INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

February 2026

The total zero-day vulnerabilities count for February month: 484

Command Injection	SQL Injection	SSRF	Cross-Site Scripting	Malicious File Upload	Path Traversal
20	183	29	240	2	10

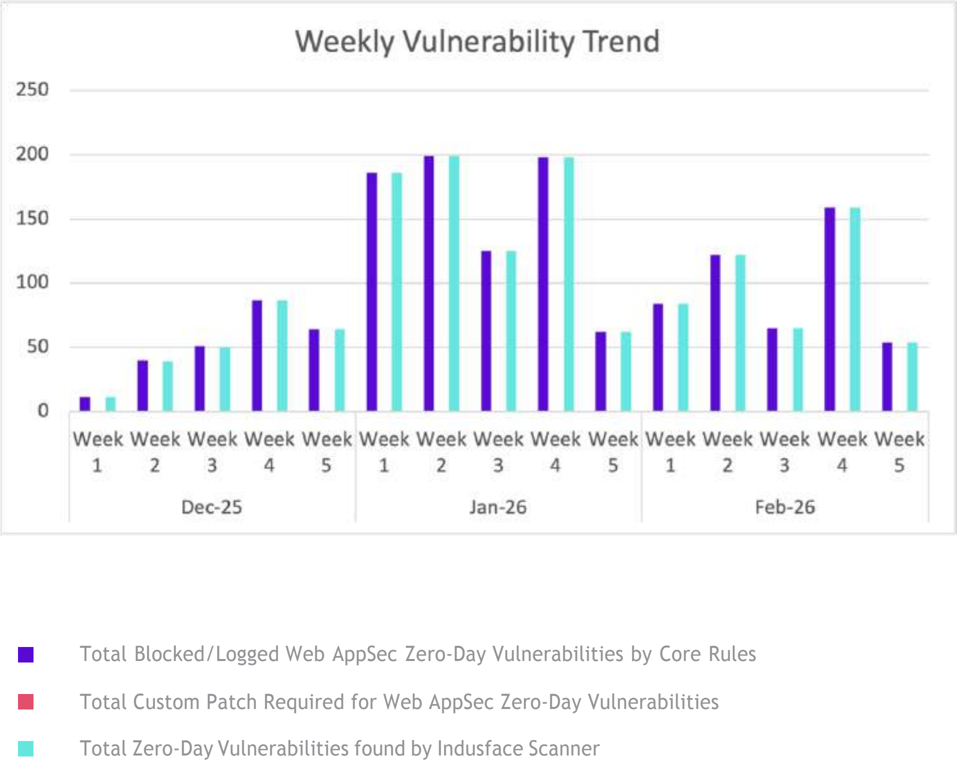
Zero-day vulnerabilities protected through core rules	484
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities found by Indusface WAS	484

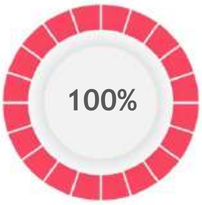
- To enable custom rules, please contact support@indusface.com
- Learn more about zero-day vulnerabilities, detection, and prevention, here

Vulnerability Trend:

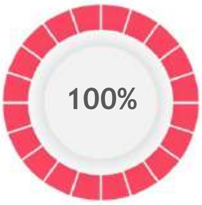
The weekly trend displays the total number of vulnerabilities discovered and the type of protection provided for the last quarter.

Weekly Vulnerability Trend



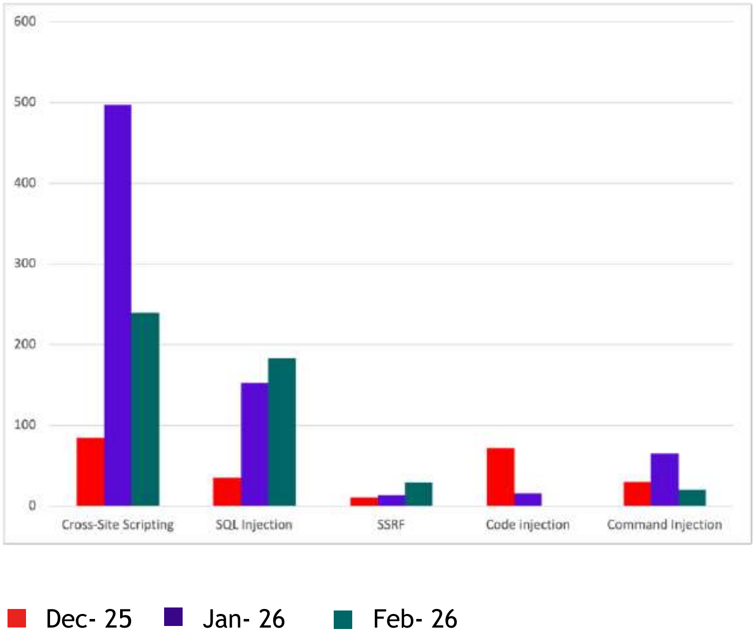


of the zero-day vulnerabilities were protected by the core rules in the last month



of the zero-day vulnerabilities were 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-2019-25441	thesystem 1.0 contains a command injection vulnerability that allows unauthenticated attackers to execute arbitrary system commands by submitting malicious input to the run_command endpoint.	thesystem 1.0 contains a command injection vulnerability that allows unauthenticated attackers to execute arbitrary system commands by submitting malicious input to the run_command endpoint. Attackers can send POST requests with shell commands in the command parameter to execute arbitrary code on the server without authentication.	Patched by core rule	Y
CVE-2020-37002	Ajenti 2.1.36 contains an authentication bypass vulnerability that allows remote attackers to execute arbitrary commands after successful login.	Ajenti 2.1.36 contains an authentication bypass vulnerability that allows remote attackers to execute arbitrary commands after successful login. Attackers can leverage the /api/terminal/create endpoint to send a netcat reverse shell payload targeting a specified IP and port.	Patched by core rule	Y
CVE-2020-37012	Tea LaTex 1.0 contains a remote code execution vulnerability that allows	Tea LaTex 1.0 contains a remote code execution vulnerability that allows	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	unauthenticated attackers to execute arbitrary shell commands through the /api.php endpoint.	unauthenticated attackers to execute arbitrary shell commands through the /api.php endpoint. Attackers can craft a malicious LaTeX payload with shell commands that are executed when processed by the application's tex2png API action.		
CVE-2020-37123	Pinger 1.0 contains a remote code execution vulnerability that allows attackers to inject shell commands through the ping and socket parameters.	Pinger 1.0 contains a remote code execution vulnerability that allows attackers to inject shell commands through the ping and socket parameters. Attackers can exploit the unsanitized input in ping.php to write arbitrary PHP files and execute system commands by appending shell metacharacters.	Patched by core rule	Y
CVE-2025-65791	ZoneMinder v1.36.34 is vulnerable to Command Injection in web/views/image.php.	ZoneMinder v1.36.34 is vulnerable to Command Injection in web/views/image.php. The application passes unsanitized user input directly to the exec() function.	Patched by core rule	Y
CVE-2025-69212	OpenSTAManager is an open source management software for technical assistance and invoicing.	OpenSTAManager is an open source management software for technical assistance and invoicing. In 2.9.8 and earlier, a critical OS Command Injection vulnerability exists in the P7M (signed XML) file decoding functionality. An authenticated attacker can upload a ZIP file containing a .p7m file with a malicious filename to execute arbitrary system commands on the server.	Patched by core rule	Y
CVE-2026-1412	A vulnerability has been found in Sangfor Operation and Maintenance Security Management System up to 3.0.12.	A vulnerability has been found in Sangfor Operation and Maintenance Security Management System up to 3.0.12. The impacted element is an unknown function of the file /fort/audit/get_clip_img of the component HTTP POST Request Handler. Such manipulation of the argument frame/dirno leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-1414	A vulnerability was determined in Sangfor Operation and Maintenance Security	A vulnerability was determined in Sangfor Operation and Maintenance Security Management	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Management System up to 3.0.12.	System up to 3.0.12. This impacts the function getInformation of the file /equipment/get_Information of the component HTTP POST Request Handler. Executing a manipulation of the argument fortEquipmentIp can lead to command injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.		
CVE-2026-2560	A vulnerability has been found in kalcaddle kodbox up to 1.64.05.	A vulnerability has been found in kalcaddle kodbox up to 1.64.05. The impacted element is the function run of the file plugins/fileThumb/lib/VideoResize.class.php of the component Media File Preview Plugin. Such manipulation of the argument localFile leads to os command injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-2686	A security vulnerability has been detected in SECCN Dingcheng G10 3.1.0.181203.	A security vulnerability has been detected in SECCN Dingcheng G10 3.1.0.181203. This impacts the function qq of the file /cgi-bin/session_login.cgi. The manipulation of the argument User leads to os command injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-27626	OliveTin gives access to predefined shell commands from a web interface.	OliveTin gives access to predefined shell commands from a web interface. In versions up to and including 3000.10.0, OliveTin's shell mode safety check (`checkShellArgumentSafety`) blocks several dangerous argument types but not `password`. A user supplying a `password`-typed argument can inject shell metacharacters that execute arbitrary OS commands. A second independent vector allows unauthenticated RCE via webhook-extracted JSON values that skip type safety checks entirely before reaching `sh -c`. When	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exploiting vector 1, any authenticated user (registration enabled by default, `authType: none` by default) can execute arbitrary OS commands on the OliveTin host with the permissions of the OliveTin process. When exploiting vector 2, an unauthenticated attacker can achieve the same if the instance receives webhooks from external sources, which is a primary OliveTin use case. When an attacker exploits both vectors, this results in unauthenticated RCE on any OliveTin instance using Shell mode with webhook-triggered actions. As of time of publication, a patched version is not available.		
