INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

July 2024

The total **zero-day vulnerabilities** count for July month: 200

Command Injection	CSRF	Local File Inclusion	SQLi	Malicious File Upload	Cross-Site Scripting
8	12	8	50	11	111

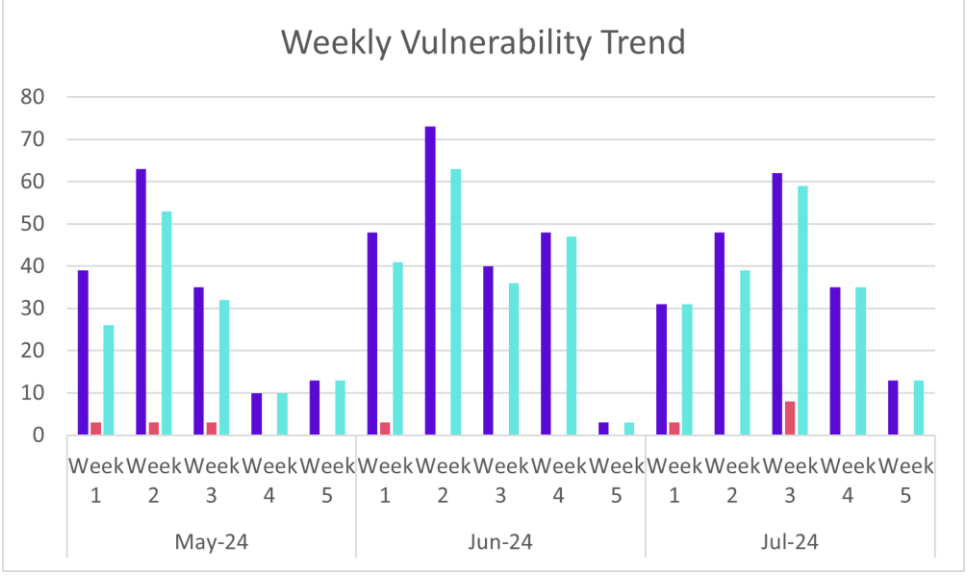
Zero-day vulnerabilities protected through core rules	189
Zero-day vulnerabilities protected through custom rules	11
Zero-day vulnerabilities for which protection cannot be done	0
Zero-day vulnerabilities found by Indusface WAS	177

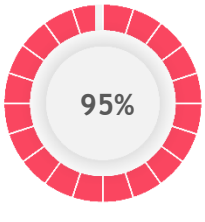
- To enable custom rules, please contact support@indusface.com
- Learn more about zero-day vulnerabilities, detection, and prevention, here

Vulnerability Trend:

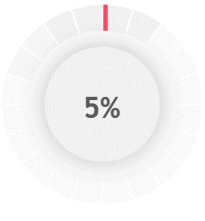
The weekly trend displays the total number of vulnerabilities discovered and the type of protection provided for the last quarter.

Weekly Vulnerability Trend

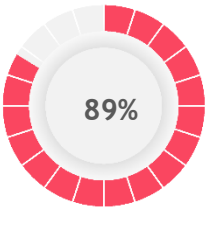




of the zero-day vulnerabilities were protected by the core rules in the last month

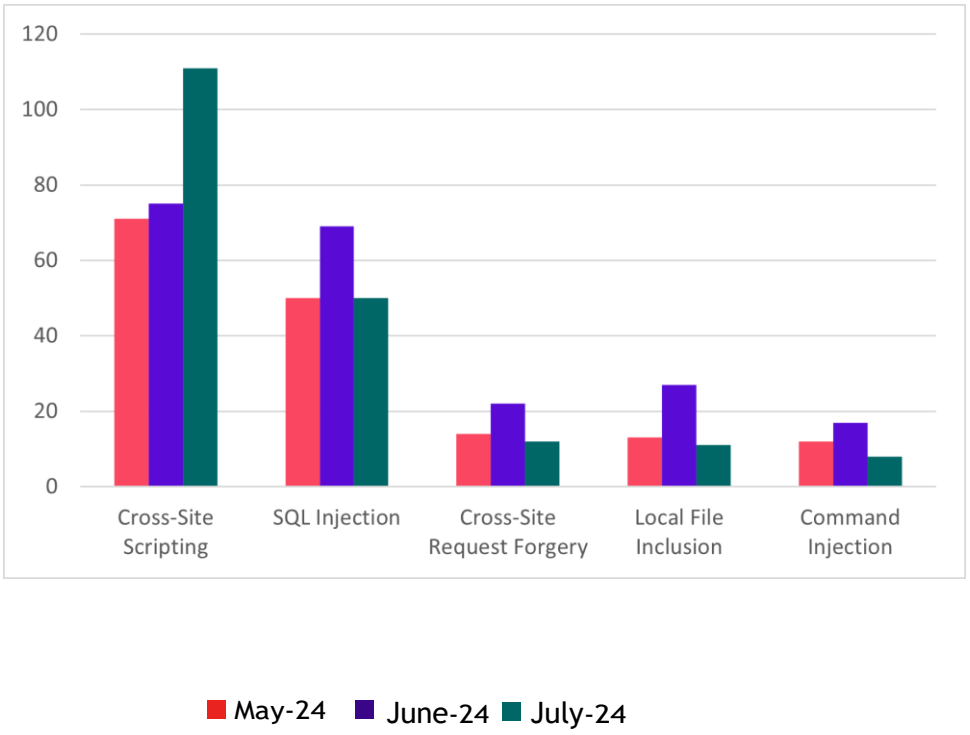


of the zero-day vulnerabilities were protected by the custom rules in the last month



