INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

March 2024

The total **zero-day vulnerabilities** count for March month: 183

Command Injection	CSRF	Local File Inclusion	SQLi	Malicious File Upload	Cross-site Scripting
10	10	9	63	8	83

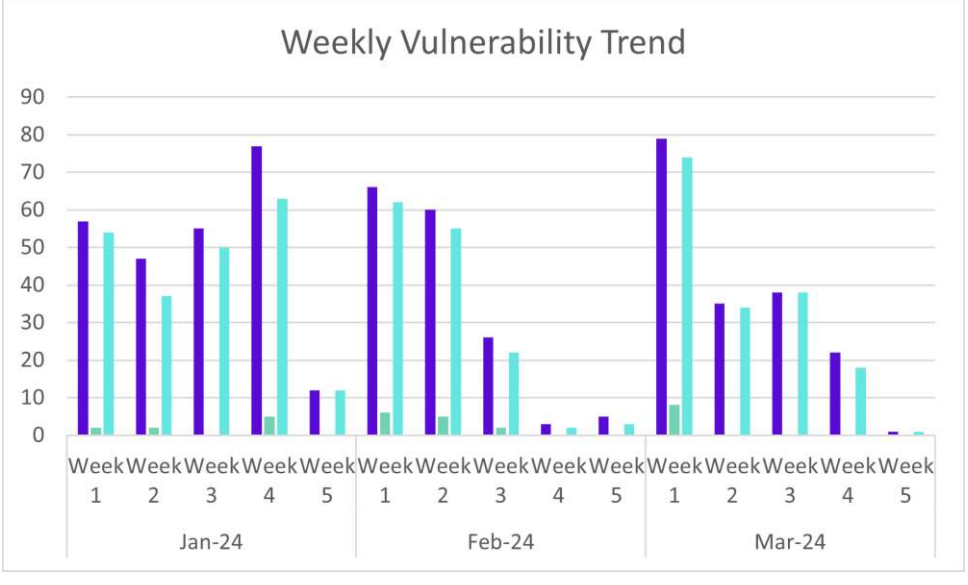
Zero-day vulnerabilities protected through core rules	175
Zero-day vulnerabilities protected through custom rules	8
Zero-day vulnerabilities for which protection cannot be done	0
Zero-day vulnerabilities found by Indusface WAS	165

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

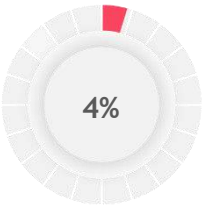
Vulnerability Trend:

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

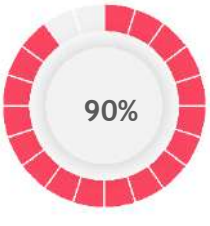
Weekly Vulnerability Trend



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

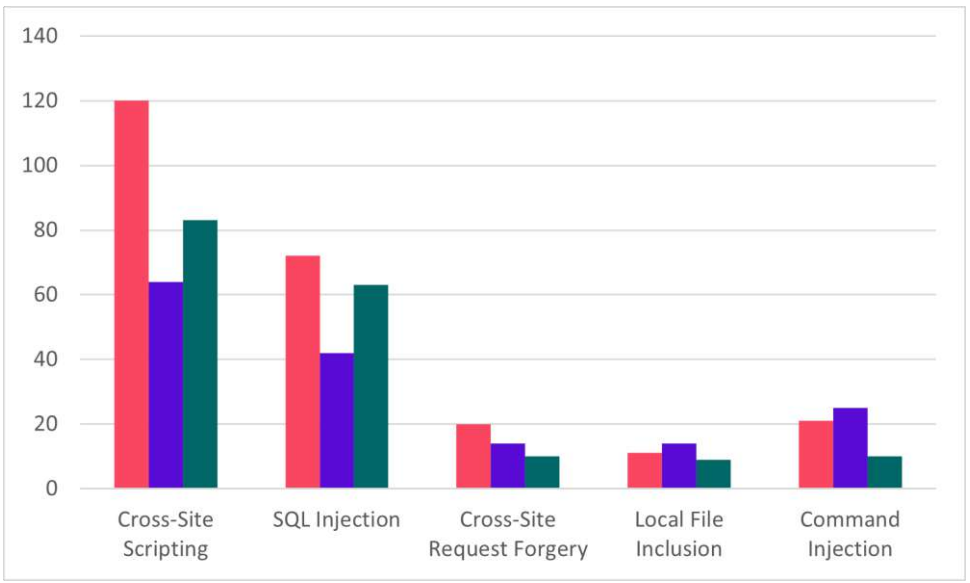


of the zero-day vulnerabilities were protected by the custom rules in the last month