CVE-2026-2846	A security vulnerability has been detected in UTT HiPER 520 1.7.7-160105.	A security vulnerability has been detected in UTT HiPER 520 1.7.7-160105. This impacts the function sub_44D264 of the file /goform/formPdbUpConfig of the component Web Management Interface. The manipulation of the argument policyNames leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-2847	A vulnerability was detected in UTT HiPER 520 1.7.7-160105.	A vulnerability was detected in UTT HiPER 520 1.7.7-160105. Affected is the function sub_44EFB4 of the file /goform/formReleaseConnect of the component Web Management Interface. The manipulation of the argument Isp_Name results in os command injection. The attack can be launched remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-2944	A security flaw has been discovered in Tosei Online Store Management System „Éç„ÉÉ„ÉàÂʃóËàóÁÆ°ÁêÜ„Ç∑„Çπ„ÉÜ„É† 1.01.	A security flaw has been discovered in Tosei Online Store Management System „Éç„ÉÉ„ÉàÂʃóËàóÁÆ°ÁêÜ„Ç∑„Çπ„ÉÜ„É† 1.01. Affected is the function system of the file /cgi-bin/monitor.php of the component HTTP POST Request Handler. Performing a manipulation of the argument DevId results in os command injection. The attack may be initiated remotely. The exploit has	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2026-2952	A flaw has been found in Vaelsys 4.1.0.	A flaw has been found in Vaelsys 4.1.0. This vulnerability affects unknown code of the file /tree/tree_server.php of the component HTTP POST Request Handler. This manipulation of the argument xajaxargs causes os command injection. The attack is possible to be carried out remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-2956	A security flaw has been discovered in qinming99 dst-admin up to 1.5.0.	A security flaw has been discovered in qinming99 dst-admin up to 1.5.0. This affects the function revertBackup of the file /home/restore. The manipulation of the argument Name results in command injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-3040	A vulnerability was identified in DrayTek Vigor 300B up to 1.5.1.6.	A vulnerability was identified in DrayTek Vigor 300B up to 1.5.1.6. This affects the function cgiGetFile of the file /cgi-bin/mainfunction.cgi/uploadlangs of the component Web Management Interface. The manipulation of the argument File leads to os command injection. The attack may be initiated remotely. The exploit is publicly available and might be used. The vendor confirms that "300B is EoL, and this is an authenticated vulnerability. We don't plan to fix it." This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2026-3064	A security vulnerability has been detected in HummerRisk up to 1.5.0.	A security vulnerability has been detected in HummerRisk up to 1.5.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Affected by this issue is some unknown functionality of the file ResourceCreateService.java of the component Cloud Task Scheduler. Such manipulation of the argument regionId leads to command injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2026-3065	A vulnerability was detected in HummerRisk up to 1.5.0.	A vulnerability was detected in HummerRisk up to 1.5.0. This affects the function CommandUtils.commonExecCmdWithResult of the file CloudTaskService.java of the component Cloud Task Dry-run. Performing a manipulation of the argument fileName results in command injection. Remote exploitation of the attack is possible. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-3066	A flaw has been found in HummerRisk up to 1.5.0.	A flaw has been found in HummerRisk up to 1.5.0. This vulnerability affects the function fixedCommand of the file hummer-common/hummer-common-core/src/main/java/com/hummer/common/core/utils/PlatformUtils.java of the component Cloud Compliance Scanning. Executing a manipulation can lead to command injection. The attack can be executed remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2019-25260	OXID eShop versions 6.x prior to 6.3.4 contains a SQL injection vulnerability in the 'sorting' parameter that allows attackers to insert malicious database content.	OXID eShop versions 6.x prior to 6.3.4 contains a SQL injection vulnerability in the 'sorting' parameter that allows attackers to insert malicious database content. Attackers can exploit the vulnerability by manipulating the sorting parameter to inject PHP code into the database and execute arbitrary code through crafted URLs.	Patched by core rule	Y
CVE-2019-25298	html5_snmp 1.11 contains multiple SQL injection vulnerabilities that allow attackers to manipulate database queries through Router_ID and Router_IP parameters.	html5_snmp 1.11 contains multiple SQL injection vulnerabilities that allow attackers to manipulate database queries through Router_ID and Router_IP parameters. Attackers can exploit error-based, time-based, and union-based injection techniques to potentially extract or modify database information by sending crafted payloads.	Patched by core rule	Y
CVE-2019-25299	RimbaLinux AhadPOS 1.11 contains a SQL injection vulnerability in the 'alamatCustomer' parameter that allows attackers to manipulate database queries through crafted POST requests.	RimbaLinux AhadPOS 1.11 contains a SQL injection vulnerability in the 'alamatCustomer' parameter that allows attackers to manipulate database queries through crafted POST requests. Attackers can exploit time-based and boolean-based blind SQL injection techniques to extract information or potentially interact with the underlying database.	Patched by core rule	Y
CVE-2019-25300	thejshen Globitek CMS 1.4 contains a SQL injection vulnerability that allows attackers to manipulate database queries through the 'id' GET parameter.	thejshen Globitek CMS 1.4 contains a SQL injection vulnerability that allows attackers to manipulate database queries through the 'id' GET parameter. Attackers can exploit boolean-based, time-based, and UNION-based SQL injection techniques to potentially extract or modify database information.	Patched by core rule	Y
CVE-2019-25303	TheJshen ContentManagementSystem 1.04 contains a SQL injection vulnerability that allows attackers to manipulate database queries through the 'id' GET parameter.	TheJshen ContentManagementSystem 1.04 contains a SQL injection vulnerability that allows attackers to manipulate database queries through the 'id' GET parameter. Attackers can exploit boolean-based, time-based, and UNION-based SQL	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		injection techniques to extract or manipulate database information by crafting malicious query payloads.		
CVE-2019-25320	E Learning Script 1.0 contains an authentication bypass vulnerability that allows attackers to access the dashboard without valid credentials by manipulating login parameters.	E Learning Script 1.0 contains an authentication bypass vulnerability that allows attackers to access the dashboard without valid credentials by manipulating login parameters. Attackers can exploit the /login.php file by sending a specific payload '=''or' to bypass authentication and gain unauthorized access to the system.	Patched by core rule	Y
CVE-2019-25325	Thrive Smart Home 1.1 contains an SQL injection vulnerability in the checklogin.php endpoint that allows unauthenticated attackers to bypass authentication by manipulating the 'user' POST parameter.	Thrive Smart Home 1.1 contains an SQL injection vulnerability in the checklogin.php endpoint that allows unauthenticated attackers to bypass authentication by manipulating the 'user' POST parameter. Attackers can inject malicious SQL code like ' or 1=1# to manipulate login queries and gain unauthorized access to the application.	Patched by core rule	Y
CVE-2019-25335	PRO-7070 Hazƒ±r Profesyonel Web Sitesi version 1.0 contains an authentication bypass vulnerability in the administration panel login page.	PRO-7070 Hazƒ±r Profesyonel Web Sitesi version 1.0 contains an authentication bypass vulnerability in the administration panel login page. Attackers can bypass authentication by using '=' 'or' as both username and password to gain unauthorized access to the administrative interface.	Patched by core rule	Y
CVE-2019-25346	TheSystem 1.0 contains a SQL injection vulnerability that allows attackers to bypass authentication by manipulating the 'server_name' parameter.	TheSystem 1.0 contains a SQL injection vulnerability that allows attackers to bypass authentication by manipulating the 'server_name' parameter. Attackers can inject malicious SQL code like ' or '1=1 to retrieve unauthorized database records and potentially access sensitive system information.	Patched by core rule	Y
CVE-2019-25347	thesystem App 1.0 contains a SQL injection vulnerability that allows attackers to bypass authentication by manipulating the username parameter.	thesystem App 1.0 contains a SQL injection vulnerability that allows attackers to bypass authentication by manipulating the username parameter. Attackers can inject malicious SQL code like ' or '1=1 to the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		username field to gain unauthorized access to user accounts.		
CVE-2019-25348	Computrols CBAS-Web 19.0.0 contains a boolean-based blind SQL injection vulnerability in the 'id' parameter that allows authenticated attackers to manipulate database queries.	Computrols CBAS-Web 19.0.0 contains a boolean-based blind SQL injection vulnerability in the 'id' parameter that allows authenticated attackers to manipulate database queries. Attackers can exploit the vulnerability by crafting boolean-based SQL injection payloads in the 'id' parameter of the servers endpoint to extract or infer database information.	Patched by core rule	Y
CVE-2019-25366	microASP Portal+ CMS contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code into the explode_tree parameter.	microASP Portal+ CMS contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code into the explode_tree parameter. Attackers can send crafted requests to pagina.phtml with SQL injection payloads using extractvalue and concat functions to extract sensitive database information like the current database name.	Patched by core rule	Y
CVE-2019-25391	Ashop Shopping Cart Software contains a time-based blind SQL injection vulnerability that allows attackers to manipulate database queries through the blacklistitemid parameter.	Ashop Shopping Cart Software contains a time-based blind SQL injection vulnerability that allows attackers to manipulate database queries through the blacklistitemid parameter. Attackers can send POST requests to the admin/bannedcustomers.php endpoint with crafted SQL payloads using SLEEP functions to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25431	delpino73 Blue-Smiley-Organizer 1.32 contains an SQL injection vulnerability in the datetime parameter that allows unauthenticated attackers to manipulate database queries.	delpino73 Blue-Smiley-Organizer 1.32 contains an SQL injection vulnerability in the datetime parameter that allows unauthenticated attackers to manipulate database queries. Attackers can inject SQL code through POST requests to extract sensitive data using boolean-based blind and time-based blind techniques, or write files to the server using INTO OUTFILE statements.	Patched by core rule	Y
CVE-2019-25432	Part-DB 0.4 contains an authentication bypass vulnerability that allows unauthenticated	Part-DB 0.4 contains an authentication bypass vulnerability that allows unauthenticated attackers to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	attackers to login by injecting SQL syntax into authentication parameters.	login by injecting SQL syntax into authentication parameters. Attackers can submit a single quote followed by 'or' in the login form to bypass credential validation and gain unauthorized access to the application.		
CVE-2019-25433	XOOPS CMS 2.5.9 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the cid parameter.	XOOPS CMS 2.5.9 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the cid parameter. Attackers can send GET requests to the gerar_pdf.php endpoint with malicious cid values to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25438	LabCollector 5.423 contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to execute arbitrary SQL commands by injecting malicious code through POST parameters.	LabCollector 5.423 contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to execute arbitrary SQL commands by injecting malicious code through POST parameters. Attackers can submit crafted SQL payloads in the login parameter of login.php or the user_name parameter of retrieve_password.php to extract sensitive database information without authentication.	Patched by core rule	Y
CVE-2019-25439	NoviSmart CMS contains an SQL injection vulnerability that allows remote attackers to execute arbitrary SQL queries by injecting malicious code through the Referer HTTP header field.	NoviSmart CMS contains an SQL injection vulnerability that allows remote attackers to execute arbitrary SQL queries by injecting malicious code through the Referer HTTP header field. Attackers can craft requests with time-based SQL injection payloads in the Referer header to extract sensitive database information or cause denial of service.	Patched by core rule	Y
CVE-2019-25440	WebIncorp ERP contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the prod_id parameter.	WebIncorp ERP contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the prod_id parameter. Attackers can send GET requests to product_detail.php with malicious prod_id values to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25442	Web Wiz Forums 12.01	Web Wiz Forums 12.01	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the PF parameter.	contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the PF parameter. Attackers can send GET requests to member_profile.asp with malicious PF values to extract sensitive database information.	rule	
CVE-2019-25443	Inventory Webapp contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through GET parameters.	Inventory Webapp contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through GET parameters. Attackers can supply malicious SQL payloads in the name, description, quantity, or cat_id parameters to add-item.php to execute arbitrary database commands.	Patched by core rule	Y
CVE-2019-25444	Fiverr Clone Script 1.2.2 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the page parameter.	Fiverr Clone Script 1.2.2 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the page parameter. Attackers can supply malicious SQL syntax in the page parameter to extract sensitive database information or modify database contents.	Patched by core rule	Y
CVE-2019-25446	DIGIT CENTRIS ERP contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the datum1, datum2, KID, and PID parameters.	DIGIT CENTRIS ERP contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the datum1, datum2, KID, and PID parameters. Attackers can send POST requests to /korisnikinfo.php with malicious SQL syntax in these parameters to extract or modify sensitive database information.	Patched by core rule	Y
CVE-2019-25450	Dolibarr ERP/CRM 10.0.1 contains multiple SQL injection vulnerabilities that allow authenticated attackers to manipulate database queries by injecting SQL code through POST parameters.	Dolibarr ERP/CRM 10.0.1 contains multiple SQL injection vulnerabilities that allow authenticated attackers to manipulate database queries by injecting SQL code through POST parameters. Attackers can inject malicious SQL through parameters like actioncode, demand_reason_id, and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		availability_id in card.php endpoints to extract sensitive database information using boolean-based blind, error-based, and time-based blind techniques.		
