. The manipulation of the argument hospital/address/city/contact 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-2024-9805. The attack may be initiated remotely. Furthermore there is an exploit available. The initial researcher advisory only mentions the parameter "hospital".		
CVE-2024-9799	SourceCodester Profile Registration without Reload Refresh 1.0 add.php cross site scripting	A vulnerability has been found in SourceCodester Profile Registration without Reload Refresh 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file add.php. The manipulation of the argument email_address/address/company_name/job_title/jobDescriptionparameter leads to cross site scripting. This vulnerability is known as CVE-2024-9799. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-9810	SourceCodester Record Management System 1.0 sort2_user.php qualification cross site scripting	A vulnerability was found in SourceCodester Record Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file sort2_user.php. The manipulation of the argument qualification leads to cross site scripting. This vulnerability is handled as CVE-2024-9810. The attack may be launched remotely.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Furthermore there is an exploit available.		
CVE-2024-9806	Craig Rodway Classroombookings up to 2.8.6 Room Page /rooms/fields Name cross site scripting	A vulnerability has been found in Craig Rodway Classroombookings up to 2.8.6 and classified as problematic. This vulnerability affects unknown code of the file /rooms/fields of the component Room Page. The manipulation of the argument Name leads to cross site scripting. This vulnerability was named CVE-2024-9806. The attack can be initiated remotely. Furthermore there is an exploit available. The project maintainer was contacted early about the disclosure. He responded very quickly friendly and professional. It is recommended to upgrade the affected component.	Patched by core rule	Y
CVE-2016-15041	OpenHIS 1.0 PayController.class.php refund sql injection	A vulnerability classified as critical has been found in OpenHIS 1.0. This affects the function refund of the file PayController.class.php. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2024-46532. Access to the local network is required for this attack to succeed. There is no exploit available.	Patched by core rule	Y
CVE-2024-10024	TablePress Plugin up to 2.4.2 on WordPress cross site scripting	A vulnerability was found in TablePress Plugin up to 2.4.2 on WordPress. It has been	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-9595. The attack can be launched remotely. There is no exploit available.		
CVE-2024-10072	Znuny up to 6.5.1/6.5.10/7.0.1/7.0.16 Activity Dialogues SLA cross site scripting	A vulnerability was found in Znuny up to 6.5.1/6.5.10/7.0.1/7.0.16. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Activity Dialogues. The manipulation of the argument SLA leads to cross site scripting. This vulnerability is known as CVE-2024-48937. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-10136	vTiger CRM 8.2.0 module cross site scripting	A vulnerability classified as problematic has been found in vTiger CRM 8.2.0. This affects an unknown part. The manipulation of the argument module leads to basic cross site scripting. This vulnerability is uniquely identified as CVE-2024-48119. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-10137	X2CRM 8.5 Opportunities Module Name cross site scripting	A vulnerability classified as problematic was found in X2CRM 8.5. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability affects unknown code of the component Opportunities Module. The manipulation of the argument Name leads to cross site scripting. This vulnerability was named CVE-2024-48120. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-10142	WooCommerce Plugin up to 9.0.2 on WordPress cross site scripting	A vulnerability which was classified as problematic has been found in WooCommerce Plugin up to 9.0.2 on WordPress. This issue affects some unknown processing. The manipulation leads to basic cross site scripting. The identification of this vulnerability is CVE-2024-9944. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-10154	SourceCodester Online Eyewear Shop 1.0 Contact Information Page contact_info Address cross site scripting	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0 and classified as problematic. This issue affects some unknown processing of the file /admin/pagesystem_info/contact_info of the component Contact Information Page. The manipulation of the argument Address leads to cross site scripting. The identification of this vulnerability is CVE-2024-9952. The attack may be initiated remotely. Furthermore there is an exploit	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		available. Other parameters might be affected as well.		