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

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-2016	ZhiCms 4.0 setcontroller.php index sitename code injection	A vulnerability which was classified as critical was found in ZhiCms 4.0. Affected is the function index of the file app/manage/controller/setcontroller.php. The manipulation of the argument sitename leads to code injection. This vulnerability is traded as CVE-2024-2016. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-27622	CMS Made Simple 2.2.19 User Defined Tags Module code injection	A vulnerability which was classified as critical has been found in CMS Made Simple 2.2.19. Affected by this issue is some unknown functionality of the component User Defined Tags Module. The manipulation leads to code injection. This vulnerability is handled as CVE-2024-27622. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-0817	paddle 2.6.0 IrGraph.draw command injection	A vulnerability classified as critical was found in paddle 2.6.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Affected by this vulnerability is the function IrGraph.draw. The manipulation leads to command injection. This vulnerability is known as CVE-2024-0817. Local access is required to approach this attack. There is no exploit available.		
CVE-2024-0815	paddle 2.6.0 paddle.utils.download._wget_download os command injection	A vulnerability was found in paddle 2.6.0. It has been classified as critical. This affects the function paddle.utils.download._wget_download. The manipulation leads to os command injection. This vulnerability is uniquely identified as CVE-2024-0815. Attacking locally is a requirement. There is no exploit available.	Patched by core rule	Y
CVE-2024-2353	Totolink X6000R 9.4.0cu.852_20230719 shttpd /cgi-bin/cstecgi.cgi setDiagnosisCfg ip os command injection	A vulnerability which was classified as critical has been found in Totolink X6000R 9.4.0cu.852_20230719. This issue affects the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi of the component shttpd. The manipulation of the argument ip leads to os command injection. The identification of this vulnerability is CVE-2024-2353. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-28353	TRENDnet TEW-827DRU 2.10B01 POST Request apply.cgi usapps.config.smb_admin_name command injection	A vulnerability was found in TRENDnet TEW-827DRU 2.10B01 and classified as critical. Affected by this issue is some unknown functionality of the file apply.cgi of the component POST Request Handler. The manipulation of the argument usapps.config.smb_admin_name leads to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		command injection. This vulnerability is handled as CVE-2024-28353. The attack needs to be done within the local network. There is no exploit available.		
CVE-2024-2812	Tenda AC15 15.03.05.18/15.03.20_multi /goform/WriteFacMac formWriteFacMac mac os command injection	A vulnerability was found in Tenda AC15 15.03.05.18/15.03.20_multi. It has been classified as critical. This affects the function formWriteFacMac of the file /goform/WriteFacMac. The manipulation of the argument mac leads to os command injection. This vulnerability is uniquely identified as CVE-2024-2812. It is possible to initiate the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-2851	Tenda AC15 15.03.05.18/15.03.20_multi /goform/setsambacfg formSetSambaConf usbName os command injection	A vulnerability was found in Tenda AC15 15.03.05.18/15.03.20_multi. It has been classified as critical. This affects the function formSetSambaConf of the file /goform/setsambacfg. The manipulation of the argument usbName leads to os command injection. This vulnerability is uniquely identified as CVE-2024-2851. It is possible to initiate the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-2854	Tenda AC18 15.03.05.05 /goform/setsambacfg formSetSambaConf usbName os	A vulnerability classified as critical has been found in Tenda AC18 15.03.05.05. Affected is the function	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	command injection	formSetSambaConf of the file /goform/setsambacfg. The manipulation of the argument usbName leads to os command injection. This vulnerability is traded as CVE-2024-2854. It is possible to launch the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-2853	Tenda AC10U 15.03.06.48/15.03.06.49 /goform/setsambacfg formSetSambaConf usbName os command injection	A vulnerability was found in Tenda AC10U 15.03.06.48/15.03.06.49. It has been rated as critical. This issue affects the function formSetSambaConf of the file /goform/setsambacfg. The manipulation of the argument usbName leads to os command injection. The identification of this vulnerability is CVE-2024-2853. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-36237	Bagisto up to 1.5.0 cross-site request forgery	A vulnerability classified as problematic has been found in Bagisto up to 1.5.0. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-36237. 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-2023-7203	Smart Forms Plugin up to 2.6.86 on WordPress AJAX Action cross-site request forgery	A vulnerability was found in Smart Forms Plugin up to 2.6.86 on WordPress. It has been rated as problematic. Affected by this issue is some unknown functionality of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-7203. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Patched by core rule	N
CVE-2024-27689	Stupid Simple CMS 1.2.4 /update-article.php cross-site request forgery	A vulnerability classified as problematic has been found in Stupid Simple CMS 1.2.4. Affected is an unknown function of the file /update-article.php. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-27689. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-27559	Stupid Simple CMS 1.2.4 /save_settings.php cross-site request forgery	A vulnerability was found in Stupid Simple CMS 1.2.4. It has been classified as problematic. This affects an unknown part of the file /save_settings.php. The manipulation leads	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to cross-site request forgery. This vulnerability is uniquely identified as CVE-2024-27559. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-2134	Bdtask Hospita AutoManager up to 20240223 Investigation Report /investigation/delete/ cross-site request forgery	A vulnerability has been found in Bdtask Hospita AutoManager up to 20240223 and classified as problematic. This vulnerability affects unknown code of the file /investigation/delete/ of the component Investigation Report Handler. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2024-2134. The attack can be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	N
CVE-2024-27694	FlyCMS 1.0 ztree_category_edit cross-site request forgery	A vulnerability was found in FlyCMS 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /system/share/ztree_category_edit. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2024-27694. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	N
CVE-2024-0779	Enjoy Social Feed Plugin up to 6.2.2 on WordPress cross-site request forgery	A vulnerability was found in Enjoy Social Feed Plugin up to 6.2.2 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2024-0779. The attack can be launched remotely. There is no exploit	Patched by core rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		available.		
CVE-2024-2817	Tenda AC15 15.03.05.18 SysToolRestoreSet fromSysToolRestoreSet cross-site request forgery	A vulnerability which was classified as problematic has been found in Tenda AC15 15.03.05.18. Affected by this issue is the function fromSysToolRestoreSet of the file /goform/SysToolRestoreSet. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2024-2817. The attack may be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	N