CVE-2019-25452	Dolibarr ERP/CRM 10.0.1 contains an SQL injection vulnerability in the elemid POST parameter of the viewcat.php endpoint that allows unauthenticated attackers to execute arbitrary SQL queries.	Dolibarr ERP/CRM 10.0.1 contains an SQL injection vulnerability in the elemid POST parameter of the viewcat.php endpoint that allows unauthenticated attackers to execute arbitrary SQL queries. Attackers can submit crafted POST requests with malicious SQL payloads in the elemid parameter to extract sensitive database information using error-based or time-based blind SQL injection techniques.	Patched by core rule	Y
CVE-2019-25455	Web Ofisi E-Ticaret v3 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'a' parameter.	Web Ofisi E-Ticaret v3 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'a' parameter. Attackers can send GET requests to with malicious 'a' parameter values to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25456	Web Ofisi Emlak v2 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'ara' GET parameter.	Web Ofisi Emlak v2 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'ara' GET parameter. Attackers can send requests to with time-based SQL injection payloads to extract sensitive database information or cause denial of service.	Patched by core rule	Y
CVE-2019-25457	Web Ofisi Firma v13 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'oz' array parameter.	Web Ofisi Firma v13 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'oz' array parameter. Attackers can send GET requests to category pages with malicious 'oz[]' values using time-based blind SQL injection payloads to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25458	Web Ofisi Firma Rehberi v1 contains an SQL	Web Ofisi Firma Rehberi v1 contains an SQL injection	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through GET parameters.	vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through GET parameters. Attackers can send requests to with malicious payloads in the 'il', 'kat', or 'kelime' parameters to extract sensitive database information or perform time-based blind SQL injection attacks.		
CVE-2019-25459	Web Ofisi Emlak V2 contains multiple SQL injection vulnerabilities in the endpoint that allow unauthenticated attackers to manipulate database queries through GET parameters.	Web Ofisi Emlak V2 contains multiple SQL injection vulnerabilities in the endpoint that allow unauthenticated attackers to manipulate database queries through GET parameters. Attackers can inject SQL code into parameters like emlak_durumu, emlak_tipi, il, ilce, kelime, and semt to extract sensitive database information or perform time-based blind SQL injection attacks.	Patched by core rule	Y
CVE-2019-25460	Web Ofisi Platinum E-Ticaret v5 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'q' GET parameter.	Web Ofisi Platinum E-Ticaret v5 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'q' GET parameter. Attackers can send requests to the arama endpoint with malicious 'q' values using time-based SQL injection techniques to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25461	Web Ofisi Platinum E-Ticaret v5 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'q' parameter.	Web Ofisi Platinum E-Ticaret v5 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'q' parameter. Attackers can send POST requests to the ajax/productsFilterSearch endpoint with malicious 'q' values using time-based blind SQL injection techniques to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25462	Web Ofisi Rent a Car v3 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code	Web Ofisi Rent a Car v3 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'klima'	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	through the 'klima' parameter.	parameter. Attackers can send GET requests to with malicious 'klima' values to extract sensitive database information or cause denial of service.		
CVE-2020-36945	WebDamn User Registration Login System contains a SQL injection vulnerability that allows unauthenticated attackers to bypass login authentication by manipulating email credentials.	WebDamn User Registration Login System contains a SQL injection vulnerability that allows unauthenticated attackers to bypass login authentication by manipulating email credentials. Attackers can inject the payload '<email>' OR '1'='1' in both username and password fields to gain unauthorized access to the user panel.	Patched by core rule	Y
CVE-2020-36947	LibreNMS 1.46 contains an authenticated SQL injection vulnerability in the MAC accounting graph endpoint that allows remote attackers to extract database information.	LibreNMS 1.46 contains an authenticated SQL injection vulnerability in the MAC accounting graph endpoint that allows remote attackers to extract database information. Attackers can exploit the vulnerability by manipulating the 'sort' parameter with crafted SQL injection techniques to retrieve sensitive database contents through time-based blind SQL injection.	Patched by core rule	Y
CVE-2020-36951	Phpscript-sgh 0.1.0 contains a time-based blind SQL injection vulnerability in the admin interface that allows attackers to manipulate database queries through the 'id' parameter.	Phpscript-sgh 0.1.0 contains a time-based blind SQL injection vulnerability in the admin interface that allows attackers to manipulate database queries through the 'id' parameter. Attackers can exploit this vulnerability by crafting malicious payloads that trigger time delays, enabling them to extract sensitive database information through conditional sleep techniques.	Patched by core rule	Y
CVE-2020-36972	SmartBlog 2.0.1 contains a blind SQL injection vulnerability in the 'id_post' parameter of the details controller that allows attackers to extract database information.	SmartBlog 2.0.1 contains a blind SQL injection vulnerability in the 'id_post' parameter of the details controller that allows attackers to extract database information. Attackers can systematically test and retrieve database contents by injecting crafted SQL queries that compare character-by-character of database information.	Patched by core rule	Y
CVE-2020-36999	Elaniin CMS 1.0 contains an authentication bypass vulnerability that allows attackers to access the	Elaniin CMS 1.0 contains an authentication bypass vulnerability that allows attackers to access the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	dashboard by manipulating the login page with SQL injection.	dashboard by manipulating the login page with SQL injection. Attackers can bypass authentication by sending crafted email and password parameters with '=''or' payload to login.php, granting unauthorized access to the system.		
CVE-2020-37004	Ultimate Project Manager CRM PRO 2.0.5 contains a blind SQL injection vulnerability that allows attackers to extract usernames and password hashes from the tbl_users database table.	Ultimate Project Manager CRM PRO 2.0.5 contains a blind SQL injection vulnerability that allows attackers to extract usernames and password hashes from the tbl_users database table. Attackers can exploit the /frontend/get_article_suggestion/ endpoint by crafting malicious search parameters to progressively guess and retrieve user credentials through boolean-based inference techniques.	Patched by core rule	Y
CVE-2020-37005	TimeClock Software 1.01 contains an authenticated time-based SQL injection vulnerability that allows attackers to enumerate valid usernames by manipulating the 'notes' parameter.	TimeClock Software 1.01 contains an authenticated time-based SQL injection vulnerability that allows attackers to enumerate valid usernames by manipulating the 'notes' parameter. Attackers can inject conditional time delays in the add_entry.php endpoint to determine user existence by measuring response time differences.	Patched by core rule	Y
CVE-2020-37006	berliCRM 1.0.24 contains a SQL injection vulnerability in the 'src_record' parameter that allows remote attackers to manipulate database queries.	berliCRM 1.0.24 contains a SQL injection vulnerability in the 'src_record' parameter that allows remote attackers to manipulate database queries. Attackers can inject malicious SQL code through a crafted POST request to the index.php endpoint to potentially extract or modify database information.	Patched by core rule	Y
CVE-2020-37033	Infor Storefront B2B 1.0 contains a SQL injection vulnerability that allows attackers to manipulate database queries through the 'usr_name' parameter in login requests.	Infor Storefront B2B 1.0 contains a SQL injection vulnerability that allows attackers to manipulate database queries through the 'usr_name' parameter in login requests. Attackers can exploit the vulnerability by injecting malicious SQL code into the 'usr_name' parameter to potentially extract or modify database information.	Patched by core rule	Y
CVE-2020-37035	e-Learning PHP Script 0.1.0 contains a SQL injection vulnerability in	e-Learning PHP Script 0.1.0 contains a SQL injection vulnerability in the search	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	the search functionality that allows attackers to manipulate database queries through unvalidated user input.	functionality that allows attackers to manipulate database queries through unvalidated user input. Attackers can inject malicious SQL code in the 'search' parameter to potentially extract, modify, or access sensitive database information.		
CVE-2020-37051	Online-Exam-System 2015 contains a time-based blind SQL injection vulnerability in the feedback form that allows attackers to extract database password hashes.	Online-Exam-System 2015 contains a time-based blind SQL injection vulnerability in the feedback form that allows attackers to extract database password hashes. Attackers can exploit the 'feed.php' endpoint by crafting malicious payload requests that use time delays to systematically enumerate user password characters.	Patched by core rule	Y
CVE-2020-37052	AirControl 1.4.2 contains a pre-authentication remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary system commands through malicious Java expression injection.	AirControl 1.4.2 contains a pre-authentication remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary system commands through malicious Java expression injection. Attackers can exploit the /.seam endpoint by crafting a specially constructed URL with embedded Java expressions to run commands with the application's system privileges.	Patched by core rule	Y
CVE-2020-37053	Navigate CMS 2.8.7 contains an authenticated SQL injection vulnerability that allows attackers to leak database information by manipulating the 'sidx' parameter in comments.	Navigate CMS 2.8.7 contains an authenticated SQL injection vulnerability that allows attackers to leak database information by manipulating the 'sidx' parameter in comments. Attackers can exploit the vulnerability to extract user activation keys by using time-based blind SQL injection techniques, potentially enabling password reset for administrative accounts.	Patched by core rule	Y
CVE-2020-37057	Online-Exam-System 2015 contains a SQL injection vulnerability in the feedback module that allows attackers to manipulate database queries through the 'fid' parameter.	Online-Exam-System 2015 contains a SQL injection vulnerability in the feedback module that allows attackers to manipulate database queries through the 'fid' parameter. Attackers can inject malicious SQL code into the 'fid' parameter to potentially extract, modify, or delete database	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		information.		
CVE-2020-37076	Victor CMS version 1.0 contains a SQL injection vulnerability in the 'post' parameter on post.php that allows remote attackers to manipulate database queries.	Victor CMS version 1.0 contains a SQL injection vulnerability in the 'post' parameter on post.php that allows remote attackers to manipulate database queries. Attackers can exploit this vulnerability by sending crafted UNION SELECT payloads to extract database information through boolean-based, error-based, and time-based injection techniques.	Patched by core rule	Y
CVE-2020-37081	Fishing Reservation System 7.5 contains multiple remote SQL injection vulnerabilities in admin.php, cart.php, and calendar.php that allow attackers to inject malicious SQL commands.	Fishing Reservation System 7.5 contains multiple remote SQL injection vulnerabilities in admin.php, cart.php, and calendar.php that allow attackers to inject malicious SQL commands. Attackers can exploit vulnerable parameters like uid, pid, type, m, y, and code to compromise the database management system and web application without user interaction.	Patched by core rule	Y
CVE-2020-37083	PHP AddressBook 9.0.0.1 contains a time-based blind SQL injection vulnerability that allows remote attackers to manipulate database queries through the 'id' parameter.	PHP AddressBook 9.0.0.1 contains a time-based blind SQL injection vulnerability that allows remote attackers to manipulate database queries through the 'id' parameter. Attackers can inject crafted SQL statements with time delays to extract information by observing response times in the photo.php endpoint.	Patched by core rule	Y
CVE-2020-37089	School ERP Pro 1.0 contains a SQL injection vulnerability in the 'es_messagesid' parameter that allows attackers to manipulate database queries through GET requests.	School ERP Pro 1.0 contains a SQL injection vulnerability in the 'es_messagesid' parameter that allows attackers to manipulate database queries through GET requests. Attackers can exploit the vulnerable parameter by injecting crafted SQL statements to potentially extract, modify, or delete database information.	Patched by core rule	Y
CVE-2020-37105	PMB 5.6 contains a SQL injection vulnerability in the administration download script that allows authenticated attackers to execute arbitrary SQL commands through the 'logid' parameter.	PMB 5.6 contains a SQL injection vulnerability in the administration download script that allows authenticated attackers to execute arbitrary SQL commands through the 'logid' parameter. Attackers can leverage this vulnerability by sending	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		crafted requests to the /admin/sauvegarde/download.php endpoint with manipulated logid values to interact with the database.		