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-2023-50381	LevelOne WBR-6013 RER4_A_v3411b_2T2R_LEV_09_170623 Realtek rtl819x Jungle SDK targetAPSsid os command injection (TALOS-2023-1899)	A vulnerability which was classified as critical was found in LevelOne WBR-6013 RER4_A_v3411b_2T2R_LEV_09_170623. This affects an unknown part of the component Realtek rtl819x Jungle SDK. The manipulation of the argument targetAPSsid leads to os command injection. This vulnerability is uniquely identified as CVE-2023-50381. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-41316	TOTOLINK A6000R 1.0.1-B20201211.2000 apcli_cancel_wps ifname command injection	A vulnerability was found in TOTOLINK A6000R 1.0.1-B20201211.2000. It has been declared as critical. This vulnerability affects the function apcli_cancel_wps. The manipulation of the argument ifname leads to command injection. This vulnerability was named CVE-2024-41316. The attack needs to be approached within the local network. There is no exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-41320	TOTOLINK A6000R 1.0.1-B20201211.2000 get_apcli_conn_info ifname command injection	A vulnerability has been found in TOTOLINK A6000R 1.0.1-B20201211.2000 and classified as critical. Affected by this vulnerability is the function get_apcli_conn_info. The manipulation of the argument ifname leads to command injection. This vulnerability is known as CVE-2024-41320. The attack needs to be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-41314	TOTOLINK A6000R 1.0.1-B20201211.2000 vif_disable iface command injection	A vulnerability was found in TOTOLINK A6000R 1.0.1-B20201211.2000 and classified as critical. Affected by this issue is the function vif_disable. The manipulation of the argument iface leads to command injection. This vulnerability is handled as CVE-2024-41314. Access to the local network is required for this attack. There is no exploit available.	Patched by core rule	Y
CVE-2024-41315	TOTOLINK A6000R 1.0.1-B20201211.2000 apcli_do_enr_pin_wps ifname command injection	A vulnerability was found in TOTOLINK A6000R 1.0.1-B20201211.2000. It has been classified as critical. This affects the function apcli_do_enr_pin_wps. The manipulation of the argument ifname leads to command injection. This vulnerability is uniquely identified as CVE-2024-41315. Access to the local network is required for this attack to succeed. There is no exploit available.	Patched by core rule	Y
CVE-2024-41317	TOTOLINK A6000R 1.0.1-B20201211.2000 apcli_do_enr_pbc_wps ifname command injection	A vulnerability was found in TOTOLINK A6000R 1.0.1-B20201211.2000. It has been rated as critical. This issue affects the function apcli_do_enr_pbc_wps. The manipulation of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the argument ifname leads to command injection. The identification of this vulnerability is CVE-2024-41317. The attack can only be done within the local network. There is no exploit available.		
CVE-2024-41319	TOTOLINK A6000R 1.0.1-B20201211.2000 webcmd command injection	A vulnerability classified as critical was found in TOTOLINK A6000R 1.0.1-B20201211.2000. This vulnerability affects the function webcmd. The manipulation of the argument cmd leads to command injection. This vulnerability was named CVE-2024-41319. The attack needs to be done within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-38288	R-HUB TurboMeeting up to 8.x Certificate Signing Request command injection (GHSA-gx6g-8mvx-3q5c)	A vulnerability was found in R-HUB TurboMeeting up to 8.x. It has been rated as critical. Affected by this issue is some unknown functionality of the component Certificate Signing Request Handler. The manipulation leads to command injection. This vulnerability is handled as CVE-2024-38288. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-2040	Himer Theme up to 2.1.0 on WordPress cross-site request forgery	A vulnerability was found in Himer Theme up to 2.1.0 on WordPress. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2024-2040. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	N
CVE-2024-2376	WPQA Builder Plugin up to 6.1.0 on WordPress cross-site request forgery	A vulnerability classified as problematic has been found in WPQA Builder Plugin up to 6.1.0 on WordPress. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-2376. 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-2024-2235	Himer Theme up to 2.1.0 on WordPress cross-site request forgery	A vulnerability which was classified as problematic was found in Himer Theme up to 2.1.0 on WordPress. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-2235. 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-2024-2233	Himer Theme up to 2.1.0 on WordPress cross-site request forgery	A vulnerability which was classified as problematic has been found in Himer Theme up to 2.1.0 on WordPress. This issue	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-2233. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-39019	idcCMS 1.35 idcProData_deal.php cross-site request forgery	A vulnerability was found in idcCMS 1.35 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/idcProData_deal.phpmudidel. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2024-39019. The attack may be launched remotely. There is no exploit available.	Patched by core rule	N
CVE-2023-47677	LevelOne WBR-6013 RER4_A_v3411b_2T2R_LEV_09_170623 boa cross-site request forgery (TALOS-2023-1872)	A vulnerability was found in LevelOne WBR-6013 RER4_A_v3411b_2T2R_LEV_09_170623. It has been classified as problematic. This affects an unknown part of the component boa. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-47677. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-40037	idcCMS 1.35 userScore_deal.php cross-site request forgery	A vulnerability was found in idcCMS 1.35. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/userScore_deal.phpmudidel. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2024-40037. The attack may	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		be launched remotely. There is no exploit available.		
CVE-2024-40034	idcCMS 1.35 userLevel_deal.php cross-site request forgery	A vulnerability was found in idcCMS 1.35. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/userLevel_deal.phpmudidel. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2024-40034. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-40039	idcCMS 1.35 userGroup_deal.php cross-site request forgery	A vulnerability which was classified as problematic has been found in idcCMS 1.35. This issue affects some unknown processing of the file /admin/userGroup_deal.phpmudidel. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-40039. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-3798	Phoniebox up to 2.7 Header Parameter cross-site request forgery (ID 2342)	A vulnerability which was classified as problematic has been found in Phoniebox up to 2.7. This issue affects some unknown processing of the component Header Parameter Handler. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-3798. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-1845	VikRentCar Car Rental Management System Plugin up to 1.3.1 on WordPress cross-site request forgery	A vulnerability was found in VikRentCar Car Rental Management System Plugin up to 1.3.1 on WordPress. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery.	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The identification of this vulnerability is CVE-2024-1845. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-6075	WP-FeedStats wp-cart-for-digital-products Plugin up to 8.5.4 on WordPress cross-site request forgery	A vulnerability was found in WP-FeedStats wp-cart-for-digital-products Plugin up to 8.5.4 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2024-6075. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	N

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-6085	parisneo lollms up to 9.6 XTTS Server path traversal	A vulnerability was found in parisneo lollms up to 9.6. It has been rated as critical. This issue affects some unknown processing of the component XTTS Server. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2024-6085. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-5926	stitionai devika path traversal	A vulnerability was found in stitionai devika. It has been classified as critical. Affected is an unknown function. The manipulation leads to path traversal: &039;\..\filename&039;. This vulnerability is traded as CVE-2024-5926. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-39178	MyPower vc8100 V100R001C00B030 tcpdump.php path traversal	A vulnerability was found in MyPower vc8100 V100R001C00B030. It has been rated as critical. This issue affects some unknown processing of the file /tcpdump/tcpdump.phpmenu_uuid. The manipulation leads to path traversal. The identification of this vulnerability is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2024-39178. The attack may be initiated remotely. There is no exploit available.		
CVE-2024-6433	stitionai devika prior - path traversal	A vulnerability was found in stitionai devika and classified as problematic. This issue affects some unknown processing. The manipulation leads to relative path traversal. The identification of this vulnerability is CVE-2024-6433. 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-2024-6396	aimhubio aim up to 3.19.3 path traversal	A vulnerability was found in aimhubio aim up to 3.19.3. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to path traversal: &039;\..\filename&039;. This vulnerability is known as CVE-2024-6396. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-6746	NaiboWang EasySpider 0.6.2 on Windows HTTP GET Request server.js path traversal (Issue 466)	A vulnerability classified as problematic was found in NaiboWang EasySpider 0.6.2 on Windows. Affected by this vulnerability is an unknown functionality of the file \EasySpider\resource	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		s\app\server.js of the component HTTP GET Request Handler. The manipulation with the input /../../../../../../../../../ Windows/win.ini leads to path traversal: &039;../filedir&039;. This vulnerability is known as CVE-2024-6746. The attack needs to be done within the local network. Furthermore there is an exploit available. The code maintainer explains that this is not a big issue "because the default is that the software runs locally without going through the Internet". It is recommended to apply restrictive firewalling.		
CVE-2024-40348	Bazaar 1.4.3 /api/swaggerui/static path traversal	A vulnerability was found in Bazaar 1.4.3. It has been declared as critical. This vulnerability affects unknown code of the file /api/swaggerui/static. The manipulation leads to path traversal. This vulnerability was named CVE-2024-40348. The attack needs to be approached within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-6949	Gargaj wuhu up to 3faad49bfcc3895e9ff76a591d05c8941273d120 /pages.php	A vulnerability classified as problematic was found in Gargaj wuhu	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	path traversal	up to 3faad49bfcc3895e9ff76a591d05c8941273d120. Affected by this vulnerability is an unknown functionality of the file /pages.phpeditNews. The manipulation leads to path traversal. This vulnerability is known as CVE-2024-6949. The attack can be launched remotely. Furthermore there is an exploit available. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.		