CVE-2024-2816	Tenda AC15 15.03.05.18 /goform/SysToolReboot fromSysToolReboot cross-site request forgery	A vulnerability classified as problematic was found in Tenda AC15 15.03.05.18. Affected by this vulnerability is the function fromSysToolReboot of the file /goform/SysToolReboot. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2024-2816. The attack can be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	N
CVE-2024-25808	Lychee 3.1.6 Create New Album cross-site request forgery (Issue 17)	A vulnerability which was classified as problematic was found in Lychee 3.1.6. Affected is an unknown function of the component Create New Album Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2024-25808. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	N

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-25386	laurelbridge DICOM Connectivity Framework up to 2.7.6a format_logfile.pl path traversal	A vulnerability has been found in laurelbridge DICOM Connectivity Framework up to 2.7.6a and classified as critical. This vulnerability affects unknown code of the file format_logfile.pl. The manipulation leads to path traversal. This vulnerability was named CVE-2024-25386. 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-2023-49544	Customer Support System 1.0 index.php page file inclusion	A vulnerability was found in Customer Support System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /customer_support/index.php. The manipulation of the argument page leads to file inclusion. The identification of this vulnerability is CVE-2023-49544. The attack can only be done within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-2150	SourceCodester Insurance Management System 1.0 page file inclusion	A vulnerability which was classified as critical has been found in SourceCodester Insurance Management System 1.0. This issue affects some unknown processing. The manipulation of the argument page leads	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to file inclusion. The identification of this vulnerability is CVE-2024-2150. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-2155	SourceCodester Best POS Management System 1.0 index.php page file inclusion	A vulnerability was found in SourceCodester Best POS Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file index.php. The manipulation of the argument page leads to file inclusion. The identification of this vulnerability is CVE-2024-2155. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-28088	LangChain up to 0.1.10 Configuration load_chain path path traversal	A vulnerability classified as critical was found in LangChain up to 0.1.10. This vulnerability affects the function load_chain of the component Configuration Handler. The manipulation of the argument path leads to path traversal. This vulnerability was named CVE-2024-28088. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-0818	paddle path traversal	A vulnerability was found in paddle and classified as critical. Affected by this issue is some unknown functionality. The manipulation leads to path traversal.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is handled as CVE-2024-0818. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-27317	Apache Pulsar up to 2.10.5/2.11.3/3.0.2/3.1.2/3.2.0 path traversal	A vulnerability was found in Apache Pulsar up to 2.10.5/2.11.3/3.0.2/3.1.2/3.2.0. It has been classified as critical. This affects an unknown part. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2024-27317. 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-2023-40280	OpenClinic 5.247.01 popup.jsp Page path traversal	A vulnerability which was classified as critical has been found in OpenClinic 5.247.01. This issue affects some unknown processing of the file popup.jsp. The manipulation of the argument Page leads to path traversal. The identification of this vulnerability is CVE-2023-40280. The attack can only be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2023-40279	OpenClinic GA 5.247.01 main.do Page path traversal	A vulnerability classified as critical has been found in OpenClinic GA 5.247.01. Affected is an unknown function of the file main.do. The manipulation of the argument Page	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		leads to path traversal. This vulnerability is traded as CVE-2023-40279. The attack needs to be done within the local network. There is no exploit available.		

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-1918	Beijing Baichuo Smart S42 Management Platform up to 20240219 userattestation.php hidwel unrestricted upload	A vulnerability has been found in Beijing Baichuo Smart S42 Management Platform up to 20240219 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /useratte/userattestation.php. The manipulation of the argument hidwel leads to unrestricted upload. This vulnerability is known as CVE-2024-1918. The attack can be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by custom rule	N
CVE-2023-6585	WP JobSearch Plugin up to 2.3.3 on WordPress unrestricted upload	A vulnerability which was classified as critical was found in WP JobSearch Plugin up to 2.3.3 on WordPress. This affects an unknown part. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-6585. It is possible to initiate the attack 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-2024-25291	Deskfiler 1.2.3 Plugin unrestricted upload	A vulnerability which was classified as problematic was found in Deskfiler 1.2.3. Affected is an unknown function of the component Plugin Handler. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2024-25291. The attack needs to be initiated within the local network. There is no exploit available.	Patched by custom rule	N
CVE-2024-25291	Deskfiler 1.2.3 Plugin unrestricted upload	A vulnerability which was classified as problematic was found in Deskfiler 1.2.3. Affected is an unknown function of the component Plugin Handler. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2024-25291. The attack needs to be initiated within the local network. There is no exploit available.	Patched by custom rule	N
CVE-2024-2059	SourceCodester Petrol Pump Management Software 1.0 service_crud.php photo unrestricted upload	A vulnerability was found in SourceCodester Petrol Pump Management Software 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/app/service_crud.php. The manipulation of the argument photo leads to unrestricted upload. This vulnerability is handled as CVE-2024-2059. The attack may be launched remotely.	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Furthermore there is an exploit available.		
CVE-2024-2058	SourceCodester Petrol Pump Management Software 1.0 /admin/app/product .php photo unrestricted upload	A vulnerability was found in SourceCodester Petrol Pump Management Software 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/app/product. php. The manipulation of the argument photo leads to unrestricted upload. This vulnerability is known as CVE-2024-2058. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by custom rule	N
CVE-2024-27747	Petrol Pump Management Software 1.0 profile.php email image unrestricted upload	A vulnerability classified as critical has been found in Petrol Pump Management Software 1.0. Affected is an unknown function of the file profile.php. The manipulation of the argument email image leads to unrestricted upload. This vulnerability is traded as CVE-2024-27747. Access to the local network is required for this attack. There is no exploit available.	Patched by custom rule	N
CVE-2024-2148	SourceCodester Online Mobile Management Store 1.0 /classes/Users.php img unrestricted upload	A vulnerability classified as critical has been found in SourceCodester Online Mobile Management Store 1.0. This affects an unknown part of the file /classes/Users.php.	Patched by custom rule	N