CVE-2020-37108	PhpIX 2012 Professional contains a SQL injection vulnerability in the 'id' parameter of product_detail.php that allows remote attackers to manipulate database queries.	PhpIX 2012 Professional contains a SQL injection vulnerability in the 'id' parameter of product_detail.php that allows remote attackers to manipulate database queries. Attackers can inject malicious SQL code through the 'id' parameter to potentially extract or modify database information.	Patched by core rule	Y
CVE-2020-37110	60CycleCMS 2.5.2 contains an SQL injection vulnerability in news.php and common/lib.php that allows attackers to manipulate database queries through unvalidated user input.	60CycleCMS 2.5.2 contains an SQL injection vulnerability in news.php and common/lib.php that allows attackers to manipulate database queries through unvalidated user input. Attackers can exploit vulnerable query parameters like 'title' to inject malicious SQL code and potentially extract or modify database contents. This issue does not involve cross-site scripting.	Patched by core rule	Y
CVE-2020-37112	GUnet OpenEclass 1.7.3 contains multiple SQL injection vulnerabilities that allow authenticated attackers to manipulate database queries through unvalidated parameters.	GUnet OpenEclass 1.7.3 contains multiple SQL injection vulnerabilities that allow authenticated attackers to manipulate database queries through unvalidated parameters. Attackers can exploit the 'month' parameter in the agenda module and other endpoints to extract sensitive database information using error-based or time-based injection techniques.	Patched by core rule	Y
CVE-2020-37141	AMSS++ version 4.31 contains a SQL injection vulnerability in the mail module's maildetail.php script through the 'id' parameter.	AMSS++ version 4.31 contains a SQL injection vulnerability in the mail module's maildetail.php script through the 'id' parameter. Attackers can manipulate the 'id' parameter in /modules/mail/main/maildetail.php to inject malicious SQL queries and potentially access or modify database contents.	Patched by core rule	Y
CVE-2020-37147	ATutor 2.2.4 contains a SQL injection vulnerability in the admin user deletion page that allows authenticated attackers to manipulate	ATutor 2.2.4 contains a SQL injection vulnerability in the admin user deletion page that allows authenticated attackers to manipulate database queries through	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	database queries through the 'id' parameter.	the 'id' parameter. Attackers can exploit the vulnerability by injecting malicious SQL code into the 'id' parameter of the admin_delete.php script to potentially extract or modify database information.		
CVE-2020-37151	phpMyChat Plus 1.98 contains a SQL injection vulnerability in the deluser.php page through the pmc_username parameter that allows attackers to manipulate database queries.	phpMyChat Plus 1.98 contains a SQL injection vulnerability in the deluser.php page through the pmc_username parameter that allows attackers to manipulate database queries. Attackers can exploit boolean-based, error-based, and time-based blind SQL injection techniques to extract sensitive database information by crafting malicious payloads in the username field.	Patched by core rule	Y
CVE-2020-37154	eLection 2.0 contains an authenticated SQL injection vulnerability in the candidate management endpoint that allows attackers to manipulate database queries through the 'id' parameter.	eLection 2.0 contains an authenticated SQL injection vulnerability in the candidate management endpoint that allows attackers to manipulate database queries through the 'id' parameter. Attackers can leverage SQLMap to exploit the vulnerability, potentially gaining remote code execution by uploading backdoor files to the web application directory.	Patched by core rule	Y
CVE-2020-37163	QuickDate 1.3.2 contains a SQL injection vulnerability that allows remote attackers to manipulate database queries through the '_located' parameter in the find_matches endpoint.	QuickDate 1.3.2 contains a SQL injection vulnerability that allows remote attackers to manipulate database queries through the '_located' parameter in the find_matches endpoint. Attackers can inject UNION-based SQL statements to extract database information including user credentials, database name, and system version.	Patched by core rule	Y
CVE-2021-47902	Testa Online Test Management System 3.4.7 contains a SQL injection vulnerability that allows attackers to manipulate database queries through the 'q' search parameter.	Testa Online Test Management System 3.4.7 contains a SQL injection vulnerability that allows attackers to manipulate database queries through the 'q' search parameter. Attackers can inject malicious SQL code in the search field to extract database information, potentially accessing sensitive user or system data.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-47915	PHP Melody version 3.0 contains a remote SQL injection vulnerability in the video edit module that allows authenticated attackers to inject malicious SQL commands.	PHP Melody version 3.0 contains a remote SQL injection vulnerability in the video edit module that allows authenticated attackers to inject malicious SQL commands. Attackers can exploit the unvalidated 'vid' parameter to execute arbitrary database queries and potentially compromise the web application and database management system.	Patched by core rule	Y
CVE-2021-47918	Simple CMS 2.1 contains a remote SQL injection vulnerability that allows privileged attackers to inject unfiltered SQL commands in the users module.	Simple CMS 2.1 contains a remote SQL injection vulnerability that allows privileged attackers to inject unfiltered SQL commands in the users module. Attackers can exploit unvalidated input parameters in the admin.php file to compromise the database management system and web application.	Patched by core rule	Y
CVE-2024-55270	phpgurukul Student Management System 1.0 is vulnerable to SQL Injection in studentms/admin/search.php via the searchdata parameter.	phpgurukul Student Management System 1.0 is vulnerable to SQL Injection in studentms/admin/search.php via the searchdata parameter.	Patched by core rule	Y
CVE-2025-10878	A SQL injection vulnerability exists in the login functionality of Fikir Odalari AdminPando 1.0.1 before 2026-01-26.	A SQL injection vulnerability exists in the login functionality of Fikir Odalari AdminPando 1.0.1 before 2026-01-26. The username and password parameters are vulnerable to SQL injection, allowing unauthenticated attackers to bypass authentication completely. Successful exploitation grants full administrative access to the application, including the ability to manipulate the public-facing website content (HTML/DOM manipulation).	Patched by core rule	Y
CVE-2025-14973	The Recipe Card Blocks Lite WordPress plugin before 3.4.13 does not sanitize and escape a parameter before using it in a SQL statement, allowing contributors and above to perform SQL injection attacks.	The Recipe Card Blocks Lite WordPress plugin before 3.4.13 does not sanitize and escape a parameter before using it in a SQL statement, allowing contributors and above to perform SQL injection attacks.	Patched by core rule	Y
CVE-2025-15585	Fileflows versions before 25.05.2 are affected by an authenticated SQL injection vulnerability in	Fileflows versions before 25.05.2 are affected by an authenticated SQL injection vulnerability in the library-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	the library-file search function.	file search function. Successful exploitation requires the system to use MySQL as the underlying database and could result in privilege escalation or data exfiltration.		
CVE-2025-57529	YouDataSum CPAS Audit Management System <=v4.9 is vulnerable to SQL Injection in /cpasList/findArchiveReportByDah due to insufficient input validation.	YouDataSum CPAS Audit Management System <=v4.9 is vulnerable to SQL Injection in /cpasList/findArchiveReportByDah due to insufficient input validation. This allows remote unauthenticated attackers to execute arbitrary SQL commands via crafted input to the parameter. Successful exploitation could lead to unauthorized data access	Patched by core rule	Y
CVE-2025-63624	SQL Injection vulnerability in Shandong Kede Electronics Co., Ltd IoT smart water meter monitoring platform v.1.0 allows a remote attacker to execute arbitrary code via the imei_list.aspx file.	SQL Injection vulnerability in Shandong Kede Electronics Co., Ltd IoT smart water meter monitoring platform v.1.0 allows a remote attacker to execute arbitrary code via the imei_list.aspx file.	Patched by core rule	Y
CVE-2025-69213	OpenSTAManager is an open source management software for technical assistance and invoicing.	OpenSTAManager is an open source management software for technical assistance and invoicing. In version 2.9.8 and prior, a SQL Injection vulnerability exists in the ajax_complete.php endpoint when handling the get_sedi operation. An authenticated attacker can inject malicious SQL code through the idanagrafica parameter, leading to unauthorized database access. At time of publication, no known patch exists.	Patched by core rule	Y
CVE-2025-69214	OpenSTAManager is an open source management software for technical assistance and invoicing.	OpenSTAManager is an open source management software for technical assistance and invoicing. In 2.9.8 and earlier, an SQL Injection vulnerability exists in the ajax_select.php endpoint when handling the componenti operation. An authenticated attacker can inject malicious SQL code through the options[matricola] parameter.	Patched by core rule	Y
CVE-2025-69215	OpenSTAManager is an open source management software for technical assistance and invoicing.	OpenSTAManager is an open source management software for technical assistance and invoicing. In version 2.9.8 and prior,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		there is a SQL Injection vulnerability in the Stampe Module. At time of publication, no known patch exists.		
CVE-2025-69216	OpenSTAManager is an open source management software for technical assistance and invoicing.	OpenSTAManager is an open source management software for technical assistance and invoicing. In 2.9.8 and earlier, an authenticated SQL injection vulnerability in OpenSTAManager's Scadenzario (Payment Schedule) print template allows any authenticated user to extract sensitive data from the database, including admin credentials, customer information, and financial records. The vulnerability exists in templates/scadenzario/init.php, where the id_anagrafica parameter is directly concatenated into an SQL query without proper sanitization. The vulnerability enables complete database read access through error-based SQL injection techniques.	Patched by core rule	Y
CVE-2025-69562	code-projects Mobile Shop Management System 1.0 is vulnerable to SQL Injection in /insertmessage.php via the userid parameter.	code-projects Mobile Shop Management System 1.0 is vulnerable to SQL Injection in /insertmessage.php via the userid parameter.	Patched by core rule	Y
CVE-2025-69563	code-projects Mobile Shop Management System 1.0 is vulnerable to SQL Injection in /ExLogin.php via the Password parameter.	code-projects Mobile Shop Management System 1.0 is vulnerable to SQL Injection in /ExLogin.php via the Password parameter.	Patched by core rule	Y
CVE-2025-69564	code-projects Mobile Shop Management System 1.0 is vulnerable to SQL Injection in /ExAddNewUser.php via the Name, Address, email, UserName, Password, confirm_password, Role, Branch, and Activate parameters.	code-projects Mobile Shop Management System 1.0 is vulnerable to SQL Injection in /ExAddNewUser.php via the Name, Address, email, UserName, Password, confirm_password, Role, Branch, and Activate parameters.	Patched by core rule	Y
CVE-2025-69662	SQL injection vulnerability in geopandas before v.1.1.2 allows an attacker to obtain sensitive information via the to_postgis()` function being used to write GeoDataFrames to a PostgreSQL database.	SQL injection vulnerability in geopandas before v.1.1.2 allows an attacker to obtain sensitive information via the to_postgis()` function being used to write GeoDataFrames to a PostgreSQL database.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-70149	CodeAstro Membership Management System 1.0 is vulnerable to SQL Injection in print_membership_card.php via the ID parameter.	CodeAstro Membership Management System 1.0 is vulnerable to SQL Injection in print_membership_card.php via the ID parameter.	Patched by core rule	Y
CVE-2025-70152	code-projects Community Project Scholars Tracking System 1.0 is vulnerable to SQL Injection in the admin user management endpoints /admin/save_user.php and /admin/update_user.php.	code-projects Community Project Scholars Tracking System 1.0 is vulnerable to SQL Injection in the admin user management endpoints /admin/save_user.php and /admin/update_user.php. These endpoints lack authentication checks and directly concatenate user-supplied POST parameters (firstname, lastname, username, password, user_id) into SQL queries without validation or parameterization.	Patched by core rule	Y
CVE-2025-70397	jizhicms 2.5.6 is vulnerable to SQL Injection in Article/deleteAll and Extmolds/deleteAll via the data parameter.	jizhicms 2.5.6 is vulnerable to SQL Injection in Article/deleteAll and Extmolds/deleteAll via the data parameter.	Patched by core rule	Y
CVE-2025-70981	CordysCRM 1.4.1 is vulnerable to SQL Injection in the employee list query interface (/user/list) via the departmentIds parameter.	CordysCRM 1.4.1 is vulnerable to SQL Injection in the employee list query interface (/user/list) via the departmentIds parameter.	Patched by core rule	Y
CVE-2026-1422	A vulnerability was found in code-projects Online Examination System 1.0.	A vulnerability was found in code-projects Online Examination System 1.0. Affected by this vulnerability is an unknown functionality of the file /index.php of the component Login Page. Performing a manipulation of the argument User results in sql injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2026-1443	A flaw has been found in code-projects Online Music Site 1.0.	A flaw has been found in code-projects Online Music Site 1.0. Affected by this issue is some unknown functionality of the file /Administrator/PHP/AdminDeleteUser.php. This manipulation of the argument ID causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-1533	A security flaw has been discovered in code-	A security flaw has been discovered in code-projects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	projects Online Music Site 1.0.	Online Music Site 1.0. The impacted element is an unknown function of the file /Administrator/PHP/AdminAddCategory.php. The manipulation results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks.		