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-6439	SourceCodester Home Owners Collection Management System 1.0 Users.php img unrestricted upload	A vulnerability was found in SourceCodester Home Owners Collection Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /classes/Users.phpfsave. The manipulation of the argument img leads to unrestricted upload. The identification of this vulnerability is CVE-2024-6439. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by custom rule	N
CVE-2024-6452	linlinjava litemall up to 1.8.0 AdminGoodscontroller.java goodsId/goodsSn/name sql injection (Issue 548)	A vulnerability classified as critical was found in linlinjava litemall up to 1.8.0. Affected by this vulnerability is an unknown functionality of the file AdminGoodscontroller.java. The manipulation of the argument goodsId/goodsSn/name leads to sql injection. This vulnerability is known as CVE-2024-6452. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by custom rule	N
CVE-2024-2819	Hitachi Ops Center Common Services 10.9.3-00 default permission (hitachi-sec-2024-132)	A vulnerability which was classified as critical has been found in Hitachi Ops Center Common Services 10.9.3-00.	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Affected by this issue is some unknown functionality. The manipulation leads to incorrect default permissions. This vulnerability is handled as CVE-2024-2819. An attack has to be approached locally. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-40550	PublicCMS 4.0.202302.e File savePlaceMetaData unrestricted upload	A vulnerability has been found in PublicCMS 4.0.202302.e and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/cmsTemplate/savePlaceMetaData of the component File Handler. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2024-40550. The attack can be launched remotely. There is no exploit available.	Patched by custom rule	N
CVE-2024-40546	Sanluan PublicCMS 4.0.202302.e File /admin/cmsWebFile/save unrestricted upload	A vulnerability was found in Sanluan PublicCMS 4.0.202302.e. It has been classified as critical. Affected is an unknown function of the file /admin/cmsWebFile/save of the component File Handler. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2024-	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		40546. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2024-40545	Sanluan PublicCMS 4.0.202302.e doUpload unrestricted upload	A vulnerability classified as critical has been found in Sanluan PublicCMS 4.0.202302.e. Affected is an unknown function of the file /admin/cmsWebFile/doUpload. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2024-40545. It is possible to launch the attack remotely. There is no exploit available.	Patched by custom rule	N
CVE-2024-40551	Sanluan PublicCMS 4.0.202302.e File doUpload unrestricted upload	A vulnerability which was classified as critical was found in Sanluan PublicCMS 4.0.202302.e. This affects an unknown part of the file /admin/cmsTemplate/doUpload of the component File Handler. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2024-40551. It is possible to initiate the attack remotely. There is no exploit available.	Patched by custom rule	N
CVE-2024-40548	Sanluan PublicCMS 4.0.202302.e File /admin/cmsTemplate/save unrestricted upload	A vulnerability classified as critical was found in Sanluan PublicCMS 4.0.202302.e. Affected by this vulnerability is an unknown functionality of the file /admin/cmsTemplate/save of the	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component File Handler. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2024-40548. The attack can be launched remotely. There is no exploit available.		
CVE-2024-40549	Sanluan PublicCMS 4.0.202302.e File savePlace unrestricted upload	A vulnerability has been found in Sanluan PublicCMS 4.0.202302.e and classified as critical. This vulnerability affects unknown code of the file /admin/cmsTemplate/savePlace of the component File Handler. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2024-40549. The attack can be initiated remotely. There is no exploit available.	Patched by custom rule	N
CVE-2024-5630	Articulate Insert or Embed Articulate Content into WordPress Plugin unrestricted upload	A vulnerability has been found in Articulate Insert or Embed Articulate Content into WordPress Plugin on WordPress and classified as critical. This vulnerability affects unknown code. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2024-5630. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-6801	SourceCodester Online Student Management System 1.0 /add-students.php image unrestricted upload	A vulnerability which was classified as critical has been found in SourceCodester Online Student Management System 1.0. This issue affects some unknown processing of the file /add-students.php. The manipulation of the argument image leads to unrestricted upload. The identification of this vulnerability is CVE-2024-6801. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by custom rule	N