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The manipulation of the argument img leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2024-2148. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-1924	CodeAstro Membership Management System 1.0 get_membership_amount.php membershipTypeId sql injection	A vulnerability was found in CodeAstro Membership Management System 1.0. It has been classified as critical. This affects an unknown part of the file /get_membership_amount.php. The manipulation of the argument membershipTypeId leads to sql injection. This vulnerability is uniquely identified as CVE-2024-1924. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-1923	SourceCodester Simple Student Attendance System 1.0 List of Classes Page /ajax-api.php delete_class id sql injection	A vulnerability was found in SourceCodester Simple Student Attendance System 1.0 and classified as critical. Affected by this issue is the function delete_class of the file /ajax-api.php of the component List of Classes Page. The manipulation of the argument id with the input 1337&039;+or+11;--+ leads to sql injection. This vulnerability is handled as CVE-2024-1923. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-1927	SourceCodester Web-Based Student Clearance System 1.0 /Admin/login.php txtpassword sql injection	A vulnerability classified as critical was found in SourceCodester Web-Based Student Clearance System 1.0. Affected by this	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerability is an unknown functionality of the file /Admin/login.php. The manipulation of the argument txtpassword leads to sql injection. This vulnerability is known as CVE-2024-1927. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2024-1926	SourceCodester Free and Open Source Inventory Management System 1.0 search_sales_report.php customer sql injection	A vulnerability was found in SourceCodester Free and Open Source Inventory Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /app/ajax/search_sales_report.php. The manipulation of the argument customer leads to sql injection. The identification of this vulnerability is CVE-2024-1926. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-24027	Likeshop up to 2.5.6 getFansLists sql injection	A vulnerability which was classified as critical has been found in Likeshop up to 2.5.6. Affected by this issue is the function DistributionMemberLogic::getFansLists. The manipulation leads to sql injection. This vulnerability is handled as CVE-2024-24027. The attack needs to be initiated within the local network. 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-2024-1928	SourceCodester Web-Based Student Clearance System 1.0 Edit User Profile Page /admin/edit-admin.php Fullname sql injection	A vulnerability which was classified as critical has been found in SourceCodester Web-Based Student Clearance System 1.0. Affected by this issue is some unknown functionality of the file /admin/edit-admin.php of the component Edit User Profile Page. The manipulation of the argument Fullname leads to sql injection. This vulnerability is handled as CVE-2024-1928. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-24323	linlinjava litemall 1.8.0 AdminOrdercontroller.java nickname/consignee/orderSN/orderStatusArray sql injection	A vulnerability has been found in linlinjava litemall 1.8.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file AdminOrdercontroller.java. The manipulation of the argument nickname/consignee/orderSN/orderStatusArray leads to sql injection. This vulnerability is known as CVE-2024-24323. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-25350	PHPGurukul Zoo Management System 1.0 edit-ticket.php tickettype/tprice sql injection	A vulnerability was found in PHPGurukul Zoo Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /zms/admin/edit-ticket.php. The manipulation of the argument	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		tickettype/tprice leads to sql injection. This vulnerability is handled as CVE-2024-25350. The attack can only be initiated within the local network. There is no exploit available.		
CVE-2024-1971	Surya2Developer Online Shopping System 1.0 POST Parameter login.php password sql injection	A vulnerability has been found in Surya2Developer Online Shopping System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file login.php of the component POST Parameter Handler. The manipulation of the argument password with the input nochizplz&039;+or+1%3d1+limit+1%23 leads to sql injection. This vulnerability is known as CVE-2024-1971. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-25866	CodeAstro Membership Management System 1.0 index.php email sql injection	A vulnerability has been found in CodeAstro Membership Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file index.php. The manipulation of the argument email leads to sql injection. This vulnerability was named CVE-2024-25866. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-25867	CodeAstro	A vulnerability which	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Membership Management System 1.0 add_type.php membershipType/membershipAmount sql injection	was classified as critical has been found in CodeAstro Membership Management System 1.0. Affected by this issue is some unknown functionality of the file add_type.php. The manipulation of the argument membershipType/membershipAmount leads to sql injection. This vulnerability is handled as CVE-2024-25867. The attack may be launched remotely. There is no exploit available.	core rule	
CVE-2024-2015	ZhiCms 4.0 mcontroller.php getindexdata key sql injection	A vulnerability which was classified as critical has been found in ZhiCms 4.0. This issue affects the function getindexdata of the file app/index/controller/mcontroller.php. The manipulation of the argument key leads to sql injection. The identification of this vulnerability is CVE-2024-2015. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-25351	PHPGurukul Zoo Management System 1.0 changeimage.php editid sql injection	A vulnerability classified as critical was found in PHPGurukul Zoo Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /zms/admin/changeimage.php. The manipulation of the argument editid leads to sql injection. This vulnerability is known as CVE-2024-25351. The attack	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		needs to be done within the local network. There is no exploit available.		
CVE-2024-2014	Panabit Panalog 202103080942 sprog_upstatus.php id sql injection	A vulnerability classified as critical was found in Panabit Panalog 202103080942. This vulnerability affects unknown code of the file /Maintain/sprog_upstatus.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-2014. The attack can be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-25239	SourceCodester Employee Management System 1.0 POST Request login.php sql injection	A vulnerability classified as critical was found in SourceCodester Employee Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /emloyee_akpoly/Account/login.php of the component POST Request Handler. The manipulation leads to sql injection. This vulnerability is known as CVE-2024-25239. Access to the local network is required for this attack to succeed. There is no exploit available.	Patched by core rule	Y
CVE-2024-2022	Netentsec NS-ASG Application Security Gateway 6.3	A vulnerability was found in Netentsec NS-ASG Application	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	list_ipAddressPolicy.php GroupId sql injection	Security Gateway 6.3. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/list_ipAddressPolicy.php. The manipulation of the argument GroupId leads to sql injection. This vulnerability is known as CVE-2024-2022. The attack can be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-2021	Netentsec NS-ASG Application Security Gateway 6.3 list_localuser.php ResId sql injection	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3. It has been classified as critical. Affected is an unknown function of the file /admin/list_localuser.php. The manipulation of the argument ResId leads to sql injection. This vulnerability is traded as CVE-2024-2021. 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-2024-2060	SourceCodester Petrol Pump Management Software 1.0 login_crud.php email sql injection	A vulnerability classified as critical has been found in SourceCodester Petrol Pump Management Software 1.0. This affects an unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		part of the file /admin/app/login_crud .php. The manipulation of the argument email leads to sql injection. This vulnerability is uniquely identified as CVE-2024-2060. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		
CVE-2024-2074	Mini-Tmall up to 20231017 ?r=tmall/admin/user /1/1 orderBy sql injection	A vulnerability was found in Mini-Tmall up to 20231017 and classified as critical. This issue affects some unknown processing of the file rtmall/admin/user/1/1. The manipulation of the argument orderBy leads to sql injection. The identification of this vulnerability is CVE-2024-2074. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2067	SourceCodester Computer Inventory System 1.0 delete-computer.php computer sql injection	A vulnerability was found in SourceCodester Computer Inventory System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /endpoint/delete-computer.php. The manipulation of the argument computer leads to sql injection. This vulnerability was named CVE-2024-2067. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2061	SourceCodester Petrol Pump Management Software 1.0 /admin/edit_supplie	A vulnerability classified as critical was found in SourceCodester Petrol Pump Management	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	r.php id sql injection	Software 1.0. This vulnerability affects unknown code of the file /admin/edit_supplier.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-2061. The attack can be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-2069	SourceCodester FAQ Management System 1.0 /endpoint/delete-faq.php faq sql injection	A vulnerability classified as critical has been found in SourceCodester FAQ Management System 1.0. Affected is an unknown function of the file /endpoint/delete-faq.php. The manipulation of the argument faq leads to sql injection. This vulnerability is traded as CVE-2024-2069. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2062	SourceCodester Petrol Pump Management Software 1.0 edit_categories.php id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Petrol Pump Management Software 1.0. This issue affects some unknown processing of the file /admin/edit_categories.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-2062. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2073	SourceCodester	A vulnerability has	Patched by	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Block Inserter for Dynamic Content 1.0 view_post.php id sql injection	been found in SourceCodester Block Inserter for Dynamic Content 1.0 and classified as critical. This vulnerability affects unknown code of the file view_post.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-2073. The attack can be initiated remotely. Furthermore there is an exploit available.	core rule	
CVE-2024-27746	Petrol Pump Management Software 1.0 index.php email address sql injection	A vulnerability was found in Petrol Pump Management Software 1.0. It has been classified as critical. This affects an unknown part of the file index.php. The manipulation of the argument email address leads to sql injection. This vulnerability is uniquely identified as CVE-2024-27746. The attack can only be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-2147	SourceCodester Online Mobile Management Store 1.0 /admin/login.php username sql injection	A vulnerability was found in SourceCodester Online Mobile Management Store 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/login.php. The manipulation of the argument username leads to sql injection. This vulnerability is handled as CVE-2024-2147. The attack may be launched remotely.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Furthermore there is an exploit available.		
CVE-2024-2154	SourceCodester Online Mobile Management Store 1.0 view_product.php id sql injection	A vulnerability has been found in SourceCodester Online Mobile Management Store 1.0 and classified as critical. This vulnerability affects unknown code of the file view_product.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2024-2154. The attack can be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2153	SourceCodester Online Mobile Management Store 1.0 view_order.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Online Mobile Management Store 1.0. This affects an unknown part of the file /admin/orders/view_order.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-2153. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2152	SourceCodester Online Mobile Management Store 1.0 manage_product.php id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Online Mobile Management Store 1.0. Affected by this issue is some unknown functionality of the file /admin/product/manage_product.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 handled as CVE-2024-2152. The attack may be launched remotely. Furthermore there is an exploit available.		