CVE-2026-1534	A weakness has been identified in code-projects Online Music Site 1.0.	A weakness has been identified in code-projects Online Music Site 1.0. This affects an unknown function of the file /Administrator/PHP/AdminEditUser.php. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-1535	A security vulnerability has been detected in code-projects Online Music Site 1.0.	A security vulnerability has been detected in code-projects Online Music Site 1.0. This impacts an unknown function of the file /Administrator/PHP/AdminReply.php. Such manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-1545	A weakness has been identified in itsourcecode School Management System 1.0.	A weakness has been identified in itsourcecode School Management System 1.0. The affected element is an unknown function of the file /course/index.php. Executing a manipulation of the argument ID can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-1546	A security vulnerability has been detected in jishenghua jshERP up to 3.6.	A security vulnerability has been detected in jishenghua jshERP up to 3.6. The impacted element is the function getBillItemByParam of the file /jshERP-boot/depotItem/importItemExcel of the component com.jsh.erp.datasource.mappers.DepotItemMapperEx. The manipulation of the argument barCodes leads to sql injection. It is possible to initiate the attack remotely.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.		
CVE-2026-1551	A weakness has been identified in itsourcecode School Management System 1.0.	A weakness has been identified in itsourcecode School Management System 1.0. This affects an unknown part of the file /ramonsys/course/controller.php. Executing a manipulation of the argument ID can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-1552	A security vulnerability has been detected in SEMCMS 5.0.	A security vulnerability has been detected in SEMCMS 5.0. This vulnerability affects unknown code of the file /SEMCMS_Info.php. The manipulation of the argument searchml leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-1589	A vulnerability was determined in itsourcecode School Management System 1.0.	A vulnerability was determined in itsourcecode School Management System 1.0. This affects an unknown function of the file /ramonsys/inquiry/index.php. This manipulation of the argument txtsearch causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-1590	A vulnerability was identified in itsourcecode School Management System 1.0.	A vulnerability was identified in itsourcecode School Management System 1.0. This impacts an unknown function of the file /ramonsys/faculty/index.php. Such manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2026-1593	A weakness has been identified in itsourcecode Society Management System 1.0.	A weakness has been identified in itsourcecode Society Management System 1.0. Affected by this vulnerability is an unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		functionality of the file /admin/edit_expenses_query.php. Executing a manipulation of the argument detail can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.		
CVE-2026-1594	A security vulnerability has been detected in itsourcecode Society Management System 1.0.	A security vulnerability has been detected in itsourcecode Society Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/add_expenses.php. The manipulation of the argument detail leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-1595	A vulnerability was detected in itsourcecode Society Management System 1.0.	A vulnerability was detected in itsourcecode Society Management System 1.0. This affects an unknown part of the file /admin/edit_student_query.php. The manipulation of the argument student_id results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-1688	A security vulnerability has been detected in itsourcecode Directory Management System 1.0.	A security vulnerability has been detected in itsourcecode Directory Management System 1.0. The affected element is an unknown function of the file /admin/index.php. The manipulation of the argument Username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-1701	A security vulnerability has been detected in itsourcecode School Management System 1.0.	A security vulnerability has been detected in itsourcecode School Management System 1.0. This issue affects some unknown processing of the file /enrollment/index.php. Such manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. Due to contradicting product	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		definitions in the original disclosure, this CVE was initially incorrectly assigned to the Student Management System.		
CVE-2026-1746	A vulnerability was identified in JeecgBoot 3.9.0.	A vulnerability was identified in JeecgBoot 3.9.0. This vulnerability affects unknown code of the file /JeecgBoot/sys/api/loadDictItemByKeyword of the component Online Report API. Such manipulation of the argument keyword leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-2011	A vulnerability was found in itsourcecode Student Management System 1.0.	A vulnerability was found in itsourcecode Student Management System 1.0. The affected element is an unknown function of the file /ramonsys/enrollment/controller.php. The manipulation of the argument ID results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2026-2012	A vulnerability was determined in itsourcecode Student Management System 1.0.	A vulnerability was determined in itsourcecode Student Management System 1.0. The impacted element is an unknown function of the file /ramonsys/facultyloading/index.php. This manipulation of the argument ID causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-2013	A vulnerability was identified in itsourcecode Student Management System 1.0.	A vulnerability was identified in itsourcecode Student Management System 1.0. This affects an unknown function of the file /ramonsys/soa/index.php. Such manipulation of the argument ID leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2026-2014	A security flaw has been discovered in itsourcecode Student Management System 1.0.	A security flaw has been discovered in itsourcecode Student Management System 1.0. This impacts an unknown function of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/ramonsys/billing/index.php. Performing a manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks.		
CVE-2026-2018	A flaw has been found in itsourcecode School Management System 1.0.	A flaw has been found in itsourcecode School Management System 1.0. This affects an unknown part of the file /ramonsys/settings/controller.php. This manipulation of the argument ID causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-2057	A vulnerability was detected in SourceCodester Medical Center Portal Management System 1.0.	A vulnerability was detected in SourceCodester Medical Center Portal Management System 1.0. This affects an unknown function of the file /login.php. The manipulation of the argument User results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-2058	A flaw has been found in mathurvishal CloudClassroom-PHP-Project up to 5dadec098bfbbf3300d60c3494db3fb95b66e7be.	A flaw has been found in mathurvishal CloudClassroom-PHP-Project up to 5dadec098bfbbf3300d60c3494db3fb95b66e7be. This impacts an unknown function of the file /postquerypublic.php of the component Post Query Details Page. This manipulation of the argument gnamex causes sql injection. The attack is possible to be carried out remotely. The exploit has been published and may be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-2059	A vulnerability has been found in SourceCodester Medical Center Portal Management System 1.0.	A vulnerability has been found in SourceCodester Medical Center Portal Management System 1.0. Affected is an unknown function of the file /emp_edit1.php. Such	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument ID leads to sql injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.		
CVE-2026-2060	A vulnerability was found in code-projects Simple Blood Donor Management System 1.0.	A vulnerability was found in code-projects Simple Blood Donor Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /simpleblooddonor/editcampaignform.php. Performing a manipulation of the argument ID results in sql injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2026-2073	A vulnerability was determined in itsourcecode School Management System 1.0.	A vulnerability was determined in itsourcecode School Management System 1.0. This affects an unknown function of the file /ramonsys/user/index.php. Executing a manipulation of the argument ID can lead to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-2083	A security flaw has been discovered in code-projects Social Networking Site 1.0.	A security flaw has been discovered in code-projects Social Networking Site 1.0. This affects an unknown function of the file /delete_post.php. Performing a manipulation of the argument ID results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y
CVE-2026-2088	A vulnerability has been found in PHPGurukul Beauty Parlour Management System 1.1.	A vulnerability has been found in PHPGurukul Beauty Parlour Management System 1.1. This affects an unknown part of the file /admin/accepted-appointment.php. Such manipulation of the argument delid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-2114	A vulnerability was detected in itsourcecode Society Management System 1.0.	A vulnerability was detected in itsourcecode Society Management System 1.0. This vulnerability affects unknown code of the file /admin/edit_admin.php. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument admin_id results in sql injection. The attack may be performed from remote. The exploit is now public and may be used.		
CVE-2026-2115	A flaw has been found in itsourcecode Society Management System 1.0.	A flaw has been found in itsourcecode Society Management System 1.0. This issue affects some unknown processing of the file /admin/delete_expenses.php. This manipulation of the argument expenses_id causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-2116	A vulnerability has been found in itsourcecode Society Management System 1.0.	A vulnerability has been found in itsourcecode Society Management System 1.0. Impacted is an unknown function of the file /admin/edit_expenses.php. Such manipulation of the argument expenses_id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-2117	A vulnerability was found in itsourcecode Society Management System 1.0.	A vulnerability was found in itsourcecode Society Management System 1.0. The affected element is an unknown function of the file /admin/edit_activity.php. Performing a manipulation of the argument activity_id results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2026-2132	A security flaw has been discovered in code-projects Online Music Site 1.0.	A security flaw has been discovered in code-projects Online Music Site 1.0. This issue affects some unknown processing of the file /Administrator/PHP/AdminUpdateCategory.php. The manipulation of the argument txtcat results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y
CVE-2026-2134	A security vulnerability has been detected in PHPGurukul Hospital Management System 4.0.	A security vulnerability has been detected in PHPGurukul Hospital Management System 4.0. The affected element is an	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unknown function of the file /hms/admin/manage-doctors.php. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.		
CVE-2026-2136	A flaw has been found in projectworlds Online Food Ordering System 1.0.	A flaw has been found in projectworlds Online Food Ordering System 1.0. This affects an unknown function of the file /view-ticket.php. Executing a manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-2158	A vulnerability was detected in code-projects Student Web Portal 1.0.	A vulnerability was detected in code-projects Student Web Portal 1.0. This impacts an unknown function of the file /check_user.php. Performing a manipulation of the argument Username results in sql injection. It is possible to initiate the attack remotely.	Patched by core rule	Y
CVE-2026-2161	A vulnerability was found in itsourcecode Directory Management System 1.0.	A vulnerability was found in itsourcecode Directory Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/forget-password.php. The manipulation of the argument email results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2026-2162	A vulnerability was determined in itsourcecode News Portal Project 1.0.	A vulnerability was determined in itsourcecode News Portal Project 1.0. This affects an unknown part of the file /admin/aboutus.php. This manipulation of the argument pagetitle causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-2166	A security vulnerability has been detected in code-projects Online Reviewer System 1.0.	A security vulnerability has been detected in code-projects Online Reviewer System 1.0. The affected element is an unknown function of the file /login/index.php of the component Login. The manipulation of the argument	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		username/password leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.		