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-6419	SourceCodester Medicine Tracker System 1.0 Master.php id sql injection	A vulnerability classified as critical was found in SourceCodester Medicine Tracker System 1.0. This vulnerability affects unknown code of the file /classes/Master.phpfsave_medicine. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-6419. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6418	SourceCodester Medicine Tracker System 1.0 Users.php username sql injection	A vulnerability classified as critical has been found in SourceCodester Medicine Tracker System 1.0. This affects an unknown part of the file /classes/Users.phpfregister_user. The manipulation of the argument username leads to sql injection. This vulnerability is uniquely identified as CVE-2024-6418. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6205	PayPlus Payment Gateway Plugin up to 6.6.8 on WordPress sql injection	A vulnerability was found in PayPlus Payment Gateway Plugin up to 6.6.8 on WordPress. It has been classified as critical. Affected is an unknown function. The manipulation leads to sql injection. This vulnerability is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		traded as CVE-2024-6205. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2024-5606	Quiz and Survey Master Plugin up to 9.0.1 on WordPress qsm_bulk_delete_question_from_database question_id sql injection	A vulnerability was found in Quiz and Survey Master Plugin up to 9.0.1 on WordPress. It has been rated as critical. Affected by this issue is the function qsm_bulk_delete_question_from_database. The manipulation of the argument question_id leads to sql injection. This vulnerability is handled as CVE-2024-5606. 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-2024-6453	itsourcecode Farm Management System 1.0 /quarantine.php pigno/breed/reason sql injection	A vulnerability was found in itsourcecode Farm Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /quarantine.phpid3. The manipulation of the argument pigno/breed/reason leads to sql injection. This vulnerability is known as CVE-2024-6453. The attack can be launched remotely. Furthermore there is an exploit available. Original submission mentioned parameter pigno only but the VulDB data analysis team determined two	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		additional parameters to be affected as well.		
CVE-2024-6440	SourceCodester Home Owners Collection Management System 1.0 Master.php id sql injection	A vulnerability was found in SourceCodester Home Owners Collection Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /classes/Master.phpfdelete_category. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-6440. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6438	Hitout Carsale 1.0 OrderController.java orderBy sql injection (Issue 23)	A vulnerability has been found in Hitout Carsale 1.0 and classified as critical. This vulnerability affects unknown code of the file OrderController.java. The manipulation of the argument orderBy leads to sql injection. This vulnerability was named CVE-2024-6438. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-39027	SeaCMS up to 12.9 index.php cid sql injection (Issue 17)	A vulnerability classified as critical was found in SeaCMS up to 12.9. This vulnerability affects unknown code of the file /js/player/dmplayer/dmku/index.phpacedit. The manipulation of the argument cid leads to sql injection. This vulnerability was named CVE-2024-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		39027. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-37873	itsourcecode Payroll Management System 1.0 view_payslip.php id sql injection	A vulnerability has been found in itsourcecode Payroll Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file view_payslip.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-37873. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-6653	code-projects Simple Task List 1.0 Login loginForm.php username sql injection	A vulnerability was found in code-projects Simple Task List 1.0. It has been declared as critical. This vulnerability affects unknown code of the file loginForm.php of the component Login. The manipulation of the argument username leads to sql injection. This vulnerability was named CVE-2024-6653. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6652	itsourcecode Gym Management System 1.0 manage_member.php id sql injection	A vulnerability was found in itsourcecode Gym Management System 1.0. It has been classified as critical. This affects an unknown part of the file manage_member.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 is uniquely identified as CVE-2024-6652. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-6728	itsourcecode Tailoring Management System 1.0 typeedit.php id sql injection	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been classified as critical. This affects an unknown part of the file typeedit.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-6728. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6736	SourceCodester Employee and Visitor Gate Pass Logging System 1.0 view_employee.php id 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 view_employee.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-6736. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6733	itsourcecode Tailoring Management System 1.0 templateedit.php id/title/msg sql injection	A vulnerability was found in itsourcecode Tailoring Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		templateedit.php. The manipulation of the argument id/title/msg leads to sql injection. This vulnerability is handled as CVE-2024-6733. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-6735	itsourcecode Tailoring Management System 1.0 setgeneral.php sitename/email/mobile/sms/currency sql injection	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file setgeneral.php. The manipulation of the argument sitename/email/mobile/sms/currency leads to sql injection. This vulnerability was named CVE-2024-6735. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6734	itsourcecode Tailoring Management System 1.0 templateadd.php title/msg sql injection	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been classified as critical. This affects an unknown part of the file templateadd.php. The manipulation of the argument title/msg leads to sql injection. This vulnerability is uniquely identified as CVE-2024-6734. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6745	code-projects Simple Ticket Booking 1.0 Login adminauthenticate.php email/password sql injection	A vulnerability classified as critical has been found in code-projects Simple Ticket Booking 1.0. Affected is an unknown function	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the file adminauthenticate.php of the component Login. The manipulation of the argument email/password leads to sql injection. This vulnerability is traded as CVE-2024-6745. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2024-6803	itsourcecode Document Management System 1.0 insert.php anothercont sql injection	A vulnerability has been found in itsourcecode Document Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file insert.php. The manipulation of the argument anothercont leads to sql injection. This vulnerability is known as CVE-2024-6803. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-40392	SourceCodester Pharmacy Medical Store Point of Sale System 1.0 addnew.php name sql injection	A vulnerability was found in SourceCodester Pharmacy Medical Store Point of Sale System 1.0. It has been classified as critical. Affected is an unknown function of the file addnew.php. The manipulation of the argument name leads to sql injection. This vulnerability is traded as CVE-2024-40392. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-40393	Online Clinic Management System 1.0 login.php user sql injection	A vulnerability classified as critical has been found in Online Clinic Management System 1.0. This affects an unknown part of the file login.php. The manipulation of the argument user leads to sql injection. This vulnerability is uniquely identified as CVE-2024-40393. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40322	JFinalCMS 5.0.0 /admin/div_data/data sql injection	A vulnerability classified as critical has been found in JFinalCMS 5.0.0. This affects an unknown part of the file /admin/div_data/data. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2024-40322. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-6802	SourceCodester Computer Laboratory Management System 1.0 Master.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Computer Laboratory Management System 1.0. Affected is an unknown function of the file /lms/classes/Master.phpfsave_record. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-6802. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6808	itsourcecode Simple	A vulnerability was	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Task List 1.0 signUp.php insertUserRecord username sql injection	found in itsourcecode Simple Task List 1.0. It has been classified as critical. This affects the function insertUserRecord of the file signUp.php. The manipulation of the argument username leads to sql injection. This vulnerability is uniquely identified as CVE-2024-6808. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	core rule	
CVE-2024-40402	Sourcecodester Simple Library Management System 1.0 ajax.php username sql injection (Issue 49)	A vulnerability classified as critical was found in Sourcecodester Simple Library Management System 1.0. This vulnerability affects unknown code of the file ajax.php. The manipulation of the argument username leads to sql injection. This vulnerability was named CVE-2024-40402. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-6904	SourceCodester Record Management System 1.0 sort2_user.php qualification sql injection	A vulnerability which was classified as critical was found in SourceCodester Record Management System 1.0. This affects an unknown part of the file sort2_user.php. The manipulation of the argument qualification leads to sql injection. This vulnerability is uniquely identified as CVE-2024-6904. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-6901	SourceCodester Record Management System 1.0 entry.php school sql injection	A vulnerability classified as critical has been found in SourceCodester Record Management System 1.0. Affected is an unknown function of the file entry.php. The manipulation of the argument school leads to sql injection. This vulnerability is traded as CVE-2024-6901. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6902	SourceCodester Record Management System 1.0 sort_user.php sort sql injection	A vulnerability classified as critical was found in SourceCodester Record Management System 1.0. Affected by this vulnerability is an unknown functionality of the file sort_user.php. The manipulation of the argument sort leads to sql injection. This vulnerability is known as CVE-2024-6902. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6898	SourceCodester Record Management System 1.0 index.php UserName sql injection	A vulnerability was found in SourceCodester Record Management System 1.0. It has been classified as critical. This affects an unknown part of the file index.php. The manipulation of the argument UserName leads to sql injection. This vulnerability is uniquely identified as CVE-2024-6898. It is possible to initiate the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack remotely. Furthermore there is an exploit available.		