CVE-2024-10155	Wavelog 1.8.5 Oqrs_model.php get_worked_modes station_id sql injection	A vulnerability was found in Wavelog 1.8.5. It has been declared as critical. Affected by this vulnerability is the function get_worked_modes of the file Oqrs_model.php. The manipulation of the argument station_id leads to sql injection. This vulnerability is known as CVE-2024-48257. The attack can only be done within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-10157	eLabFTW up to 5.1.4 experiments.php cross site scripting (GHSA-cjww-pr9f-4c4w)	A vulnerability has been found in eLabFTW up to 5.1.4 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file experiments.php. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-47826. 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-2024-10159	Enalean Tuleap Community Edition/Tuleap Enterprise Edition cross site scripting	A vulnerability was found in Enalean Tuleap Community Edition and Tuleap Enterprise Edition. It has been classified as problematic. 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-2024-46980. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-10162	withastro up to 4.16.0 cross site scripting (GHSA-m85w-3h95-hcf9)	A vulnerability which was classified as problematic has been found in withastro astro up to 4.16.0. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-47885. 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-2024-10165	Splunk Enterprise/Cloud Platform Configuration File local api.uri cross site scripting (SVD-2024-1011)	A vulnerability was found in Splunk Enterprise and Cloud Platform. It has been classified as problematic. Affected is an unknown function of the file /manager/search/apps/local of the component Configuration File Handler. The manipulation of the argument api.uri leads to cross site scripting. This vulnerability is traded as CVE-2024-45741. 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
		It is recommended to upgrade the affected component.		
CVE-2024-10166	PHPGurukul User Registration & Login and User Management System /search-result.php cross site scripting	A vulnerability was found in PHPGurukul User Registration & Login and User Management System 3.2 and classified as problematic. This issue affects some unknown processing of the file /search-result.php. The manipulation of the argument searchkey leads to basic cross site scripting. The identification of this vulnerability is CVE-2024-48279. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-10167	markdown-to-jsx up to 7.3.x src cross site scripting (SNYK-JS-MARKDOWNTOJSX-6258886)	A vulnerability classified as problematic was found in markdown-to-jsx up to 7.3.x. This vulnerability affects unknown code. The manipulation of the argument src leads to cross site scripting. This vulnerability was named CVE-2024-21535. 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-2024-10169	NewType WebEIP 3.0 cross site scripting	A vulnerability classified as problematic has been found in NewType WebEIP 3.0. Affected is an unknown function. The manipulation leads to cross site scripting. NOTE: This vulnerability only affects products that	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		are no longer supported by the maintainer. This vulnerability is traded as CVE-2024-9969. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-10176	code-projects Pharmacy Management System 1.0 manage_customer.php?action=search text sql injection	A vulnerability classified as critical has been found in code-projects Pharmacy Management System 1.0. This affects an unknown part of the file /php/manage_customer.phpactionsearch. The manipulation of the argument text leads to sql injection. This vulnerability is uniquely identified as CVE-2024-9976. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-10191	ChanGate Property Management System sql injection	A vulnerability was found in ChanGate Property Management System and classified as critical. Affected by this issue is some unknown functionality. The manipulation leads to sql injection. This vulnerability is handled as CVE-2024-9972. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-10192	NVIDIA NeMo up to All versions r2.0.0rc0 Tar File Extraction SaveRestoreConnector path traversal	A vulnerability which was classified as critical has been found in NVIDIA NeMo up to All versions r2.0.0rc0. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		issue affects the function SaveRestoreConnector of the component Tar File Extraction Handler. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2024-0129. Attacking locally is a requirement. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-10197	code-projects Blood Bank Management System 1.0 member_register.php fullname/username/password/email sql injection	A vulnerability was found in code-projects Blood Bank Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file member_register.php. The manipulation of the argument fullname/username/password/email leads to sql injection. The identification of this vulnerability is CVE-2024-9986. The attack may be initiated remotely. Furthermore there is an exploit available. The initial researcher advisory only mentions the parameter "password" to be affected. But it must be assumed that other parameters are affected as well.	Patched by core rule	Y