CVE-2024-2168	SourceCodester Online Tours & Travels Management System 1.0 HTTP POST Request expense_category.php status sql injection	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/operations/expense_category.php of the component HTTP POST Request Handler. The manipulation of the argument status leads to sql injection. This vulnerability is traded as CVE-2024-2168. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-49968	Customer Support System 1.0 manage_department.php id sql injection	A vulnerability was found in Customer Support System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /customer_support/manage_department.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-49968. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-49970	Customer Support System 1.0 ajax.php subject sql injection	A vulnerability classified as critical has been found in Customer Support System 1.0. This affects an unknown part of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/customer_support/ajax.phpactionsave_ticket. The manipulation of the argument subject leads to sql injection. This vulnerability is uniquely identified as CVE-2023-49970. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2023-49547	Customer Support System 1.0 ajax.php username sql injection	A vulnerability was found in Customer Support System 1.0 and classified as critical. This issue affects some unknown processing of the file /customer_support/ajax.phpactionlogin. The manipulation of the argument username leads to sql injection. The identification of this vulnerability is CVE-2023-49547. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-49969	Customer Support System 1.0 index.php id sql injection	A vulnerability was found in Customer Support System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /customer_support/index.phppageedit_customer. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-49969. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-49548	Customer Support System 1.0 ajax.php lastname sql injection	A vulnerability was found in Customer Support System 1.0. It has been classified as critical. Affected is an unknown function of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/customer_support/ajax.phpactionsave_user. The manipulation of the argument lastname leads to sql injection. This vulnerability is traded as CVE-2023-49548. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2023-49546	Customer Support System 1.0 ajax.php email sql injection	A vulnerability has been found in Customer Support System 1.0 and classified as critical. This vulnerability affects unknown code of the file /customer_support/ajax.php. The manipulation of the argument email leads to sql injection. This vulnerability was named CVE-2023-49546. The attack can only be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-24375	JFinalCMS 5.0.0 /admin/admin name sql injection	A vulnerability which was classified as critical has been found in JFinalCMS 5.0.0. Affected by this issue is some unknown functionality of the file /admin/admin. The manipulation of the argument name leads to sql injection. This vulnerability is handled as CVE-2024-24375. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-49988	Hotel Booking Management 1.0 rooms.php npss sql injection	A vulnerability which was classified as critical has been found in Hotel Booking Management 1.0. This issue affects some	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown processing of the file rooms.php. The manipulation of the argument npss leads to sql injection. The identification of this vulnerability is CVE-2023-49988. The attack can only be initiated within the local network. There is no exploit available.		
CVE-2023-49989	Hotel Booking Management 1.0 update.php id sql injection	A vulnerability which was classified as critical was found in Hotel Booking Management 1.0. Affected is an unknown function of the file update.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-49989. The attack needs to be done within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-2329	Netentsec NS-ASG Application Security Gateway 6.3 list_resource_icon.php IconId sql injection	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/list_resource_icon.phpactiondelete. The manipulation of the argument IconId leads to sql injection. This vulnerability is handled as CVE-2024-2329. The attack may be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-2332	SourceCodester Online Mobile Management Store 1.0 HTTP GET Request manage_category.php id sql injection	A vulnerability was found in SourceCodester Online Mobile Management Store 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/maintenance/manage_category.php of the component HTTP GET Request Handler. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2024-2332. The attack may be initiated remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2333	CodeAstro Membership Management System 1.0 /add_members.php fullname sql injection	A vulnerability classified as critical has been found in CodeAstro Membership Management System 1.0. Affected is an unknown function of the file /add_members.php. The manipulation of the argument fullname leads to sql injection. This vulnerability is traded as CVE-2024-2333. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2330	Netentsec NS-ASG Application Security Gateway 6.3 /protocol/index.php IPAddr sql injection	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3. It has been classified as critical. This affects an unknown part of the file /protocol/index.php. The manipulation of the argument IPAddr 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-2024-2330. It is possible to initiate the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-28816	Student Information Chatbot 1.0 Login index.php username/password sql injection	A vulnerability was found in Student Information Chatbot 1.0. It has been classified as critical. Affected is an unknown function of the file index.php of the component Login. The manipulation of the argument username/password leads to sql injection. This vulnerability is traded as CVE-2024-28816. It is possible to launch the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y
CVE-2024-1068	404 Solution Plugin up to 2.35.7 on WordPress sql injection	A vulnerability was found in 404 Solution Plugin up to 2.35.7 on WordPress. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to sql injection. This vulnerability was named CVE-2024-1068. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		component.		
CVE-2024-24101	code-projects Scholars Tracking System 1.0 Eligibility Information Update sql injection	A vulnerability classified as critical has been found in code-projects Scholars Tracking System 1.0. This affects an unknown part of the component Eligibility Information Update. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2024-24101. The attack needs to be initiated within the local network. There is no exploit available.	Patched by core rule	Y
CVE-2024-2393	SourceCodester CRUD without Page Reload 1.0 add_user.php city sql injection	A vulnerability was found in SourceCodester CRUD without Page Reload 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file add_user.php. The manipulation of the argument city leads to sql injection. This vulnerability is known as CVE-2024-2393. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2418	SourceCodester Best POS Management System 1.0 /view_order.php id sql injection	A vulnerability was found in SourceCodester Best POS Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /view_order.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 known as CVE-2024-2418. The attack can be launched remotely. Furthermore there is an exploit available.		
CVE-2024-2514	MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 /login.php email sql injection	A vulnerability classified as critical was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. Affected by this vulnerability is an unknown functionality of the file /login.php. The manipulation of the argument email leads to sql injection. This vulnerability is known as CVE-2024-2514. The attack can be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-2532	MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 /admin/update-users.php id sql injection	A vulnerability classified as critical was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/update-users.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2024-2532. The attack can be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		way.		
CVE-2024-2527	MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 /admin/rooms.php room_id sql injection	A vulnerability was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/rooms.php. The manipulation of the argument room_id leads to sql injection. This vulnerability is handled as CVE-2024-2527. The attack may be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-2522	MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 /admin/booktime.php room_id sql injection	A vulnerability classified as critical has been found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. This affects an unknown part of the file /admin/booktime.php. The manipulation of the argument room_id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-2522. It is possible to initiate the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-2516	MAGESH-K21 Online-College-	A vulnerability which was classified as critical	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Event-Hall-Reservation-System 1.0 home.php id sql injection	was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. This affects an unknown part of the file home.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-2516. It is possible to initiate the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-2517	MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 book_history.php del_id sql injection	A vulnerability has been found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 and classified as critical. This vulnerability affects unknown code of the file book_history.php. The manipulation of the argument del_id leads to sql injection. This vulnerability was named CVE-2024-2517. The attack can be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-25227	ABO.CMS 5.8 Admin Login Page tb_login sql injection	A vulnerability which was classified as critical has been found in ABO.CMS 5.8. This issue affects some unknown processing of the component Admin Login Page. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument tb_login leads to sql injection. The identification of this vulnerability is CVE-2024-25227. The attack may be initiated remotely. There is no exploit available.		
CVE-2024-2556	SourceCodester Employee Task Management System 1.0 attendance-info.php user_id sql injection	A vulnerability was found in SourceCodester Employee Task Management System 1.0. It has been classified as critical. This affects an unknown part of the file attendance-info.php. The manipulation of the argument user_id leads to sql injection. This vulnerability is uniquely identified as CVE-2024-2556. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2568	heyewei JFinalCMS 5.0.0 Custom Data Page delete sql injection	A vulnerability has been found in heyewei JFinalCMS 5.0.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/div_data/deletedivId9 of the component Custom Data Page. The manipulation leads to sql injection. This vulnerability is known as CVE-2024-2568. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-0365	Fancy Product Designer Plugin up to 6.1.4 on WordPress sql	A vulnerability classified as critical was found in Fancy Product Designer Plugin up to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection	6.1.4 on WordPress. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2024-0365. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-2647	Netentsec NS-ASG Application Security Gateway 6.3 /admin/singlelogin.php loginId sql injection	A vulnerability which was classified as critical has been found in Netentsec NS-ASG Application Security Gateway 6.3. This issue affects some unknown processing of the file /admin/singlelogin.php. The manipulation of the argument loginId leads to sql injection. The identification of this vulnerability is CVE-2024-2647. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-2646	Netentsec NS-ASG Application Security Gateway 6.3 index.php check_VirtualSiteId sql injection	A vulnerability classified as critical was found in Netentsec NS-ASG Application Security Gateway 6.3. This vulnerability affects unknown code of the file /vpnweb/index.phpparaindex. The manipulation of the argument check_VirtualSiteId 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-2024-2646. The attack can be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-28595	Employee Management System 1.0 update-admin.php admin_id sql injection	A vulnerability was found in Employee Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file update-admin.php. The manipulation of the argument admin_id leads to sql injection. This vulnerability is known as CVE-2024-28595. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-28303	Open Source Medicine Ordering System 1.0 /admin/reports/index.php date sql injection	A vulnerability classified as critical was found in Open Source Medicine Ordering System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/reports/index.php. The manipulation of the argument date leads to sql injection. This vulnerability is known as CVE-2024-28303. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-28521	Netentsec NS-ASG Application Security Gateway 6.3.1 /singlelogin.php loginid sql injection	A vulnerability which was classified as critical was found in Netentsec NS-ASG Application Security Gateway 6.3.1.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This affects an unknown part of the file /singlelogin.php. The manipulation of the argument loginid leads to sql injection. This vulnerability is uniquely identified as CVE-2024-28521. It is possible to initiate the attack remotely. Furthermore there is an exploit available.		