CVE-2024-6900	SourceCodester Record Management System 1.0 edit_emp.php id sql injection	A vulnerability was found in SourceCodester Record Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file edit_emp.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-6900. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6905	SourceCodester Record Management System 1.0 view_info_user.php id sql injection	A vulnerability has been found in SourceCodester Record Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file view_info_user.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-6905. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6899	SourceCodester Record Management System 1.0 view_info.php id sql injection	A vulnerability was found in SourceCodester Record Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file view_info.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-2024-6899. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-6906	SourceCodester Record Management System 1.0 add_leave_non_user .php LSS sql injection	A vulnerability was found in SourceCodester Record Management System 1.0 and classified as critical. This issue affects some unknown processing of the file add_leave_non_user.php. The manipulation of the argument LSS leads to sql injection. The identification of this vulnerability is CVE-2024-6906. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6903	SourceCodester Record Management System 1.0 sort1_user.php position sql injection	A vulnerability which was classified as critical has been found in SourceCodester Record Management System 1.0. Affected by this issue is some unknown functionality of the file sort1_user.php. The manipulation of the argument position leads to sql injection. This vulnerability is handled as CVE-2024-6903. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6957	itsourcecode University Management System 1.0 Login functions.php username sql injection	A vulnerability classified as critical has been found in itsourcecode University Management System 1.0. This affects an unknown part of the file functions.php of the component Login. The manipulation of the argument	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		username leads to sql injection. This vulnerability is uniquely identified as CVE-2024-6957. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-6951	SourceCodester Simple Online Book Store System 1.0 admin_delete.php bookisbn sql injection	A vulnerability which was classified as critical was found in SourceCodester Simple Online Book Store System 1.0. This affects an unknown part of the file admin_delete.php. The manipulation of the argument bookisbn leads to sql injection. This vulnerability is uniquely identified as CVE-2024-6951. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6969	SourceCodester Clinics Patient Management System 1.0 get_patient_history.php patient_id sql injection	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /ajax/get_patient_history.php. The manipulation of the argument patient_id leads to sql injection. The identification of this vulnerability is CVE-2024-6969. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6967	SourceCodester Employee and Visitor Gate Pass Logging System 1.0 id sql injection	A vulnerability was found in SourceCodester Employee and Visitor Gate Pass Logging	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		System 1.0. It has been classified as critical. This affects an unknown part of the file /employee_gatepass/admin/pageemployee/manage_employee. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-6967. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-6968	SourceCodester Clinics Patient Management System 1.0 print_patients_visits.php from/to sql injection	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /print_patients_visits.php. The manipulation of the argument from/to leads to sql injection. This vulnerability was named CVE-2024-6968. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6966	itsourcecode Online Blood Bank Management System 1.0 Login login.php user/pass sql injection	A vulnerability was found in itsourcecode Online Blood Bank Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file login.php of the component Login. The manipulation of the argument user/pass leads to sql injection. This vulnerability is handled as CVE-2024-6966. The attack may	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		be launched remotely. Furthermore there is an exploit available.		
CVE-2024-7069	SourceCodester Employee and Visitor Gate Pass Logging System 1.0 Master.php id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. This issue affects some unknown processing of the file /employee_gatepass/classes/Master.phpfdelete_department. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-7069. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-7081	itsourcecode Tailoring Management System 1.0 expcatadd.php title sql injection	A vulnerability was found in itsourcecode Tailoring Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file expcatadd.php. The manipulation of the argument title leads to sql injection. This vulnerability is handled as CVE-2024-7081. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-41551	Campcodes Supplier Management System 1.0 view_order_items.php id sql injection	A vulnerability which was classified as critical has been found in Campcodes Supplier Management System 1.0. Affected by this issue is some unknown functionality of the file Supply_Management_System/admin/view_order_items.php. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-41551. The attack may be launched remotely. There is no exploit available.		
CVE-2024-41550	Campcodes Supplier Management System 1.0 view_invoice_items.php id sql injection	A vulnerability classified as critical has been found in Campcodes Supplier Management System 1.0. Affected is an unknown function of the file Supply_Management_System/admin/view_invoice_items.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-41550. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-7118	MD-MAFUJUL-HASAN Online-Payroll-Management-System up to 20230911 /department_viewmore.php id sql injection	A vulnerability classified as critical was found in MD-MAFUJUL-HASAN Online-Payroll-Management-System up to 20230911. Affected by this vulnerability is an unknown functionality of the file /department_viewmore.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2024-7118. The attack can be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		not respond in any way. This product takes the approach of rolling releases to provide continious delivery. Therefore version details for affected and updated releases are not available.		
CVE-2024-7119	MD-MAFUJUL-HASAN Online-Payroll-Management-System up to 20230911 /employee_viewmore.php id sql injection	A vulnerability which was classified as critical has been found in MD-MAFUJUL-HASAN Online-Payroll-Management-System up to 20230911. Affected by this issue is some unknown functionality of the file /employee_viewmore.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2024-7119. The attack may be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way. Continious delivery 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-2024-7115	MD-MAFUJUL-HASAN Online-Payroll-Management-System up to 20230911 designation_viewmore.php id sql injection	A vulnerability was found in MD-MAFUJUL-HASAN Online-Payroll-Management-System up to 20230911. It has been declared as critical. This vulnerability affects unknown code of the file /designation_viewmor	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		e.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-7115. 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. Continious delivery with rolling releases is used by this product. Therefore no version details of affected nor updated releases are available.		
CVE-2024-7116	MD-MAFUJUL-HASAN Online-Payroll-Management-System up to 20230911 /branch_viewmore.php id sql injection	A vulnerability was found in MD-MAFUJUL-HASAN Online-Payroll-Management-System up to 20230911. It has been rated as critical. This issue affects some unknown processing of the file /branch_viewmore.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-7116. 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. This product does not use versioning. This is why information about affected and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unaffected releases are unavailable.		
CVE-2024-7117	MD-MAFUJUL-HASAN Online-Payroll-Management-System up to 20230911 /shift_viewmore.php id sql injection	A vulnerability classified as critical has been found in MD-MAFUJUL-HASAN Online-Payroll-Management-System up to 20230911. Affected is an unknown function of the file /shift_viewmore.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2024-7117. 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. This product is using a rolling release to provide continious delivery. Therefore no version details for affected nor updated releases are available.	Patched by core rule	Y
CVE-2024-7114	Tianchoy Blog up to 1.8.8 /so.php search sql injection	A vulnerability was found in Tianchoy Blog up to 1.8.8. It has been classified as critical. This affects an unknown part of the file /so.php. The manipulation of the argument search leads to sql injection. This vulnerability is uniquely identified as CVE-2024-7114. It is possible to initiate the attack 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-2024-38289	R-HUB TurboMeeting up to 8.x sql injection (GHSA-vx5j-8pgx-v42v)	A vulnerability was found in R-HUB TurboMeeting up to 8.x. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2024-38289. The attack can be launched remotely. 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-2024-4959	Frontend Checklist Plugin up to 2.3.2 on WordPress Setting cross site scripting	A vulnerability classified as problematic was found in Frontend Checklist Plugin up to 2.3.2 on WordPress. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-4959. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-5199	Spotify Play Button Plugin up to 1.0 on WordPress Shortcode cross site scripting	A vulnerability which was classified as problematic was found in Spotify Play Button Plugin up to 1.0 on WordPress. Affected is an unknown function of the component Shortcode Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-5199. 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-2024-5473	Simple Photoswipe Plugin up to 0.1 on WordPress Setting cross site scripting	A vulnerability has been found in Simple Photoswipe Plugin up to 0.1 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is known as CVE-2024-5473. The attack can be launched remotely. There is no exploit available.		
CVE-2024-5169	Video Widget Plugin up to 1.2.3 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic has been found in Video Widget Plugin up to 1.2.3 on WordPress. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-5169. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-5933	parisneo lollms-webui Chat Message cross site scripting	A vulnerability was found in parisneo lollms-webui and classified as problematic. Affected by this issue is some unknown functionality of the component Chat Message Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-5933. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-3111	Interactive Content Plugin up to 1.15.7 on WordPress SVG File cross site scripting	A vulnerability classified as problematic has been found in Interactive Content Plugin up to 1.15.7 on WordPress. This affects an unknown part of the component SVG File 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 uniquely identified as CVE-2024-3111. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-4664	WP Chat App Plugin up to 3.6.4 on WordPress Setting cross site scripting	A vulnerability was found in WP Chat App Plugin up to 3.6.4 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-4664. 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-2024-37741	OpenPLC up to 9cd8f1b Profile Picture cross site scripting (Issue 242)	A vulnerability was found in OpenPLC up to 9cd8f1b. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Profile Picture Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-37741. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-5737	Nikola Vasilijevski AdmirorFrames up to 4.x	A vulnerability was found in Nikola Vasilijevski	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	afGdStream.php cross site scripting	AdmirorFrames up to 4.x. It has been rated as problematic. This issue affects some unknown processing of the file afGdStream.php. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-5737. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-5730	Pagerank Tools Plugin up to 1.1.5 on WordPress cross site scripting	A vulnerability was found in Pagerank Tools Plugin up to 1.1.5 on WordPress and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-5730. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-5729	Simple AL Slider Plugin up to 1.2.10 on WordPress cross site scripting	A vulnerability has been found in Simple AL Slider Plugin up to 1.2.10 on WordPress and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-5729. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-5728	Animated AL List Plugin up to 1.0.6 on WordPress cross site	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