CVE-2024-10198	Ragic Enterprise Cloud Database System Files path traversal	A vulnerability classified as problematic has been found in Ragic Enterprise Cloud Database. Affected is an unknown function of the component	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		System Files Handler. The manipulation leads to relative path traversal. This vulnerability is traded as CVE-2024-9983. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-10199	SourceCodester Online Eyewear Shop 1.0 Report Viewing Page /admin/?page=reports date sql injection	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/pagereports of the component Report Viewing Page. The manipulation of the argument date leads to sql injection. This vulnerability is traded as CVE-2024-9973. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-10278	Discount Rules for WooCommerce Plugin up to 2.6.5 on WordPress cross site scripting	A vulnerability has been found in Discount Rules for WooCommerce Plugin up to 2.6.5 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-8541. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-10335	heateor Social Sharing Plugin up to 3.3.3 on WordPress heateor_sss_sharing_count urls cross site scripting	A vulnerability classified as problematic has been found in heateor Social Sharing Plugin up to 3.3.3 on WordPress. Affected is the function heateor_sss_sharing_count. The manipulation of the argument urls leads to cross site scripting. This vulnerability is traded as CVE-2022-4971. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-10348	pickplugins Post Grid and Gutenberg Blocks Plugin up to 2.1.12 on WordPress sql injection (ID 2644269)	A vulnerability was found in pickplugins Post Grid and Gutenberg Blocks Plugin up to 2.1.12 on WordPress and classified as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2021-4450. 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-2024-10355	PeepSo Community Plugin up to 6.4.6.1 on WordPress cross site scripting	A vulnerability was found in PeepSo Community Plugin up to 6.4.6.1 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-2024-9873. The attack may be initiated	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remotely. There is no exploit available.		
CVE-2024-10368	SolarWinds Platform up to 2024.2.1 Edit cross site scripting	A vulnerability was found in SolarWinds Platform up to 2024.2.1. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Edit Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-45715. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-10369	PHPGurukul Teachers Record Management System 2.1 POST Request Parameter listed-teachers.php searchinput cross site scripting	A vulnerability was found in PHPGurukul Teachers Record Management System 2.1. It has been classified as problematic. This affects an unknown part of the file /trms/listed-teachers.php of the component POST Request Parameter Handler. The manipulation of the argument searchinput leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-48744. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-10370	SolarWinds Serv-U up to 15.4.2 HF2 cross site scripting	A vulnerability was found in SolarWinds Serv-U up to 15.4.2 HF2. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross site scripting. This vulnerability is handled as CVE-2024-45714. The attack may be launched remotely. There is no exploit available.		
CVE-2024-10378	ElementInvader Addons for Elementor Plugin up to 1.2.8 on WordPress cross site scripting	A vulnerability classified as problematic was found in ElementInvader Addons for Elementor Plugin up to 1.2.8 on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-9888. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-20269	code-projects Pharmacy Management System 1.0 add_new_medicine.php name/packing/generic_name/suppliers_name sql injection	A vulnerability classified as critical was found in code-projects Pharmacy Management System 1.0. This vulnerability affects unknown code of the file /php/add_new_medicine.php. The manipulation of the argument name/packing/generic_name/suppliers_name leads to sql injection. This vulnerability was named CVE-2024-10023. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-20364	code-projects Pharmacy Management System 1.0 manage_supplier.php?action=search text sql injection	A vulnerability classified as critical has been found in code-projects Pharmacy Management System 1.0. This affects an unknown part of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/php/manage_supplier.phpactionsearch. The manipulation of the argument text leads to sql injection. This vulnerability is uniquely identified as CVE-2024-10022. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-20377	code-projects Pharmacy Management System 1.0 text sql injection	A vulnerability was found in code-projects Pharmacy Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /php/manage_purchase.phpactionsearch&tagVOUCHER_NUMBER. The manipulation of the argument text leads to sql injection. This vulnerability is handled as CVE-2024-10021. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-10101	binary-husky gpt_academic up to 3.83 HTML File HTML injection	A vulnerability was found in binary-husky gpt_academic up to 3.83 and classified as problematic. This issue affects some unknown processing of the component HTML File Handler. The manipulation leads to HTML injection. The identification of this vulnerability is CVE-2024-10101. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-47881	comfyanonymous comfyui up to 0.2.2 API Endpoint /view	A vulnerability has been found in comfyanonymous	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	cross site scripting	comfyui up to 0.2.2 and classified as problematic. This vulnerability affects unknown code of the file /view of the component API Endpoint. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-10099. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-48049	SourceCodester Sentiment Based Movie Rating System 1.0 /msrps/movie_details.php id sql injection	A vulnerability was found in SourceCodester Sentiment Based Movie Rating System 1.0. It has been classified as critical. Affected is an unknown function of the file /msrps/movie_details.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-10163. It is possible to launch the attack remotely. Furthermore there is an exploit available. The initial researcher disclosure mentions a slightly changed product name.	Patched by core rule	Y
CVE-2024-48251	PHPGurukul Boat Booking System 1.0 Book a Boat Page book-boat.php?bid=1 phone_number cross site scripting	A vulnerability was found in PHPGurukul Boat Booking System 1.0. It has been classified as problematic. This affects an unknown part of the file book-boat.phpbid1 of the component Book a Boat Page. The manipulation of the argument phone_number leads	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to cross site scripting. This vulnerability is uniquely identified as CVE-2024-10155. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-48636	code-projects Blood Bank System 1.0 /viewrequest.php cross site scripting	A vulnerability has been found in code-projects Blood Bank System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /viewrequest.php. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-10142. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-48657	PHPGurukul IFSC Code Finder Project 1.0 search.php cross site scripting	A vulnerability has been found in PHPGurukul IFSC Code Finder Project 1.0 and classified as problematic. This vulnerability affects unknown code of the file search.php. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-10192. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-48708	PHPGurukul Boat Booking System 1.0 Booking Details Page /admin/book-details.php Official Remark cross site scripting	A vulnerability which was classified as problematic was found in PHPGurukul Boat Booking System 1.0. This affects an unknown part of the file /admin/book-details.php of the component Booking Details Page. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument Official Remark leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-10191. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-48743	code-projects Pharmacy Management System 1.0 Manage Customer Page /manage_customer.php suppliers_name/address cross site scripting	A vulnerability was found in code-projects Pharmacy Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /manage_customer.php of the component Manage Customer Page. The manipulation of the argument suppliers_name/address leads to cross site scripting. This vulnerability is known as CVE-2024-10198. The attack can be launched remotely. Furthermore there is an exploit available. The initial researcher advisory mentions contradicting files to be affected. Other parameters might be affected as well.	Patched by core rule	Y
CVE-2024-49225	code-projects Pharmacy Management System 1.0 Manage Supplier Page /manage_supplier.php address cross site scripting	A vulnerability was found in code-projects Pharmacy Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file /manage_supplier.php of the component Manage Supplier Page. The manipulation of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the argument address leads to cross site scripting. This vulnerability is traded as CVE-2024-10197. It is possible to launch the attack remotely. Furthermore there is an exploit available. Other parameters might be affected as well.		