CVE-2026-2179	A vulnerability was determined in PHPGurukul Hospital Management System 4.0.	A vulnerability was determined in PHPGurukul Hospital Management System 4.0. This impacts an unknown function of the file /admin/manage-users.php. This manipulation of the argument ID causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-2189	A vulnerability was identified in itsourcecode School Management System 1.0.	A vulnerability was identified in itsourcecode School Management System 1.0. This affects an unknown function of the file /ramonsys/report/index.php . The manipulation of the argument ay leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2026-2190	A security flaw has been discovered in itsourcecode School Management System 1.0.	A security flaw has been discovered in itsourcecode School Management System 1.0. This impacts an unknown function of the file /ramonsys/user/controller.php. The manipulation of the argument ID results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y
CVE-2026-2195	A vulnerability has been found in code-projects Online Reviewer System 1.0.	A vulnerability has been found in code-projects Online Reviewer System 1.0. This vulnerability affects unknown code of the file /system/system/admins/assessments/pretest/questions-view.php. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-2196	A vulnerability was found in code-projects Online Reviewer System 1.0.	A vulnerability was found in code-projects Online Reviewer System 1.0. This issue affects some unknown processing of the file /system/system/admins/assessments/pretest/exam-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		update.php. The manipulation of the argument test_id results in sql injection. The attack may be performed from remote. The exploit has been made public and could be used.		
CVE-2026-2197	A vulnerability was determined in code-projects Online Reviewer System 1.0.	A vulnerability was determined in code-projects Online Reviewer System 1.0. Impacted is an unknown function of the file /system/system/admins/assessments/pretest/exam-delete.php. This manipulation of the argument test_id causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-2198	A vulnerability was identified in code-projects Online Reviewer System 1.0.	A vulnerability was identified in code-projects Online Reviewer System 1.0. The affected element is an unknown function of the file /system/system/admins/assessments/pretest/loaddata.php. Such manipulation of the argument difficulty_id leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2026-2199	A security flaw has been discovered in code-projects Online Reviewer System 1.0.	A security flaw has been discovered in code-projects Online Reviewer System 1.0. The impacted element is an unknown function of the file /reviewer/system/system/admins/manage/users/user-delete.php. Performing a manipulation of the argument ID results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y
CVE-2026-2211	A vulnerability was determined in code-projects Online Music Site 1.0.	A vulnerability was determined in code-projects Online Music Site 1.0. Affected is an unknown function of the file /Administrator/PHP/AdminDeleteCategory.php. Executing a manipulation of the argument ID can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-2212	A vulnerability was identified in code-projects Online Music Site 1.0.	A vulnerability was identified in code-projects Online Music Site 1.0. Affected by this vulnerability is an unknown functionality of the file /Administrator/PHP/AdminEditCategory.php. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2026-2217	A vulnerability was found in itsourcecode Event Management System 1.0.	A vulnerability was found in itsourcecode Event Management System 1.0. The impacted element is an unknown function of the file /admin/manage_user.php. The manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2026-2220	A vulnerability was identified in code-projects Online Reviewer System 1.0.	A vulnerability was identified in code-projects Online Reviewer System 1.0. This impacts an unknown function of the file /system/system/admins/assessments/pretest/btn_functions.php. Such manipulation of the argument difficulty_id leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2026-2221	A security flaw has been discovered in code-projects Online Reviewer System 1.0.	A security flaw has been discovered in code-projects Online Reviewer System 1.0. Affected is an unknown function of the file /login/index.php of the component Login. Performing a manipulation of the argument Username results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y
CVE-2026-2223	A security vulnerability has been detected in code-projects Online Reviewer System 1.0.	A security vulnerability has been detected in code-projects Online Reviewer System 1.0. Affected by this issue is some unknown functionality of the file /system/system/students/assessments/pretest/take/index.php. The manipulation of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.		
CVE-2026-22243	EGroupware is a Web based groupware server written in PHP.	EGroupware is a Web based groupware server written in PHP. A SQL Injection vulnerability exists in the core components of EGroupware prior to versions 23.1.20260113 and 26.0.20260113, specifically in the `Nextmatch` filter processing. The flaw allows authenticated attackers to inject arbitrary SQL commands into the `WHERE` clause of database queries. This is achieved by exploiting a PHP type juggling issue where JSON decoding converts numeric strings into integers, bypassing the `is_int()` security check used by the application. Versions 23.1.20260113 and 26.0.20260113 patch the vulnerability.	Patched by core rule	Y
CVE-2026-2225	A flaw has been found in itsourcecode News Portal Project 1.0.	A flaw has been found in itsourcecode News Portal Project 1.0. This vulnerability affects unknown code of the file /admin/index.php of the component Administrator Login. This manipulation of the argument email causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-24043	jsPDF is a library to generate PDFs in JavaScript.	jsPDF is a library to generate PDFs in JavaScript. Prior to 4.1.0, user control of the first argument of the addMetadata function allows users to inject arbitrary XML. If given the possibility to pass unsanitized input to the addMetadata method, a user can inject arbitrary XMP metadata into the generated PDF. If the generated PDF is signed, stored or otherwise processed after, the integrity of the PDF can no longer be guaranteed. The vulnerability has been fixed in jsPDF@4.1.0.	Patched by core rule	Y
CVE-2026-24416	OpenSTAManager is an open source management software for technical assistance	OpenSTAManager is an open source management software for technical assistance and invoicing.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	and invoicing.	OpenSTAManager v2.9.8 and earlier contain a critical Time-Based Blind SQL Injection vulnerability in the article pricing completion handler. The application fails to properly sanitize the idarticolo parameter before using it in SQL queries, allowing attackers to inject arbitrary SQL commands and extract sensitive data through time-based Boolean inference.		
CVE-2026-24417	OpenSTAManager is an open source management software for technical assistance and invoicing.	OpenSTAManager is an open source management software for technical assistance and invoicing. OpenSTAManager v2.9.8 and earlier contain a critical Time-Based Blind SQL Injection vulnerability in the global search functionality. The application fails to properly sanitize the term parameter before using it in SQL LIKE clauses across multiple module-specific search handlers, allowing attackers to inject arbitrary SQL commands and extract sensitive data through time-based Boolean inference.	Patched by core rule	Y
CVE-2026-24418	OpenSTAManager is an open source management software for technical assistance and invoicing.	OpenSTAManager is an open source management software for technical assistance and invoicing. OpenSTAManager v2.9.8 and earlier contain a critical Error-Based SQL Injection vulnerability in the bulk operations handler for the Scadenzario (Payment Schedule) module. The application fails to validate that elements of the id_records array are integers before using them in an SQL IN() clause, allowing attackers to inject arbitrary SQL commands and extract sensitive data through XPATH error messages.	Patched by core rule	Y
CVE-2026-24419	OpenSTAManager is an open source management software for technical assistance and invoicing.	OpenSTAManager is an open source management software for technical assistance and invoicing. OpenSTAManager v2.9.8 and earlier contain a critical Error-Based SQL Injection vulnerability in the Prima Nota (Journal Entry) module's add.php file. The application fails to validate that comma-separated values from the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		id_documenti GET parameter are integers before using them in SQL IN() clauses, allowing attackers to inject arbitrary SQL commands and extract sensitive data through XPATH error messages.		
CVE-2026-24764	OpenClaw (formerly Clawdbot) is a personal AI assistant users run on their own devices.	OpenClaw (formerly Clawdbot) is a personal AI assistant users run on their own devices. In versions 2026.2.2 and below, when the Slack integration is enabled, channel metadata (topic/description) can be incorporated into the model's system prompt. Prompt injection is a documented risk for LLM-driven systems. This issue increases the injection surface by allowing untrusted Slack channel metadata to be treated as higher-trust system input. This issue has been fixed in version 2026.2.3.	Patched by core rule	Y
CVE-2026-24854	ChurchCRM is an open-source church management system.	ChurchCRM is an open-source church management system. A SQL Injection vulnerability exists in endpoint `/PaddleNumEditor.php` in ChurchCRM prior to version 6.7.2. Any authenticated user, including one with zero assigned permissions, can exploit SQL injection through the `PerID` parameter. Version 6.7.2 contains a patch for the issue.	Patched by core rule	Y
CVE-2026-25495	Craft is a platform for creating digital experiences.	Craft is a platform for creating digital experiences. In Craft versions 4.0.0-RC1 through 4.16.17 and 5.0.0-RC1 through 5.8.21, the element-indexes/get-elements endpoint is vulnerable to SQL Injection via the criteria[orderBy] parameter (JSON body). The application fails to sanitize this input before using it in the database query. An attacker with Control Panel access can inject arbitrary SQL into the ORDER BY clause by omitting viewState[order] (or setting both to the same payload). This issue is patched in versions 4.16.18 and 5.8.22.	Patched by core rule	Y
CVE-2026-25510	CI4MS is a CodeIgniter 4-based CMS skeleton that	CI4MS is a CodeIgniter 4-based CMS skeleton that	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	delivers a production-ready, modular architecture with RBAC authorization and theme support.	delivers a production-ready, modular architecture with RBAC authorization and theme support. Prior to version 0.28.5.0, an authenticated user with file editor permissions can achieve Remote Code Execution (RCE) by leveraging the file creation and save endpoints, an attacker can upload and execute arbitrary PHP code on the server. This issue has been patched in version 0.28.5.0.		
CVE-2026-25513	FacturaScripts is open-source enterprise resource planning and accounting software.	FacturaScripts is open-source enterprise resource planning and accounting software. Prior to version 2025.81, FacturaScripts contains a critical SQL injection vulnerability in the REST API that allows authenticated API users to execute arbitrary SQL queries through the sort parameter. The vulnerability exists in the ModelClass::getOrderBy() method where user-supplied sorting parameters are directly concatenated into the SQL ORDER BY clause without validation or sanitization. This affects all API endpoints that support sorting functionality. This issue has been patched in version 2025.81.	Patched by core rule	Y
CVE-2026-25514	FacturaScripts is open-source enterprise resource planning and accounting software.	FacturaScripts is open-source enterprise resource planning and accounting software. Prior to version 2025.81, FacturaScripts contains a critical SQL injection vulnerability in the autocomplete functionality that allows authenticated attackers to extract sensitive data from the database including user credentials, configuration settings, and all stored business data. The vulnerability exists in the CodeModel::all() method where user-supplied parameters are directly concatenated into SQL queries without sanitization or parameterized binding. This issue has been patched in version 2025.81.	Patched by core rule	Y
CVE-2026-25520	SandboxJS is a JavaScript sandboxing library.	SandboxJS is a JavaScript sandboxing library. Prior to 0.8.29, The return values of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		functions aren't wrapped. Object.values/Object.entries can be used to get an Array containing the host's Function constructor, by using Array.prototype.at you can obtain the hosts Function constructor, which can be used to execute arbitrary code outside of the sandbox. This vulnerability is fixed in 0.8.29.		