	scripting	in Animated AL List Plugin up to 1.0.6 on WordPress. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-5728. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-5727	Widget4Call Plugin up to 1.0.7 on WordPress cross site scripting	A vulnerability which was classified as problematic has been found in Widget4Call Plugin up to 1.0.7 on WordPress. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-5727. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-5727	Widget4Call Plugin up to 1.0.7 on WordPress cross site scripting	A vulnerability which was classified as problematic has been found in Widget4Call Plugin up to 1.0.7 on WordPress. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-5727. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-4934	Quiz and Survey Master Plugin up to 9.0.1 on WordPress cross site scripting	A vulnerability was found in Quiz and Survey Master Plugin up to 9.0.1 on WordPress. It has been declared as problematic. This vulnerability affects unknown code. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation leads to cross site scripting. This vulnerability was named CVE-2024-4934. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-6130	10Web Form Maker Plugin up to 1.15.25 on WordPress Setting cross site scripting	A vulnerability was found in 10Web Form Maker Plugin up to 1.15.25 on WordPress. It has been rated as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-6130. 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-2024-4627	Rank Math SEO Plugin up to 1.0.218 on WordPress Setting cross site scripting	A vulnerability classified as problematic was found in Rank Math SEO Plugin up to 1.0.218 on WordPress. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-4627. The attack can be initiated remotely. There is no exploit available. It is recommended to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		upgrade the affected component.		
CVE-2024-3999	EazyDocs Plugin up to 2.4.x on WordPress Setting cross site scripting	A vulnerability classified as problematic has been found in EazyDocs Plugin up to 2.4.x on WordPress. This affects an unknown part of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-3999. 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-2024-39143	ResidenceCMS 2.10.1 cross site scripting	A vulnerability which was classified as problematic has been found in ResidenceCMS 2.10.1. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-39143. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-5767	WP-FeedStats sitetweet Plugin up to 0.2 on WordPress cross site scripting	A vulnerability which was classified as problematic has been found in WP-FeedStats sitetweet Plugin up to 0.2 on WordPress. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-5767. The attack may be initiated remotely. There is no	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit available.		
CVE-2024-6011	Cost Calculator Builder Plugin up to 3.2.12 on WordPress cross site scripting	A vulnerability which was classified as problematic was found in Cost Calculator Builder Plugin up to 3.2.12 on WordPress. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-6011. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-37763	MachForm up to 19 cross site scripting	A vulnerability classified as problematic was found in MachForm up to 19. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-37763. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-2375	WPQA Builder Plugin up to 6.1.0 on WordPress Slider Setting cross site scripting	A vulnerability was found in WPQA Builder Plugin up to 6.1.0 on WordPress. It has been classified as problematic. This affects an unknown part of the component Slider Setting Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-2375. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-2234	Himer Theme up to 2.1.0 on WordPress Post Setting cross site scripting	A vulnerability was found in Himer Theme up to 2.1.0 on WordPress and classified as problematic. Affected by this issue is some unknown functionality of the component Post Setting Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-2234. 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-2024-23997	Lukas Bach yana 1.0.16 src/electron-main.ts cross site scripting	A vulnerability was found in Lukas Bach yana 1.0.16. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file src/electron-main.ts. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-23997. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-39174	yzmcms 7.1 Publish Article cross site scripting	A vulnerability was found in yzmcms 7.1 and classified as problematic. This issue affects some unknown processing of the component Publish Article Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-39174. 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-2024-29318	Volmarg Personal Management System 1.4.64 SVG File cross site scripting	A vulnerability was found in Volmarg Personal Management System 1.4.64. It has been classified as problematic. Affected is an unknown function of the component SVG File Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-29318. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-6523	ZKTeco BioTime up to 9.5.2 system-group-add user cross site scripting	A vulnerability was found in ZKTeco BioTime up to 9.5.2. It has been classified as problematic. Affected is an unknown function of the component system-group-add Handler. The manipulation of the argument user with the input <script>alert</script> leads to cross site scripting. This vulnerability is traded as CVE-2024-6523. It is possible to launch the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-23998	goanother Another Redis Desktop Manager 1.6.1 Setting.vue cross site scripting	A vulnerability was found in goanother Another Redis Desktop Manager 1.6.1. It has been rated as problematic. Affected by this issue is some	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown functionality of the file src/components/Setting.vue. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-23998. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-40605	Foreground Skin up to 1.42.1 on MediaWiki Sidebar Menu cross site scripting	A vulnerability was found in Foreground Skin up to 1.42.1 on MediaWiki. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Sidebar Menu Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-40605. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40604	Nimbus Skin up to 1.42.1 on MediaWiki Sidebar Menu cross site scripting	A vulnerability which was classified as problematic was found in Nimbus Skin up to 1.42.1 on MediaWiki. Affected is an unknown function of the component Sidebar Menu Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-40604. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40600	Metrolook Skin up to 1.42.1 on MediaWiki Sidebar Menu cross site scripting	A vulnerability was found in Metrolook Skin up to 1.42.1 on MediaWiki. It has been classified as problematic. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affects an unknown part of the component Sidebar Menu Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-40600. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-6539	heyewei SpringBootCMS up to 2024-05-28 Guestbook /guestbook Content cross site scripting (IA9D7F)	A vulnerability classified as problematic has been found in heyewei SpringBootCMS up to 2024-05-28. Affected is an unknown function of the file /guestbook of the component Guestbook Handler. The manipulation of the argument Content leads to cross site scripting. This vulnerability is traded as CVE-2024-6539. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6229	stangirard quivr cross site scripting	A vulnerability which was classified as problematic has been found in stangirard quivr. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-6229. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40599	GuMaxDD Skin up to 1.42.1 on MediaWiki Sidebar Menu cross site scripting	A vulnerability was found in GuMaxDD Skin up to 1.42.1 on MediaWiki. It has been declared as problematic. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability affects unknown code of the component Sidebar Menu Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-40599. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-39203	Z-BlogPHP 1.7.3 Theme Management Module cross site scripting	A vulnerability classified as problematic has been found in Z-BlogPHP 1.7.3. This affects an unknown part of the component Theme Management Module. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-39203. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-6170	Unlimited Elements For Elementor Plugin up to 1.5.112 on WordPress email cross site scripting	A vulnerability was found in Unlimited Elements For Elementor Plugin up to 1.5.112 on WordPress. It has been rated as problematic. This issue affects some unknown processing. The manipulation of the argument email leads to cross site scripting. The identification of this vulnerability is CVE-2024-6170. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-5711	stitionai devika cross site scripting	A vulnerability was found in stitionai devika and classified as problematic. This issue affects some unknown processing. The manipulation leads to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross site scripting. The identification of this vulnerability is CVE-2024-5711. The attack may be initiated remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.		
CVE-2024-6169	Unlimited Elements For Elementor Plugin up to 1.5.112 on WordPress username cross site scripting	A vulnerability was found in Unlimited Elements For Elementor Plugin up to 1.5.112 on WordPress. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument username leads to cross site scripting. This vulnerability was named CVE-2024-6169. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40731	Netbox 4.0.3 Name cross site scripting	A vulnerability has been found in Netbox 4.0.3 and classified as problematic. This vulnerability affects unknown code of the file /dcim/rear-ports/{id}/edit/. The manipulation of the argument Name leads to cross site scripting. This vulnerability was named CVE-2024-40731. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40728	Netbox 4.0.3 Name cross site scripting	A vulnerability was found in Netbox 4.0.3. It has been declared as problematic. Affected by this vulnerability is an unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		functionality of the file /dcim/console-server-ports/{id}/edit/. The manipulation of the argument Name leads to cross site scripting. This vulnerability is known as CVE-2024-40728. The attack can be launched remotely. There is no exploit available.		