CVE-2024-49265	Hospital Management System 1.0.0 sql injection	A vulnerability which was classified as critical has been found in Hospital Management System 1.0.0. Affected by this issue is some unknown functionality. The manipulation leads to sql injection. This vulnerability is handled as CVE-2024-48657. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-49268	Student Management System 1.0.0 cross site scripting	A vulnerability was found in Student Management System 1.0.0 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-48656. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-49279	Collabtive 3.1 name cross site scripting	A vulnerability classified as problematic was found in Collabtive 3.1. This vulnerability affects unknown code. The manipulation of the argument name leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability was named CVE-2024-46240. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-49289	Client Management System 1.0 bwdates-reports-ds.php Between Dates Reports sql injection	A vulnerability has been found in Client Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/bwdates-reports-ds.php. The manipulation of the argument Between Dates Reports leads to sql injection. This vulnerability is known as CVE-2024-48570. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-49298	Collabtive 3.1 managemessage.php title cross site scripting	A vulnerability was found in Collabtive 3.1 and classified as problematic. Affected by this issue is some unknown functionality of the file managemessage.php. The manipulation of the argument title leads to cross site scripting. This vulnerability is handled as CVE-2024-48706. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-49308	Collabtive 3.1 tasklist.php name cross site scripting	A vulnerability was found in Collabtive 3.1. It has been declared as problematic. This vulnerability affects unknown code of the file tasklist.php. The manipulation of the argument name leads	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to cross site scripting. This vulnerability was named CVE-2024-48708. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-49693	Camaleon CMS 2.7.5 content group name cross site scripting	A vulnerability was found in Camaleon CMS 2.7.5 and classified as problematic. This issue affects some unknown processing. The manipulation of the argument content group name leads to cross site scripting. The identification of this vulnerability is CVE-2024-48652. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-46482	Faveo-Helpdesk 2.0.3 Ticket Generation unrestricted upload	A vulnerability was found in Faveo-Helpdesk 2.0.3. It has been classified as critical. This affects an unknown part of the component Ticket Generation. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2024-46482. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-48448	Huly Platform 0.6.295 Tracker Comments Page unrestricted upload	A vulnerability which was classified as critical was found in Huly Platform 0.6.295. This affects an unknown part of the component Tracker Comments Page. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2024-48448. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-9856	ESAFENET CDG 5 AutoSignService.java actionPassOrNotAutoSign UniqueId sql injection	A vulnerability was found in ESAFENET CDG 5. It has been declared as critical. This vulnerability affects the function actionPassOrNotAutoSign of the file /com/esafenet/servlet/service/processsign/AutoSignService.java. The manipulation of the argument UniqueId leads to sql injection. This vulnerability was named CVE-2024-10376. The attack can be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-9905	PriPre Plugin up to 0.4.11 on WordPress SVG File Upload cross site scripting	A vulnerability was found in PriPre Plugin up to 0.4.11 on WordPress. It has been classified as problematic. This affects an unknown part of the component SVG File Upload Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-9454. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-9906	ElementsKit Elementor Addons Plugin up to 3.2.9 on WordPress Image Comparison Widget cross site scripting	A vulnerability was found in ElementsKit Elementor Addons Plugin up to 3.2.9 on WordPress and classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		problematic. Affected by this issue is some unknown functionality of the component Image Comparison Widget. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-10091. The attack may be launched remotely. There is no exploit available.		
CVE-2024-9973	Poll Maker Plugin up to 5.4.6 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic has been found in Poll Maker Plugin up to 5.4.6 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-2024-9462. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-9974	Simple News Plugin up to 2.8 on WordPress Shortcode cross site scripting	A vulnerability classified as problematic was found in Simple News Plugin up to 2.8 on WordPress. This vulnerability affects unknown code of the component Shortcode Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-10112. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-9976	FormFacade Plugin up to 1.3.6 on WordPress cross site	A vulnerability was found in FormFacade Plugin up to 1.3.6 on	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	scripting	WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-9613. The attack may be launched remotely. There is no exploit available.		

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-42640	angular-base64-upload up to 0.1.20 demo/server.php improper authentication	A vulnerability was found in angular-base64-upload up to 0.1.20. It has been classified as critical. Affected is an unknown function of the file demo/server.php. The manipulation leads to improper authentication. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability is traded as CVE-2024-42640. 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-2024-9855	07FLYCMS/07FLY-CMS/07FlyCRM 1.3.8 Module Plug-In sysmodule_1 uploadFile file unrestricted upload	A vulnerability was found in 07FLYCMS 07FLY-CMS and 07FlyCRM 1.3.8. It has been declared as critical. Affected by this vulnerability is the function uploadFile of the file /admin/SysModule/upload/ajaxmodel/upload/uploadfilepath/sysmodule_1 of the component Module Plug-In Handler. The manipulation of the argument file leads to unrestricted upload. This vulnerability is known as CVE-2024-9855. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The affected product is known with different names like 07FLYCMS 07FLY-CMS and 07FlyCRM. It was not possible to reach out to the vendor before assigning a CVE due to a not working mail address.		