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2024-25344	ITFlow settings.php cross site scripting	A vulnerability was found in ITFlow. It has been declared as problematic. This vulnerability affects unknown code of the file settings.php. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-25344. The attack can be initiated remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Patched by core rule	Y
CVE-2024-0435	mintplex-labs anything-llm up to 0.0.x Chat cross site scripting	A vulnerability was found in mintplex-labs anything-llm up to 0.0.x. It has been classified as problematic. This affects an unknown part of the component Chat Handler. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-0435. 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-2023-7115	Pagelayer Plugin up to 1.8.0 on WordPress Setting cross site scripting	A vulnerability was found in Pagelayer Plugin up to 1.8.0 on WordPress. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross site scripting. This vulnerability is known as CVE-2023-7115. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-25435	Md1health Md1patient 2.0.0 Msg cross site scripting	A vulnerability was found in Md1health Md1patient 2.0.0. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument Msg leads to cross site scripting. This vulnerability is handled as CVE-2024-25435. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-26542	Bonitasoft up to 7.14.7/7.15.6/8.0.2/9.0.1 Groups Display Name cross site scripting	A vulnerability classified as problematic has been found in Bonitasoft up to 7.14.7/7.15.6/8.0.2/9.0.1. This affects an unknown part. The manipulation of the argument Groups Display Name leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-26542. 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-2024-0700	Simple Tweet Plugin up to 1.4.0.2 on WordPress cross site scripting	A vulnerability which was classified as problematic was found in Simple Tweet Plugin	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		up to 1.4.0.2 on WordPress. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-0700. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-25202	PHPGurukul User Registration & Login and User Management System Search Bar cross site scripting	A vulnerability which was classified as problematic has been found in PHPGurukul User Registration & Login and User Management System 1.0. This issue affects some unknown processing of the component Search Bar. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-25202. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-1970	SourceCodester Online Learning System V2 1.0 /index.php page cross site scripting	A vulnerability which was classified as problematic was found in SourceCodester Online Learning System V2 1.0. Affected is an unknown function of the file /index.php. The manipulation of the argument page leads to cross site scripting. This vulnerability is traded as CVE-2024-1970. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-51802	Simple Student Attendance System 1.0 attendance_report class_month cross site scripting	A vulnerability has been found in Simple Student Attendance System 1.0 and classified as problematic. Affected	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		by this vulnerability is an unknown functionality of the file /php-attendance/attendance_report. The manipulation of the argument class_month leads to cross site scripting. This vulnerability is known as CVE-2023-51802. The attack can be launched remotely. There is no exploit available.		
CVE-2024-25868	CodeAstro Membership Management System 1.0 add_type.php membershipType cross site scripting	A vulnerability was found in CodeAstro Membership Management System 1.0. It has been classified as problematic. This affects an unknown part of the file add_type.php. The manipulation of the argument membershipType leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-25868. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-26476	open-emr up to 7.0.1 ereq_form.php formid cross site scripting (Issue 867)	A vulnerability was found in open-emr up to 7.0.1. It has been declared as problematic. This vulnerability affects unknown code of the file ereq_form.php. The manipulation of the argument formid leads to cross site scripting. This vulnerability was named CVE-2024-26476. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		It is recommended to upgrade the affected component.		
CVE-2024-25292	RenderTune 1.1.4 Upload Title cross site scripting	A vulnerability was found in RenderTune 1.1.4. It has been classified as problematic. This affects an unknown part. The manipulation of the argument Upload Title leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-25292. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-51800	School Fees Management System 1.0 main_settings add_new_parent cross site scripting	A vulnerability has been found in School Fees Management System 1.0 and classified as problematic. This vulnerability affects the function add_new_parent of the component main_settings. The manipulation of the argument phone/address/bank/acc_name/acc_number parameters/new_class/cname leads to cross site scripting. This vulnerability was named CVE-2023-51800. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-25292	RenderTune 1.1.4 Upload Title cross site scripting	A vulnerability was found in RenderTune 1.1.4. It has been classified as problematic. This affects an unknown part. The manipulation of the argument Upload Title leads to cross site scripting. This vulnerability is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		uniquely identified as CVE-2024-25292. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-25167	eblog 1.0 Comment description cross site scripting	A vulnerability which was classified as problematic has been found in eblog 1.0. Affected by this issue is some unknown functionality of the component Comment Handler. The manipulation of the argument description leads to cross site scripting. This vulnerability is handled as CVE-2024-25167. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-27734	CSZ CMS 1.3.0 Site Settings Site Name cross site scripting	A vulnerability has been found in CSZ CMS 1.3.0 and classified as problematic. This vulnerability affects unknown code of the component Site Settings. The manipulation of the argument Site Name leads to cross site scripting. This vulnerability was named CVE-2024-27734. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-27558	Stupid Simple CMS 1.2.4 Setting Blog Title cross site scripting	A vulnerability was found in Stupid Simple CMS 1.2.4. It has been declared as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation of the argument Blog Title leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability was named CVE-2024-27558. The attack can be initiated remotely. There is no exploit available.		
CVE-2024-2072	SourceCodester Flashcard Quiz App 1.0 update-flashcard.php question/answer cross site scripting	A vulnerability which was classified as problematic was found in SourceCodester Flashcard Quiz App 1.0. This affects an unknown part of the file /endpoint/update-flashcard.php. The manipulation of the argument question/answer leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-2072. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2071	SourceCodester FAQ Management System 1.0 Update FAQ Frequently Asked Question cross site scripting	A vulnerability which was classified as problematic has been found in SourceCodester FAQ Management System 1.0. Affected by this issue is some unknown functionality of the component Update FAQ. The manipulation of the argument Frequently Asked Question leads to cross site scripting. This vulnerability is handled as CVE-2024-2071. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-2068	SourceCodester Computer Inventory System 1.0 update-computer.php model cross site scripting	A vulnerability was found in SourceCodester Computer Inventory System 1.0. It has been rated as problematic. This issue affects some	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown processing of the file /endpoint/update-computer.php. The manipulation of the argument model leads to cross site scripting. The identification of this vulnerability is CVE-2024-2068. The attack may be initiated remotely. Furthermore there is an exploit available.		
CVE-2024-2063	SourceCodester Petrol Pump Management Software 1.0 profile_crud.php username cross site scripting	A vulnerability which was classified as problematic was found in SourceCodester Petrol Pump Management Software 1.0. Affected is an unknown function of the file /admin/app/profile_crud.php. The manipulation of the argument username leads to cross site scripting. This vulnerability is traded as CVE-2024-2063. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2075	SourceCodester Daily Habit Tracker 1.0 update-tracker.php day cross site scripting	A vulnerability was found in SourceCodester Daily Habit Tracker 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /endpoint/update-tracker.php. The manipulation of the argument day leads to cross site scripting. This vulnerability is known as CVE-2024-2075. The attack can be launched remotely.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Furthermore there is an exploit available.		
CVE-2024-2065	SourceCodester Barangay Population Monitoring System up to 1.0 update-resident.php full_name cross site scripting	A vulnerability was found in SourceCodester Barangay Population Monitoring System up to 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /endpoint/update-resident.php. The manipulation of the argument full_name leads to cross site scripting. This vulnerability is handled as CVE-2024-2065. The attack may be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2066	SourceCodester Computer Inventory System 1.0 add-computer.php model cross site scripting	A vulnerability was found in SourceCodester Computer Inventory System 1.0. It has been classified as problematic. This affects an unknown part of the file /endpoint/add-computer.php. The manipulation of the argument model leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-2066. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-27499	Bagisto 1.5.1 Product Review Option cross site scripting	A vulnerability which was classified as problematic was found in Bagisto 1.5.1. This affects an unknown part of the component Product Review Option. 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-2024-27499. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2024-2070	SourceCodester FAQ Management System 1.0 /endpoint/add-faq.php question/answer cross site scripting	A vulnerability classified as problematic was found in SourceCodester FAQ Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /endpoint/add-faq.php. The manipulation of the argument question/answer leads to cross site scripting. This vulnerability is known as CVE-2024-2070. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-25438	pkp ojs 3.3 Submission Module subject cross site scripting	A vulnerability which was classified as problematic has been found in pkp ojs 3.3. This issue affects some unknown processing of the component Submission Module. The manipulation of the argument subject leads to cross site scripting. The identification of this vulnerability is CVE-2024-25438. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-25434	pkp ojs 3.3 Publicname cross site scripting	A vulnerability was found in pkp ojs 3.3 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument Publicname leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is handled as CVE-2024-25434. The attack may be launched remotely. There is no exploit available.		