CVE-2026-25586	SandboxJS is a JavaScript sandboxing library.	SandboxJS is a JavaScript sandboxing library. Prior to 0.8.29, a sandbox escape is possible by shadowing hasOwnProperty on a sandbox object, which disables prototype whitelist enforcement in the property-access path. This permits direct access to __proto__ and other blocked prototype properties, enabling host Object.prototype pollution and persistent cross-sandbox impact. This vulnerability is fixed in 0.8.29.	Patched by core rule	Y
CVE-2026-25947	Worklenz is a project management tool.	Worklenz is a project management tool. Prior to 2.1.7, there are multiple SQL injection vulnerabilities were discovered in backend SQL query construction affecting project and task management controllers, reporting and financial data endpoints, real-time socket.io handlers, and resource allocation and scheduling features. The vulnerability has been patched in version v2.1.7.	Patched by core rule	Y
CVE-2026-26198	Ormar is a async mini ORM for Python.	Ormar is a async mini ORM for Python. In versions 0.9.9 through 0.22.0, when performing aggregate queries, Ormar ORM constructs SQL expressions by passing user-supplied column names directly into \`sqlalchemy.text()\` without any validation or sanitization. The \`min()\` and \`max()\` methods in the \`QuerySet\` class accept arbitrary string input as the column parameter. While \`sum()\` and \`avg()\` are partially protected by an \`is_numeric\` type check that rejects non-existent fields, \`min()\` and \`max()\` skip this validation entirely. As a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		result, an attacker-controlled string is embedded as raw SQL inside the aggregate function call. Any unauthorized user can exploit this vulnerability to read the entire database contents, including tables unrelated to the queried model, by injecting a subquery as the column parameter. Version 0.23.0 contains a patch.		
CVE-2026-26745	OpenSourcePOS 3.4.1 has a second order SQL Injection vulnerability in the handling of the currency_symbol configuration field.	OpenSourcePOS 3.4.1 has a second order SQL Injection vulnerability in the handling of the currency_symbol configuration field. Although the input is initially stored without immediate execution, it is later concatenated into a dynamically constructed SQL query without proper sanitization or parameter binding. This allows an attacker with access to modify the currency_symbol value to inject arbitrary SQL expressions, which are executed when the affected query is subsequently processed.	Patched by core rule	Y
CVE-2026-2682	A vulnerability has been found in Tsinghua Unigroup Electronic Archives System up to 3.2.210802(62532).	A vulnerability has been found in Tsinghua Unigroup Electronic Archives System up to 3.2.210802(62532). Impacted is an unknown function of the file /mine/PublicReport/prinReport.html?token=java. Such manipulation of the argument comid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-2689	A vulnerability was detected in itsourcecode Event Management System 1.0.	A vulnerability was detected in itsourcecode Event Management System 1.0. Affected is an unknown function of the file /admin/manage_booking.php. The manipulation of the argument ID results in sql injection. The attack may be performed from remote. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-2690	A flaw has been found in itsourcecode Event	A flaw has been found in itsourcecode Event	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Management System 1.0.	Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/ajax.php?action=login of the component Admin Login. This manipulation of the argument Username causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.		
CVE-2026-2691	A vulnerability has been found in itsourcecode Event Management System 1.0.	A vulnerability has been found in itsourcecode Event Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/manage_register.php. Such manipulation of the argument ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-26988	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool.	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool. Versions 25.12.0 and below contain an SQL Injection vulnerability in the ajax_table.php endpoint. The application fails to properly sanitize or parameterize user input when processing IPv6 address searches. Specifically, the address parameter is split into an address and a prefix, and the prefix portion is directly concatenated into the SQL query string without validation. This allows an attacker to inject arbitrary SQL commands, potentially leading to unauthorized data access or database manipulation. This issue has been fixed in version 26.2.0.	Patched by core rule	Y
CVE-2026-26990	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool.	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool. Versions 25.12.0 and below have a Time-Based Blind SQL Injection vulnerability in address-search.inc.php via the address parameter. When a crafted subnet prefix is supplied, the prefix value is concatenated directly into an SQL query	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		without proper parameter binding, allowing an attacker to manipulate query logic and infer database information through time-based conditional responses. This vulnerability requires authentication and is exploitable by any authenticated user. This issue has been fixedd in version 26.2.0.		
CVE-2026-2706	A flaw has been found in code-projects Patient Record Management System 1.0.	A flaw has been found in code-projects Patient Record Management System 1.0. This affects an unknown function of the file /fecalysis_not.php. This manipulation of the argument comp_id causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-27179	MajorDoMo (aka Major Domestic Module) contains an unauthenticated SQL injection vulnerability in the commands module.	MajorDoMo (aka Major Domestic Module) contains an unauthenticated SQL injection vulnerability in the commands module. The commands_search.inc.php file directly interpolates the $_GET['parent'] parameter into multiple SQL queries without sanitization or parameterized queries. The commands module is loadable without authentication via the /objects/?module=commands endpoint, which includes arbitrary modules by name and calls their usual() method. Time-based blind SQL injection is exploitable using UNION SELECT SLEEP() syntax. Because MajorDoMo stores admin passwords as unsalted MD5 hashes in the users table, successful exploitation enables extraction of credentials and subsequent admin panel access.	Patched by core rule	Y
CVE-2026-27461	Pimcore is an Open Source Data & Experience Management Platform.	Pimcore is an Open Source Data & Experience Management Platform. In versions up to and including 11.5.14.1 and 12.3.2, the filter query parameter in the dependency listing endpoints is JSON-decoded and the value field is concatenated directly into RLIKE clauses without sanitization or parameterized queries.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Exploiting this issue requires admin authentication. An attacker with admin panel access can extract the full database including password hashes of other admin users. Version 12.3.3 contains a patch.		
CVE-2026-27470	ZoneMinder is a free, open source closed-circuit television software application.	ZoneMinder is a free, open source closed-circuit television software application. In versions 1.36.37 and below and 1.37.61 through 1.38.0, there is a second-order SQL Injection vulnerability in the web/ajax/status.php file within the getNearEvents() function. Event field values (specifically Name and Cause) are stored safely via parameterized queries but are later retrieved and concatenated directly into SQL WHERE clauses without escaping. An authenticated user with Events edit and view permissions can exploit this to execute arbitrary SQL queries.	Patched by core rule	Y
CVE-2026-27743	The SPIP referer_spam plugin versions prior to 1.3.0 contain an unauthenticated SQL injection vulnerability in the referer_spam_ajouter and referer_spam_supprimer action handlers.	The SPIP referer_spam plugin versions prior to 1.3.0 contain an unauthenticated SQL injection vulnerability in the referer_spam_ajouter and referer_spam_supprimer action handlers. The handlers read the url parameter from a GET request and interpolate it directly into SQL LIKE clauses without input validation or parameterization. The endpoints do not enforce authorization checks and do not use SPIP action protections such as securiser_action(), allowing remote attackers to execute arbitrary SQL queries.	Patched by core rule	Y
CVE-2026-2820	A security flaw has been discovered in Fujian Smart Integrated Management Platform System up to 7.5.	A security flaw has been discovered in Fujian Smart Integrated Management Platform System up to 7.5. This issue affects some unknown processing of the file /Module/CRXT/Controller/XAccessPermissionPlus.ashx. The manipulation of the argument DeviceIDS results in sql injection. The attack may be launched remotely. The exploit has been released to the public and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		may be used for attacks.		
CVE-2026-2821	A weakness has been identified in Fujian Smart Integrated Management Platform System up to 7.5.	A weakness has been identified in Fujian Smart Integrated Management Platform System up to 7.5. Impacted is an unknown function of the file /Module/CRXT/Controller/XCamera.ashx. This manipulation of the argument ChannelName causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-2848	A flaw has been found in SourceCodester Simple Responsive Tourism Website 1.0.	A flaw has been found in SourceCodester Simple Responsive Tourism Website 1.0. Affected by this vulnerability is an unknown functionality of the file /classes/Master.php?f=register of the component Registration. This manipulation of the argument Username causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-2865	A vulnerability was found in itsourcecode Agri-Trading Online Shopping System 1.0.	A vulnerability was found in itsourcecode Agri-Trading Online Shopping System 1.0. This impacts an unknown function of the file admin/productcontroller.php of the component HTTP POST Request Handler. Performing a manipulation of the argument Product results in sql injection. The attack may be initiated remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2026-2912	A vulnerability was found in code-projects Online Reviewer System 1.0.	A vulnerability was found in code-projects Online Reviewer System 1.0. Impacted is an unknown function of the file /system/system/students/assessments/results/studentresult-view.php. The manipulation of the argument test_id results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2026-3042	A vulnerability was detected in itsourcecode Event Management	A vulnerability was detected in itsourcecode Event Management System 1.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	System 1.0.	The affected element is an unknown function of the file /admin/index.php. Performing a manipulation of the argument ID results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.		
CVE-2026-3046	A security vulnerability has been detected in itsourcecode E-Logbook with Health Monitoring System for COVID-19 1.0.	A security vulnerability has been detected in itsourcecode E-Logbook with Health Monitoring System for COVID-19 1.0. This vulnerability affects unknown code of the file /check_profile_old.php. The manipulation of the argument profile_id leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-3068	A weakness has been identified in itsourcecode Document Management System 1.0.	A weakness has been identified in itsourcecode Document Management System 1.0. This impacts an unknown function of the file /deluser.php. Executing a manipulation of the argument user2del can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-3069	A security vulnerability has been detected in itsourcecode Document Management System 1.0.	A security vulnerability has been detected in itsourcecode Document Management System 1.0. Affected is an unknown function of the file /edtlbls.php. The manipulation of the argument field1 leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-3133	A vulnerability has been found in itsourcecode Document Management System 1.0.	A vulnerability has been found in itsourcecode Document Management System 1.0. This issue affects some unknown processing of the file /loging.php of the component Login. The manipulation of the argument Username leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-3134	A security flaw has been	A security flaw has been	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	discovered in itsourcecode News Portal Project 1.0.	discovered in itsourcecode News Portal Project 1.0. The affected element is an unknown function of the file /newsportal/admin/edit-category.php. The manipulation of the argument Category results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks.	rule	
CVE-2026-3135	A weakness has been identified in itsourcecode News Portal Project 1.0.	A weakness has been identified in itsourcecode News Portal Project 1.0. The impacted element is an unknown function of the file /admin/add-category.php. This manipulation of the argument Category causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-3148	A vulnerability was determined in SourceCodester Simple and Nice Shopping Cart Script 1.0.	A vulnerability was determined in SourceCodester Simple and Nice Shopping Cart Script 1.0. This impacts an unknown function of the file /signup.php. This manipulation of the argument Username causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-3149	A weakness has been identified in itsourcecode College Management System 1.0.	A weakness has been identified in itsourcecode College Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/asign-single-student-subjects.php. Executing a manipulation of the argument course_code can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-3150	A security vulnerability has been detected in itsourcecode College Management System 1.0.	A security vulnerability has been detected in itsourcecode College Management System 1.0. This affects an unknown part of the file /admin/display-teacher.php. The manipulation of the argument teacher_id leads	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.		