CVE-2024-40735	Netbox 4.0.3 Name cross site scripting	A vulnerability was found in Netbox 4.0.3. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /dcim/power-outlets/{id}/edit/. The manipulation of the argument Name leads to cross site scripting. This vulnerability is handled as CVE-2024-40735. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40727	Netbox 4.0.3 Name cross site scripting	A vulnerability which was classified as problematic has been found in Netbox 4.0.3. Affected by this issue is some unknown functionality of the file /dcim/console-server-ports/add/. The manipulation of the argument Name leads to cross site scripting. This vulnerability is handled as CVE-2024-40727. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40730	Netbox 4.0.3 Name cross site scripting	A vulnerability classified as problematic has been found in Netbox 4.0.3. Affected is an unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		function of the file /dcim/interfaces/{id}/edit/. The manipulation of the argument Name leads to cross site scripting. This vulnerability is traded as CVE-2024-40730. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2024-40734	Netbox 4.0.3 /dcim/front-ports/add/ Name cross site scripting	A vulnerability classified as problematic was found in Netbox 4.0.3. Affected by this vulnerability is an unknown functionality of the file /dcim/front-ports/add/. The manipulation of the argument Name leads to cross site scripting. This vulnerability is known as CVE-2024-40734. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-38972	Netbox 4.0.3 /dcim/power-ports/add/ Name cross site scripting	A vulnerability has been found in Netbox 4.0.3 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /dcim/power-ports/add/. The manipulation of the argument Name leads to cross site scripting. This vulnerability is known as CVE-2024-38972. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40726	Netbox 4.0.3 Name cross site scripting	A vulnerability was found in Netbox 4.0.3. It has been classified as problematic. This affects an unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		part of the file /dcim/power-ports/{id}/edit/. The manipulation of the argument Name leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-40726. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-40733	Netbox 4.0.3 Name cross site scripting	A vulnerability which was classified as problematic was found in Netbox 4.0.3. This affects an unknown part of the file /dcim/front-ports/{id}/edit/. The manipulation of the argument Name leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-40733. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40732	Netbox 4.0.3 /dcim/rear-ports/add/ Name cross site scripting	A vulnerability was found in Netbox 4.0.3 and classified as problematic. This issue affects some unknown processing of the file /dcim/rear-ports/add/. The manipulation of the argument Name leads to cross site scripting. The identification of this vulnerability is CVE-2024-40732. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40729	Netbox 4.0.3 /dcim/interfaces/add/ Name cross site scripting	A vulnerability was found in Netbox 4.0.3. It has been classified as problematic. Affected is an unknown function of the file /dcim/interfaces/add/.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The manipulation of the argument Name leads to cross site scripting. This vulnerability is traded as CVE-2024-40729. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2024-40737	Netbox 4.0.3 /dcim/console-ports/add Name cross site scripting	A vulnerability classified as problematic was found in Netbox 4.0.3. This vulnerability affects unknown code of the file /dcim/console-ports/add. The manipulation of the argument Name leads to cross site scripting. This vulnerability was named CVE-2024-40737. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40736	Netbox 4.0.3 /dcim/power-outlets/add Name cross site scripting	A vulnerability classified as problematic has been found in Netbox 4.0.3. This affects an unknown part of the file /dcim/power-outlets/add. The manipulation of the argument Name leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-40736. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40738	Netbox 4.0.3 Name cross site scripting	A vulnerability which was classified as problematic was found in Netbox 4.0.3. Affected is an unknown function of the file /dcim/console-ports/{id}/edit/. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument Name leads to cross site scripting. This vulnerability is traded as CVE-2024-40738. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2024-40740	Netbox 4.0.3 Name cross site scripting	A vulnerability which was classified as problematic has been found in Netbox 4.0.3. This issue affects some unknown processing of the file /dcim/power-feeds/{id}/edit/. The manipulation of the argument Name leads to cross site scripting. The identification of this vulnerability is CVE-2024-40740. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40742	Netbox 4.0.3 /circuits/circuits/add ID cross site scripting	A vulnerability was found in Netbox 4.0.3. It has been classified as problematic. This affects an unknown part of the file /circuits/circuits/add. The manipulation of the argument ID leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-40742. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40739	Netbox 4.0.3 /dcim/power-feeds/add Name cross site scripting	A vulnerability has been found in Netbox 4.0.3 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /dcim/power-feeds/add. 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 is known as CVE-2024-40739. The attack can be launched remotely. There is no exploit available.		
CVE-2024-40741	Netbox 4.0.3 ID cross site scripting	A vulnerability was found in Netbox 4.0.3 and classified as problematic. Affected by this issue is some unknown functionality of the file /circuits/circuits/{id}/edit/. The manipulation of the argument ID leads to cross site scripting. This vulnerability is handled as CVE-2024-40741. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-38963	Nopcommerce 4.70.1 cross site scripting (Issue 7224)	A vulnerability classified as problematic has been found in Nopcommerce 4.70.1. Affected is an unknown function. The manipulation of the argument AddProductReview.Title/AddProductReview.ReviewText leads to cross site scripting. This vulnerability is traded as CVE-2024-38963. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-40336	idcCMS 1.35 Image Advertising Management cross site scripting	A vulnerability classified as problematic has been found in idcCMS 1.35. This affects an unknown part of the component Image Advertising Management. 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 uniquely identified as CVE-2024-40336. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-4655	Ultimate Blocks Plugin up to 3.1.8 on WordPress Block Option cross site scripting	A vulnerability classified as problematic has been found in Ultimate Blocks Plugin up to 3.1.8 on WordPress. Affected is an unknown function of the component Block Option Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-4655. 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-2024-6025	Quiz and Survey Master Plugin up to 9.0.4 on WordPress Setting cross site scripting	A vulnerability classified as problematic was found in Quiz and Survey Master Plugin up to 9.0.4 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-2024-6025. 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-2024-6035	gaizhenbiao chuanhuchatgpt up	A vulnerability was found in gaizhenbiao	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	to 20240410 cross site scripting	chuanhuchatgpt up to 20240410. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-6035. The attack can be launched remotely. There is no exploit available.		
CVE-2024-6026	10Web Slider Plugin up to 1.2.55 on WordPress cross site scripting	A vulnerability was found in 10Web Slider Plugin up to 1.2.55 on WordPress. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-6026. 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-2024-6138	Secure Copy Content Protection and Content Locking Plugin Setting cross site scripting	A vulnerability which was classified as problematic has been found in Secure Copy Content Protection and Content Locking Plugin up to 4.0.8 on WordPress. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-6138. The attack may be launched remotely. There is no exploit	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		available. It is recommended to upgrade the affected component.		
CVE-2024-5626	Inline Related Posts Plugin up to 3.6.x on WordPress cross site scripting	A vulnerability was found in Inline Related Posts Plugin up to 3.6.x on WordPress and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-5626. 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-2024-2430	Website Content in Page or Post Plugin prior 2024.04.09 on WordPress Shortcode Attribute cross site scripting	A vulnerability which was classified as problematic has been found in Website Content in Page or Post Plugin on WordPress. Affected by this issue is some unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-2430. 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-2024-5811	Simple Video Directory Plugin up to 1.4.3 on WordPress Setting cross site scripting	A vulnerability was found in Simple Video Directory Plugin up to 1.4.3 on WordPress. It has been classified as problematic. Affected	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		is an unknown function of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-5811. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-0974	Social Media Widget Plugin up to 4.0.8 on WordPress Setting cross site scripting	A vulnerability classified as problematic was found in Social Media Widget Plugin up to 4.0.8 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-2024-0974. 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-2024-2640	Watu Quiz Plugin up to 3.4.1.1 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic was found in Watu Quiz Plugin up to 3.4.1.1 on WordPress. This affects an unknown part of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-2640. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		It is recommended to upgrade the affected component.		
CVE-2024-3751	Seriously Simple Podcasting Plugin up to 3.2.x on WordPress Setting cross site scripting	A vulnerability was found in Seriously Simple Podcasting Plugin up to 3.2.x on WordPress. It has been classified as problematic. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-3751. 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-2024-5715	WP-FeedStats wp-eMember Plugin up to 10.6.6 on WordPress cross site scripting	A vulnerability has been found in WP-FeedStats wp-eMember Plugin up to 10.6.6 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-2024-5715. 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-2024-4217	WP-FeedStats shortcodes-ultimate-pro Plugin up to 7.1.4 on WordPress Shortcode cross site scripting	A vulnerability has been found in WP-FeedStats shortcodes-ultimate-pro Plugin up to 7.1.4 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 vulnerability is an unknown functionality of the component Shortcode Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-4217. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-4977	Index WP MySQL for Speed Plugin up to 1.4.17 on WordPress cross site scripting	A vulnerability was found in Index WP MySQL for Speed Plugin up to 1.4.17 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-2024-4977. 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-2024-5442	Photo Gallery, Sliders, Proofing Plugin up to 3.59.2 on WordPress Setting cross site scripting	A vulnerability was found in Photo Gallery Sliders Proofing Plugin up to 3.59.2 on WordPress and classified as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-5442. 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. It is recommended to upgrade the affected component.		
CVE-2024-3026	MaxButtons Button Plugin up to 9.7.7 on WordPress cross site scripting	A vulnerability which was classified as problematic was found in MaxButtons Button Plugin up to 9.7.7 on WordPress. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-3026. 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-2024-5713	If-So Dynamic Content Personalization Plugin up to 1.8.0.3 on WordPress Attribute $_SERVER['REQUEST_URI'] cross site scripting	A vulnerability classified as problematic has been found in If-So Dynamic Content Personalization Plugin up to 1.8.0.3 on WordPress. Affected is an unknown function of the component Attribute Handler. The manipulation of the argument $_SERVER[&039;REQUEST_URI&039;] leads to cross site scripting. This vulnerability is traded as CVE-2024-5713. 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-2024-4752	EventON Plugin up to 2.2.14 on	A vulnerability was found in EventON	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	WordPress Setting cross site scripting	Plugin up to 2.2.14 on WordPress and classified as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-4752. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-2870	WP-FeedStats socialdriver-framework Plugin 2024.0.0 on WordPress cross site scripting	A vulnerability which was classified as problematic has been found in WP-FeedStats socialdriver-framework Plugin 2024.0.0 on WordPress. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-2870. 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-2024-5282	WP-FeedStats wp-affiliate-platform Plugin up to 6.5.0 on WordPress cross site scripting	A vulnerability was found in WP-FeedStats wp-affiliate-platform Plugin up to 6.5.0 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		5282. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-3710	Image Photo Gallery Final Tiles Grid Plugin up to 3.5.x on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in Image Photo Gallery Final Tiles Grid Plugin up to 3.5.x on WordPress and classified as problematic. This issue affects some unknown processing of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-3710. 