CVE-2024-27743	Petrol Pump Management Software 1.0 add_invoices.php Address cross site scripting	A vulnerability has been found in Petrol Pump Management Software 1.0 and classified as problematic. This vulnerability affects unknown code of the file add_invoices.php. The manipulation of the argument Address leads to cross site scripting. This vulnerability was named CVE-2024-27743. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-27744	Petrol Pump Management Software 1.0 profile.php image cross site scripting	A vulnerability was found in Petrol Pump Management Software 1.0. It has been classified as problematic. This affects an unknown part of the file profile.php. The manipulation of the argument image leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-27744. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-0968	langchain-ai chat-langchain cross site scripting	A vulnerability which was classified as problematic was found in langchain-ai chat-langchain. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		CVE-2024-0968. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.		
CVE-2024-24511	pkp ojs 3.4 Input Title cross site scripting	A vulnerability which was classified as problematic was found in pkp ojs 3.4. Affected is an unknown function of the component Input Title. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-24511. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-2133	Bdtask Isshue Multi Store eCommerce Shopping Cart Solution Manage Sale Page manage_invoice cross site scripting	A vulnerability which was classified as problematic was found in Bdtask Isshue Multi Store eCommerce Shopping Cart Solution 4.0. This affects an unknown part of the file /dashboard/Cinvoice/manage_invoice of the component Manage Sale Page. The manipulation of the argument Title leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-2133. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-2135	Bdtask Hospita AutoManager up to 20240223 Hospital Activities Page form Description cross site scripting	A vulnerability was found in Bdtask Hospita AutoManager up to 20240223 and classified as problematic. This issue affects some unknown processing of the file /hospital_activities/birt	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		h/form of the component Hospital Activities Page. The manipulation of the argument Description with the input <img srca onerroralert> leads to cross site scripting. The identification of this vulnerability is CVE-2024-2135. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2023-49540	Book Store Management System 1.0 history cross site scripting	A vulnerability classified as problematic has been found in Book Store Management System 1.0. Affected is an unknown function of the file /bsms_ci/index.php/history. The manipulation of the argument history leads to cross site scripting. This vulnerability is traded as CVE-2023-49540. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-2145	SourceCodester Online Mobile Management Store 1.0 update-tracker.php firstname cross site scripting	A vulnerability was found in SourceCodester Online Mobile Management Store 1.0. It has been classified as problematic. Affected is an unknown function of the file /endpoint/update-tracker.php. The manipulation of the argument firstname leads to cross site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		scripting. This vulnerability is traded as CVE-2024-2145. It is possible to launch the attack remotely. Furthermore there is an exploit available.		
CVE-2023-49539	Book Store Management System 1.0 category cross site scripting	A vulnerability was found in Book Store Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /bsms_ci/index.php/category. The manipulation of the argument category leads to cross site scripting. This vulnerability is known as CVE-2023-49539. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-25436	pkp ojs 3.3 Production Module subject cross site scripting	A vulnerability classified as problematic was found in pkp ojs 3.3. This vulnerability affects unknown code of the component Production Module. The manipulation of the argument subject leads to cross site scripting. This vulnerability was named CVE-2024-25436. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-24512	pkp ojs 3.4 Input Subtitle cross site scripting	A vulnerability has been found in pkp ojs 3.4 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Input	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Subtitle. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-24512. The attack can be launched remotely. There is no exploit available.		
CVE-2024-2146	SourceCodester Online Mobile Management Store 1.0 /?p=products search cross site scripting	A vulnerability was found in SourceCodester Online Mobile Management Store 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /pproducts. The manipulation of the argument search leads to cross site scripting. This vulnerability is known as CVE-2024-2146. The attack can be launched remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-27668	flusity CMS 2.33 Custom Blocks cross site scripting	A vulnerability was found in flusity CMS 2.33. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Custom Blocks. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-27668. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-27680	flusity CMS 2.33 Contact Form cross site scripting	A vulnerability classified as problematic has been found in flusity CMS 2.33. Affected is an unknown function of the component Contact	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Form. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-27680. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2024-27627	SuperCali 1.1.0 bad_password.php email cross site scripting (ID 177254)	A vulnerability was found in SuperCali 1.1.0 and classified as problematic. This issue affects some unknown processing of the file bad_password.php. The manipulation of the argument email leads to cross site scripting. The identification of this vulnerability is CVE-2024-27627. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-27626	Dotclear 2.29 Admin Panel cross site scripting (ID 177239)	A vulnerability was found in Dotclear 2.29. It has been classified as problematic. Affected is an unknown function of the component Admin Panel. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-27626. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-27625	CMS Made Simple 2.2.19 File Manager Module New directory cross site scripting (ID 177243)	A vulnerability which was classified as problematic was found in CMS Made Simple 2.2.19. This affects an unknown part of the component File Manager Module. The manipulation of the argument New directory 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-2024-27625. It is possible to initiate the attack remotely. There is no exploit available.		
CVE-2023-49977	Customer Support System 1.0 index.php address cross site scripting	A vulnerability was found in Customer Support System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /customer_support/index.phppagenew_customer. The manipulation of the argument address leads to cross site scripting. This vulnerability is handled as CVE-2023-49977. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-49971	Customer Support System 1.0 index.php firstname cross site scripting	A vulnerability was found in Customer Support System 1.0. It has been classified as problematic. Affected is an unknown function of the file /customer_support/index.phppagecustomer_list. The manipulation of the argument firstname leads to cross site scripting. This vulnerability is traded as CVE-2023-49971. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-49976	Customer Support System 1.0 index.php subject cross site scripting	A vulnerability which was classified as problematic was found in Customer Support System 1.0. Affected is an unknown function of the file /customer_support/index.phppagenew_ticket. The manipulation of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the argument subject leads to cross site scripting. This vulnerability is traded as CVE-2023-49976. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2023-49973	Customer Support System 1.0 index.php email cross site scripting	A vulnerability was found in Customer Support System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /customer_support/index.phppagecustomer_list. The manipulation of the argument email leads to cross site scripting. This vulnerability is known as CVE-2023-49973. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-49974	Customer Support System 1.0 index.php contact cross site scripting	A vulnerability classified as problematic has been found in Customer Support System 1.0. This affects an unknown part of the file /customer_support/index.phppagecustomer_list. The manipulation of the argument contact leads to cross site scripting. This vulnerability is uniquely identified as CVE-2023-49974. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-49986	School Fees Management System 1.0 /admin/parent name cross site scripting	A vulnerability classified as problematic has been found in School Fees Management System	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		1.0. Affected is an unknown function of the file /admin/parent. The manipulation of the argument name leads to cross site scripting. This vulnerability is traded as CVE-2023-49986. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2023-51281	Customer Support System 1.0 firstname/lastname/middlename/contact/address cross site scripting	A vulnerability was found in Customer Support System 1.0 and classified as problematic. This issue affects some unknown processing. The manipulation of the argument firstname/lastname/middlename/contact/address leads to cross site scripting. The identification of this vulnerability is CVE-2023-51281. The attack may be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-49987	School Fees Management System 1.0 /management/termtname cross site scripting	A vulnerability has been found in School Fees Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /management/term. The manipulation of the argument tname leads to cross site scripting. This vulnerability is known as CVE-2023-49987. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-28089	Hitron CODA-4582/AHKM-	A vulnerability was found in Hitron CODA-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	CODA4589 7.2.4.5.1b8 Device Location Page index.html#advanced_location cross site scripting	4582 and AHKM-CODA4589 7.2.4.5.1b8. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file index.htmladvanced_location of the component Device Location Page. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2024-28089. The attack can be launched remotely. There is no exploit available.		
CVE-2024-1487	Photos and Files Contest Gallery Plugin up to 21.3.0 on WordPress cross site scripting	A vulnerability was found in Photos and Files Contest Gallery Plugin up to 21.3.0 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-2024-1487. 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-2024-1401	Profile Box Shortcode and Widget Plugin up to 1.2.0 on WordPress cross site scripting	A vulnerability classified as problematic was found in Profile Box Shortcode and Widget Plugin up to 1.2.0 on WordPress. This vulnerability affects unknown code. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-1401.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The attack can be initiated remotely. There is no exploit available.		