CVE-2024-9904	07FLYCMS/07FLY-CMS/07FlyCRM up to 1.2.0 pictureUpload file unrestricted upload	A vulnerability classified as critical was found in 07FLYCMS 07FLY-CMS and 07FlyCRM up to 1.2.0. This vulnerability affects the function pictureUpload of the file /admin/File/pictureUpload. The manipulation of the argument file leads to unrestricted upload. This vulnerability was named CVE-2024-9904. The attack can be initiated remotely. Furthermore there is an exploit available. The affected product is known with different names like 07FLYCMS 07FLY-CMS and 07FlyCRM. It was not possible to reach out to the vendor before assigning a CVE due to a not working mail address.	Patched by custom rule	N
CVE-2024-9903	07FLYCMS/07FLY-CMS/07FlyCRM up to 1.2.0 /admin/File/fileUpload file unrestricted upload	A vulnerability classified as critical has been found in 07FLYCMS 07FLY-CMS and 07FlyCRM up to 1.2.0. This affects the function fileUpload of the file /admin/File/fileUpload. The manipulation of the argument file leads to unrestricted upload. This vulnerability is	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		uniquely identified as CVE-2024-9903. It is possible to initiate the attack remotely. Furthermore there is an exploit available. The affected product is known with different names like 07FLYCMS 07FLY-CMS and 07FlyCRM. It was not possible to reach out to the vendor before assigning a CVE due to a not working mail address.		
CVE-2024-9975	SourceCodester Drag and Drop Image Upload 1.0 /upload.php unrestricted upload	A vulnerability was found in SourceCodester Drag and Drop Image Upload 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /upload.php. The manipulation leads to unrestricted upload. This vulnerability is handled as CVE-2024-9975. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by custom rule	N
CVE-2021-4449	ZoomIt ZoomSounds Plugin up to 5.96 on WordPress savepng.php unrestricted upload	A vulnerability which was classified as critical was found in ZoomIt ZoomSounds Plugin up to 5.96 on WordPress. Affected is an unknown function of the file savepng.php. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2021-4449. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by custom rule	N
CVE-2016-15042	nmedia Frontend File Manager Plugin/Post Front-	A vulnerability was found in nmedia Frontend File Manager	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	End Form on WordPress unrestricted upload	Plugin and Post Front-End Form on WordPress. It has been classified as critical. Affected is the function nm_filemanager_upload_file/nm_postfront_upload_file. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2016-15042. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-10161	PHPGurukul Boat Booking System 1.0 Update Boat Image Page change-image.php image unrestricted upload	A vulnerability which was classified as critical was found in PHPGurukul Boat Booking System 1.0. This affects an unknown part of the file change-image.php of the component Update Boat Image Page. The manipulation of the argument image leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2024-10161. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by custom rule	N
CVE-2024-10120	wfh45678 Radar up to 1.0.8 upload file unrestricted upload	A vulnerability has been found in wfh45678 Radar up to 1.0.8 and classified as critical. This vulnerability affects unknown code of the file /services/v1/common/upload. The manipulation of the argument file leads to unrestricted upload.	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability was named CVE-2024-10120. 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-2024-37847	MangoOS up to 5.1.3 API unrestricted upload	A vulnerability was found in MangoOS up to 5.1.3 and classified as critical. This issue affects some unknown processing of the component API. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2024-37847. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by custom rule	N
CVE-2024-45263	GL-iNet MT6000/MT3000/MT2500/AXT1800/AX1800 4.6.2 Upload Interface information disclosure	A vulnerability was found in GL-iNet MT6000 MT3000 MT2500 AXT1800 and AX1800 4.6.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Upload Interface. The manipulation leads to information disclosure. This vulnerability is known as CVE-2024-45263. The attack can only be done within the local network. There is no exploit available.	Patched by custom rule	N

Monthly Zero-Day Vulnerability Coverage Bulletin October 2024

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™