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-2024-5079	WP-FeedStats wp-eMember Plugin up to 10.6.6 on WordPress cross site scripting	A vulnerability has been found in WP-FeedStats wp-eMember Plugin up to 10.6.6 on WordPress and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-5079. 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-2024-3964	Product Enquiry for WooCommerce	A vulnerability classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Plugin up to 3.1.7 on WordPress Setting cross site scripting	problematic has been found in Product Enquiry for WooCommerce Plugin up to 3.1.7 on WordPress. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-3964. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-5644	Tournamatch Plugin up to 4.6.0 on WordPress Setting cross site scripting	A vulnerability was found in Tournamatch Plugin up to 4.6.0 on WordPress. It has been declared as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-5644. 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-2024-5472	WP QuickLaTeX Plugin up to 3.8.6 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic was found in WP QuickLaTeX Plugin up to 3.8.6 on WordPress. Affected is an unknown function of the component Setting 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 traded as CVE-2024-5472. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-5286	WP-FeedStats wp-affiliate-platform Plugin up to 6.5.0 on WordPress cross site scripting	A vulnerability classified as problematic was found in WP-FeedStats wp-affiliate-platform Plugin up to 6.5.0 on WordPress. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-5286. 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-2024-5281	WP-FeedStats wp-affiliate-platform Plugin up to 6.5.0 on WordPress cross site scripting	A vulnerability was found in WP-FeedStats wp-affiliate-platform Plugin up to 6.5.0 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-5281. 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-2024-5744	WP-FeedStats wp-	A vulnerability which	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	eMember Plugin up to 10.6.6 on WordPress Attribute $_SERVER['REQUEST_URI'] cross site scripting	was classified as problematic was found in WP-FeedStats wp-eMember Plugin up to 10.6.6 on WordPress. This affects an unknown part of the component Attribute Handler. The manipulation of the argument $_SERVER[&039;REQUEST_URI&039;] leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-5744. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	core rule	
CVE-2024-5151	SULly Plugin up to 4.3.0 on WordPress Setting cross site scripting	A vulnerability was found in SULly Plugin up to 4.3.0 on WordPress and classified as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-5151. 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-2024-5075	WP-FeedStats wp-eMember Plugin up to 10.6.5 on WordPress cross site scripting	A vulnerability which was classified as problematic was found in WP-FeedStats wp-eMember Plugin up to 10.6.5 on WordPress. This affects an unknown part. 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 uniquely identified as CVE-2024-5075. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-5283	WP-FeedStats wp-affiliate-platform Plugin up to 6.5.0 on WordPress cross site scripting	A vulnerability classified as problematic has been found in WP-FeedStats wp-affiliate-platform Plugin up to 6.5.0 on WordPress. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-5283. 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-2024-3753	Hostel Plugin up to 1.1.5.2 on WordPress cross site scripting	A vulnerability was found in Hostel Plugin up to 1.1.5.2 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-3753. 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-2024-5032	SULly Plugin up to	A vulnerability	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	4.3.0 on WordPress cross site scripting	classified as problematic was found in SULly Plugin up to 4.3.0 on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-5032. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	core rule	
CVE-2024-6070	If-So Dynamic Content Personalization Plugin up to 1.8.0.3 on WordPress Setting cross site scripting	A vulnerability which was classified as problematic has been found in If-So Dynamic Content Personalization Plugin up to 1.8.0.3 on WordPress. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-6070. 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-2024-6072	WP-FeedStats wp-cart-for-digital-products Plugin up to 8.5.4 on WordPress Attribute $_SERVER['REQUEST_URI'] cross site scripting	A vulnerability was found in WP-FeedStats wp-cart-for-digital-products Plugin up to 8.5.4 on WordPress. It has been classified as problematic. Affected is an unknown function of the component Attribute Handler. The manipulation of the argument	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		$_SERVER[&039;REQUEST_URI&039;] leads to cross site scripting. This vulnerability is traded as CVE-2024-6072. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-6073	WP-FeedStats wp-cart-for-digital-products Plugin up to 8.5.4 on WordPress cross site scripting	A vulnerability was found in WP-FeedStats wp-cart-for-digital-products Plugin up to 8.5.4 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-6073. 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-2024-6076	WP-FeedStats wp-cart-for-digital-products Plugin up to 8.5.4 on WordPress cross site scripting	A vulnerability classified as problematic has been found in WP-FeedStats wp-cart-for-digital-products Plugin up to 8.5.4 on WordPress. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-6076. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		upgrade the affected component.		
CVE-2024-6074	WP-FeedStats wp-cart-for-digital-products Plugin up to 8.5.4 on WordPress cross site scripting	A vulnerability was found in WP-FeedStats wp-cart-for-digital-products Plugin up to 8.5.4 on WordPress and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-6074. 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-2024-6740	Openfind Mail2000 7.0/8.0 Attachment cross site scripting (Patch 131)	A vulnerability was found in Openfind Mail2000 7.0/8.0. It has been classified as problematic. This affects an unknown part of the component Attachment Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-6740. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y
CVE-2024-6807	SourceCodester Student Study Center Desk Management System 1.0 HTTP POST Request Users.php firstname/middlename/lastname/username cross site scripting	A vulnerability was found in SourceCodester Student Study Center Desk Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/sscdms/classes/Users.phpfsave of the component HTTP POST Request Handler. The manipulation of the argument firstname/middlename/lastname/username leads to cross site scripting. This vulnerability is handled as CVE-2024-6807. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-40492	Heartbeat Chat 15.2.1 setname cross site scripting	A vulnerability was found in Heartbeat Chat 15.2.1. It has been declared as problematic. This vulnerability affects the function setname. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-40492. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-6907	SourceCodester Record Management System 1.0 sort.php sort cross site scripting	A vulnerability was found in SourceCodester Record Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file sort.php. The manipulation of the argument sort leads to cross site scripting. This vulnerability is traded as CVE-2024-6907. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-39682	XjSv Cooked Plugin up to 1.7.x on WordPress cross site	A vulnerability was found in XjSv Cooked Plugin up to 1.7.x on	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	scripting (GHSA-fx69-f77x-84gr)	WordPress. It has been classified as problematic. Affected is an unknown function. The manipulation leads to basic cross site scripting. This vulnerability is traded as CVE-2024-39682. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-39123	janeczku Calibre-Web up to 0.6.21 edit_book_comments cross site scripting	A vulnerability has been found in janeczku Calibre-Web up to 0.6.21 and classified as problematic. Affected by this vulnerability is the function edit_book_comments. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-39123. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-41599	RuoYi up to 4.7.9 File Upload cross site scripting	A vulnerability was found in RuoYi up to 4.7.9 and classified as problematic. Affected by this issue is some unknown functionality of the component File Upload. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-41599. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-6932	ClassCMS 4.5 order cross site scripting	A vulnerability was found in ClassCMS 4.5. It has been declared as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		problematic. Affected by this vulnerability is an unknown functionality of the file /admin/actionhome&doshop:index&keyword&kindall. The manipulation of the argument order leads to cross site scripting. This vulnerability is known as CVE-2024-6932. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2024-6939	Xinhu RockOA 2.6.3 tpl_upload.html okla callback cross site scripting	A vulnerability was found in Xinhu RockOA 2.6.3 and classified as problematic. Affected by this issue is the function okla of the file /webmain/public/upload/tpl_upload.html. The manipulation of the argument callback leads to cross site scripting. This vulnerability is handled as CVE-2024-6939. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6935	formtools.org Form Tools 3.1.1 User Settings Page /admin/clients/ cross site scripting	A vulnerability classified as problematic was found in formtools.org Form Tools 3.1.1. This vulnerability affects unknown code of the file /admin/clients/ of the component User Settings Page. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-6935. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-6954	SourceCodester Record Management System 1.0 sort1.php position cross site scripting	A vulnerability was found in SourceCodester Record Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file sort1.php. The manipulation of the argument position leads to cross site scripting. This vulnerability is known as CVE-2024-6954. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-6955	SourceCodester Record Management System 1.0 sort2.php qualification cross site scripting	A vulnerability was found in SourceCodester Record Management System 1.0. It has been classified as problematic. Affected is an unknown function of the file sort2.php. The manipulation of the argument qualification leads to cross site scripting. This vulnerability is traded as CVE-2024-6955. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-40347	Hyland Alfresco 23.2.1-r96 htmlid cross site scripting	A vulnerability was found in Hyland Alfresco 23.2.1-r96. It has been rated as problematic. This issue affects some unknown processing. The manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument htmlid leads to cross site scripting. The identification of this vulnerability is CVE-2024-40347. The attack may be initiated remotely. There is no exploit available.		
CVE-2024-7068	SourceCodester Insurance Management System 1.0 update_sub_category name cross site scripting	A vulnerability classified as problematic has been found in SourceCodester Insurance Management System 1.0. This affects an unknown part of the file /Script/admin/core/update_sub_category. The manipulation of the argument name leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-7068. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y

INDUSFACE™

Indusface is a leading application security SaaS company that secures critical Web, Mobile & API applications of 5000+ global customers using its award-winning fully managed platform that integrates a web application scanner, web application firewall, DDoS &, BOT Mitigation, CDN, and threat intelligence engine.

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

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

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