CVE-2024-0561	Ultimate Posts Widget Plugin up to 2.3.0 on WordPress Widget Option cross site scripting	A vulnerability which was classified as problematic has been found in Ultimate Posts Widget Plugin up to 2.3.0 on WordPress. This issue affects some unknown processing of the component Widget Option Handler. The manipulation leads to cross site scripting. The identification of this vulnerability is CVE-2024-0561. 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-2024-1273	Starbox Plugin up to 3.4.x on WordPress cross site scripting	A vulnerability which was classified as problematic was found in Starbox Plugin up to 3.4.x on WordPress. This affects an unknown part. The manipulation leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-1273. 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-2023-42307	code-projects Exam Form Submission 1.0 Subject Name/Subject Code cross site scripting	A vulnerability was found in code-projects Exam Form Submission 1.0. It has been classified as problematic. Affected is an unknown function. The manipulation of the argument Subject	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Name/Subject Code leads to cross site scripting. This vulnerability is traded as CVE-2023-42307. It is possible to launch the attack remotely. There is no exploit available.		
CVE-2023-42308	code-projects Exam Form Submission 1.0 Manage Fastrack Subjects cross site scripting	A vulnerability was found in code-projects Exam Form Submission 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Manage Fastrack Subjects. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-42308. The attack can be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-26521	CE Phoenix up to 1.0.8.20 english.php cross site scripting	A vulnerability which was classified as problematic was found in CE Phoenix up to 1.0.8.20. Affected is an unknown function of the file english.php. The manipulation leads to basic cross site scripting. This vulnerability is traded as CVE-2024-26521. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-2194	WP Statistics Plugin up to 14.5 on WordPress cross site scripting	A vulnerability has been found in WP Statistics Plugin up to 14.5 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		cross site scripting. This vulnerability is known as CVE-2024-2194. The attack can be launched remotely. There is no exploit available.		
CVE-2024-25854	Sourcecodester Insurance Management System 1.0 Support Ticket Subject/Description cross site scripting	A vulnerability classified as problematic has been found in Sourcecodester Insurance Management System 1.0. Affected is an unknown function of the component Support Ticket Handler. The manipulation of the argument Subject/Description leads to cross site scripting. This vulnerability is traded as CVE-2024-25854. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-49453	Racktables up to 0.22.0 index.php cross site scripting	A vulnerability which was classified as problematic has been found in Racktables up to 0.22.0. Affected by this issue is some unknown functionality of the file index.php. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2023-49453. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-27703	Leantime 3.0.6 to-do title cross site scripting	A vulnerability was found in Leantime 3.0.6 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument to-do title leads to cross site scripting.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This vulnerability is handled as CVE-2024-27703. The attack may be launched remotely. There is no exploit available.		
CVE-2024-28676	DedeCMS 5.7 /dede/article_edit.php cross site scripting	A vulnerability which was classified as problematic was found in DedeCMS 5.7. Affected is an unknown function of the file /dede/article_edit.php. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-28676. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-28623	RiteCMS 3.0.0 Edit Section cross site scripting	A vulnerability classified as problematic was found in RiteCMS 3.0.0. This vulnerability affects unknown code of the component Edit Section Handler. The manipulation leads to cross site scripting. This vulnerability was named CVE-2024-28623. The attack can be initiated remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-28417	Webedition CMS 9.2.2.0 /webEdition/we_cmd.php cross site scripting	A vulnerability classified as problematic has been found in Webedition CMS 9.2.2.0. Affected is an unknown function of the file /webEdition/we_cmd.php. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-28417. It is possible to launch the attack remotely. There is no	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploit available.		
CVE-2024-2479	MHA Sistemas arMHAzena 9.6.0.0 Cadastro Page Query cross site scripting	A vulnerability classified as problematic has been found in MHA Sistemas arMHAzena 9.6.0.0. This affects an unknown part of the component Cadastro Page. The manipulation of the argument Query leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-2479. It is possible to initiate the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-2518	MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 book_history.php id cross site scripting	A vulnerability was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 and classified as problematic. This issue affects some unknown processing of the file book_history.php. The manipulation of the argument id leads to cross site scripting. The identification of this vulnerability is CVE-2024-2518. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-2521	MAGESH-K21 Online-College-	A vulnerability was found in MAGESH-K21	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Event-Hall-Reservation-System 1.0 /admin/bookdate.php id cross site scripting	Online-College-Event-Hall-Reservation-System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/bookdate.php. The manipulation of the argument id leads to cross site scripting. This vulnerability is handled as CVE-2024-2521. The attack may be launched remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-2530	MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 /admin/update-rooms.php id cross site scripting	A vulnerability was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/update-rooms.php. The manipulation of the argument id leads to cross site scripting. The identification of this vulnerability is CVE-2024-2530. The attack may be initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2024-2519	MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 navbar.php id cross site scripting	A vulnerability was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. It has been classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		problematic. Affected is an unknown function of the file navbar.php. The manipulation of the argument id leads to cross site scripting. This vulnerability is traded as CVE-2024-2519. It is possible to launch the attack remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-26454	Healthcare-Chatbot up to 9b7058a login.php email1/pwd1 cross site scripting	A vulnerability which was classified as problematic has been found in Healthcare-Chatbot up to 9b7058a. Affected by this issue is some unknown functionality of the file login.php. The manipulation of the argument email1/pwd1 leads to cross site scripting. This vulnerability is handled as CVE-2024-26454. The attack may be launched remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-2535	MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 /admin/users.php id cross site scripting	A vulnerability has been found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/users.php. The manipulation of the argument id leads to cross site scripting. This vulnerability was named CVE-2024-2535. The attack can be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		initiated remotely. Furthermore there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2024-2553	SourceCodester Product Review Rating System 1.0 Rate Product Your Name/Comment cross site scripting	A vulnerability which was classified as problematic was found in SourceCodester Product Review Rating System 1.0. Affected is an unknown function of the component Rate Product Handler. The manipulation of the argument Your Name/Comment leads to cross site scripting. This vulnerability is traded as CVE-2024-2553. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2024-27757	flusity CMS up to 2.45 tools/addons_model.php Gallery Name cross site scripting (GHSA-5843-5m74-7fqh)	A vulnerability classified as problematic has been found in flusity CMS up to 2.45. This affects an unknown part of the file tools/addons_model.php. The manipulation of the argument Gallery Name leads to cross site scripting. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability is uniquely identified as CVE-2024-27757. It is possible to initiate the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2024-0820	Jobs Plugin up to 2.7.3 on WordPress	A vulnerability which was classified as	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	cross site scripting	problematic has been found in Jobs Plugin up to 2.7.3 on WordPress. Affected by this issue is some unknown functionality. The manipulation leads to cross site scripting. This vulnerability is handled as CVE-2024-0820. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.		
CVE-2024-0711	Buttons Shortcode and Widget Plugin up to 1.16 on WordPress Shortcode Attribute cross site scripting	A vulnerability was found in Buttons Shortcode and Widget Plugin up to 1.16 on WordPress. It has been classified as problematic. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross site scripting. This vulnerability is traded as CVE-2024-0711. It is possible to launch the attack remotely. There is no exploit available.	Patched by core rule	Y
CVE-2023-40277	OpenClinic 5.247.01 login.jsp message cross site scripting	A vulnerability which was classified as problematic was found in OpenClinic 5.247.01. Affected is an unknown function of the file login.jsp. The manipulation of the argument message leads to cross site scripting. This vulnerability is traded as CVE-2023-40277. 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-2024-2685	Campcodes Online Job Finder System 1.0 index.php view cross site scripting	A vulnerability which was classified as problematic was found in Campcodes Online Job Finder System 1.0. This affects an unknown part of the file /admin/applicants/index.php. The manipulation of the argument view leads to cross site scripting. This vulnerability is uniquely identified as CVE-2024-2685. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Patched by core rule	Y
CVE-2023-7246	System Dashboard Plugin up to 2.8.9 on WordPress Configuration cross site scripting	A vulnerability has been found in System Dashboard Plugin up to 2.8.9 on WordPress and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Configuration Handler. The manipulation leads to cross site scripting. This vulnerability is known as CVE-2023-7246. 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-2024-25175	Kickdler prior 1.107.0 HTTP Response cross site scripting	A vulnerability classified as problematic was found in Kickdler. This vulnerability affects unknown code of the component HTTP Response Handler. The manipulation leads to cross site scripting. This vulnerability was	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		named CVE-2024-25175. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.		

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. The company has been funded by Tata Capital Growth Fund, is a “Great Place to Work” 2022 Winner in the Mid-Size category in India 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 3 consecutive years

A Customers' Choice for 2022 and 2023 Gartner® Peer Insights™