CVE-2026-3151	A vulnerability was detected in itsourcecode College Management System 1.0.	A vulnerability was detected in itsourcecode College Management System 1.0. This vulnerability affects unknown code of the file /login/login.php. The manipulation of the argument email results in sql injection. The attack may be performed from remote. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-3152	A flaw has been found in itsourcecode College Management System 1.0.	A flaw has been found in itsourcecode College Management System 1.0. This issue affects some unknown processing of the file /admin/teacher-salary.php. This manipulation of the argument teacher_id causes sql injection. It is possible to initiate the attack remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-3153	A vulnerability has been found in itsourcecode Document Management System 1.0.	A vulnerability has been found in itsourcecode Document Management System 1.0. Impacted is an unknown function of the file /register.php. Such manipulation of the argument Username leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-3164	A vulnerability was found in itsourcecode News Portal Project 1.0.	A vulnerability was found in itsourcecode News Portal Project 1.0. This issue affects some unknown processing of the file /admin/contactus.php. The manipulation of the argument pagetitle results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	Patched by core rule	Y

Server-Side Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2019-25451	phpMoAdmin 1.1.5 contains a cross-site request forgery vulnerability that allows attackers to perform unauthorized database operations by crafting malicious requests.	phpMoAdmin 1.1.5 contains a cross-site request forgery vulnerability that allows attackers to perform unauthorized database operations by crafting malicious requests. Attackers can trick authenticated users into submitting GET requests to moadmin.php with parameters like action, db, and collection to create, drop, or repair databases and collections without user consent.	Patched by core rule	Y
CVE-2020-36944	ILIAS Learning Management System 4.3 contains a server-side request forgery vulnerability that allows attackers to read local files through portfolio PDF export functionality.	ILIAS Learning Management System 4.3 contains a server-side request forgery vulnerability that allows attackers to read local files through portfolio PDF export functionality. Attackers can inject a script that uses XMLHttpRequest to retrieve local file contents when the portfolio is exported to PDF.	Patched by core rule	Y
CVE-2025-50180	esm.sh is a no-build content delivery network (CDN) for web development.	esm.sh is a no-build content delivery network (CDN) for web development. In version 136, esm.sh is vulnerable to a full-response SSRF, allowing an attacker to retrieve information from internal websites through the vulnerability. Version 137 fixes the vulnerability.	Patched by core rule	Y
CVE-2025-62615	AutoGPT is a platform that allows users to create, deploy, and manage continuous artificial intelligence agents that automate complex workflows.	AutoGPT is a platform that allows users to create, deploy, and manage continuous artificial intelligence agents that automate complex workflows. Prior to autogpt-platform-beta-v0.6.34, in RSSFeedBlock, the third-party library urllib.request.urlopen is used directly to access the URL, but the input URL is not filtered, which will cause SSRF vulnerability. This issue has been patched in autogpt-platform-beta-v0.6.34.	Patched by core rule	Y
CVE-2025-62616	AutoGPT is a platform that allows users to create, deploy, and manage continuous artificial intelligence agents that automate complex workflows.	AutoGPT is a platform that allows users to create, deploy, and manage continuous artificial intelligence agents that automate complex workflows. Prior to autogpt-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		platform-beta-v0.6.34, in SendDiscordFileBlock, the third-party library aiohttp.ClientSession().get is used directly to access the URL, but the input URL is not filtered, which will cause SSRF vulnerability. This issue has been patched in autogpt-platform-beta-v0.6.34.		
CVE-2025-68157	Webpack is a module bundler.	Webpack is a module bundler. From version 5.49.0 to before 5.104.0, when experiments.buildHttp is enabled, webpack‚Äôs HTTP(S) resolver (HttpUriPlugin) enforces allowedUris only for the initial URL, but does not re-validate allowedUris after following HTTP 30x redirects. As a result, an import that appears restricted to a trusted allow-list can be redirected to HTTP(S) URLs outside the allow-list. This is a policy/allow-list bypass that enables build-time SSRF behavior (requests from the build machine to internal-only endpoints, depending on network access) and untrusted content inclusion in build outputs (redirected content is treated as module source and bundled). This issue has been patched in version 5.104.0.	Patched by core rule	Y
CVE-2025-68458	Webpack is a module bundler.	Webpack is a module bundler. From version 5.49.0 to before 5.104.1, when experiments.buildHttp is enabled, webpack‚Äôs HTTP(S) resolver (HttpUriPlugin) can be bypassed to fetch resources from hosts outside allowedUris by using crafted URLs that include userinfo (username:password@host). If allowedUris enforcement relies on a raw string prefix check (e.g., uri.startsWith(allowed)), a URL that looks allow-listed can pass validation while the actual network request is sent to a different authority/host after URL parsing. This is a policy/allow-list bypass that enables build-time SSRF behavior (outbound requests from the build	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		machine to internal-only endpoints, depending on network access) and untrusted content inclusion (the fetched response is treated as module source and bundled). This issue has been patched in version 5.104.1.		
CVE-2026-24736	Squidex is an open source headless content management system and content management hub.	Squidex is an open source headless content management system and content management hub. Versions of the application up to and including 7.21.0 allow users to define "Webhooks" as actions within the Rules engine. The url parameter in the webhook configuration does not appear to validate or restrict destination IP addresses. It accepts local addresses such as 127.0.0.1 or localhost. When a rule is triggered (Either manual trigger by manually calling the trigger endpoint or by a content update or any other triggers), the backend server executes an HTTP request to the user-supplied URL. Crucially, the server logs the full HTTP response in the rule execution log (lastDump field), which is accessible via the API. Which turns a "Blind" SSRF into a "Full Read" SSRF. As of time of publication, no patched versions are available.	Patched by core rule	Y
CVE-2026-24767	NocoDB is software for building databases as spreadsheets.	NocoDB is software for building databases as spreadsheets. Prior to version 0.301.0, a blind Server-Side Request Forgery (SSRF) vulnerability exists in the `uploadViaURL` functionality due to an unprotected `HEAD` request. While the subsequent file retrieval logic correctly enforces SSRF protections, the initial metadata request executes without validation. This allows limited outbound requests to arbitrary URLs before SSRF controls are applied. Version 0.301.0 contains a patch for the issue.	Patched by core rule	Y
CVE-2026-24779	vLLM is an inference and serving engine for large language models (LLMs).	vLLM is an inference and serving engine for large language models (LLMs). Prior to version 0.14.1, a Server-Side Request Forgery	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		(SSRF) vulnerability exists in the `MediaConnector` class within the vLLM project's multimodal feature set. The load_from_url and load_from_url_async methods obtain and process media from URLs provided by users, using different Python parsing libraries when restricting the target host. These two parsing libraries have different interpretations of backslashes, which allows the host name restriction to be bypassed. This allows an attacker to coerce the vLLM server into making arbitrary requests to internal network resources. This vulnerability is particularly critical in containerized environments like `llm-d`, where a compromised vLLM pod could be used to scan the internal network, interact with other pods, and potentially cause denial of service or access sensitive data. For example, an attacker could make the vLLM pod send malicious requests to an internal `llm-d` management endpoint, leading to system instability by falsely reporting metrics like the KV cache state. Version 0.14.1 contains a patch for the issue.		
CVE-2026-2531	A security vulnerability has been detected in MindsDB up to 25.14.1.	A security vulnerability has been detected in MindsDB up to 25.14.1. This vulnerability affects the function clear_filename of the file mindsdb/utilities/security.py of the component File Upload. Such manipulation leads to server-side request forgery. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. The name of the patch is 74d6f0fd4b630218519a700fbee1c05c7fd4b1ed. It is best practice to apply a patch to resolve this issue.	Patched by core rule	Y
CVE-2026-25492	Craft CMS is a content management system.	Craft CMS is a content management system. In Craft versions 3.5.0 through 4.16.17 and 5.0.0-RC1 through 5.8.21, the save_images_Asset GraphQL mutation can be abused to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		fetch internal URLs by providing a domain name that resolves to an internal IP address, bypassing hostname validation. When a non-image file extension such as .txt is allowed, downstream image validation is bypassed, which can allow an authenticated attacker with permission to use save_images_Asset to retrieve sensitive data such as AWS instance metadata credentials from the underlying host. This issue is patched in versions 4.16.18 and 5.8.22.		
CVE-2026-25493	Craft is a platform for creating digital experiences.	Craft is a platform for creating digital experiences. In Craft versions 4.0.0-RC1 through 4.16.17 and 5.0.0-RC1 through 5.8.21, the saveAsset GraphQL mutation validates the initial URL hostname and resolved IP against a blocklist, but Guzzle follows HTTP redirects by default. An attacker can bypass all SSRF protections by hosting a redirect that points to cloud metadata endpoints or any internal IP addresses. This issue is patched in versions 4.16.18 and 5.8.22.	Patched by core rule	Y
CVE-2026-25494	Craft is a platform for creating digital experiences.	Craft is a platform for creating digital experiences. In Craft versions 4.0.0-RC1 through 4.16.17 and 5.0.0-RC1 through 5.8.21, the saveAsset GraphQL mutation uses filter_var(..., FILTER_VALIDATE_IP) to block a specific list of IP addresses. However, alternative IP notations (hexadecimal, mixed) are not recognized by this function, allowing attackers to bypass the blocklist and access cloud metadata services. This issue is patched in versions 4.16.18 and 5.8.22.	Patched by core rule	Y
CVE-2026-25511	Group-Office is an enterprise customer relationship management and groupware tool.	Group-Office is an enterprise customer relationship management and groupware tool. Prior to versions 6.8.150, 25.0.82, and 26.0.5, an authenticated user within the System Administrator group can trigger a full SSRF via the WOPI service discovery URL, including access to internal	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		hosts/ports. The SSRF response body can be exfiltrated via the built‚Äëin debug system, turning it into a visible SSRF. This also allows full server-side file read. This issue has been patched in versions 6.8.150, 25.0.82, and 26.0.5.		
CVE-2026-25545	Astro is a web framework.	Astro is a web framework. Prior to version 9.5.4, Server-Side Rendered pages that return an error with a prerendered custom error page (eg. `404.astro` or `500.astro`) are vulnerable to SSRF. If the `Host:` header is changed to an attacker's server, it will be fetched on `/500.html` and they can redirect this to any internal URL to read the response body through the first request. An attacker who can access the application without `Host:` header validation (eg. through finding the origin IP behind a proxy, or just by default) can fetch their own server to redirect to any internal IP. With this they can fetch cloud metadata IPs and interact with services in the internal network or localhost. For this to be vulnerable, a common feature needs to be used, with direct access to the server (no proxies). Version 9.5.4 fixes the issue.	Patched by core rule	Y
CVE-2026-2556	A security vulnerability has been detected in cskefu up to 8.0.1.	A security vulnerability has been detected in cskefu up to 8.0.1. This issue affects some unknown processing of the file com/cskefu/cc/controller/resource/MediaController.java of the component Endpoint. The manipulation of the argument url leads to server-side request forgery. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-25580	Pydantic AI is a Python agent framework for building applications and workflows with Generative AI.	Pydantic AI is a Python agent framework for building applications and workflows with Generative AI. From 0.0.26 to before 1.56.0, aServer-Side Request Forgery (SSRF) vulnerability	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		exists in Pydantic AI's URL download functionality. When applications accept message history from untrusted sources, attackers can include malicious URLs that cause the server to make HTTP requests to internal network resources, potentially accessing internal services or cloud credentials. This vulnerability only affects applications that accept message history from external users. This vulnerability is fixed in 1.56.0.		
CVE-2026-25991	Tandoor Recipes is an application for managing recipes, planning meals, and building shopping lists.	Tandoor Recipes is an application for managing recipes, planning meals, and building shopping lists. Prior to 2.5.1, there is a Blind Server-Side Request Forgery (SSRF) vulnerability in the Cookmate recipe import feature of Tandoor Recipes. The application fails to validate the destination URL after following HTTP redirects, allowing any authenticated user (including standard users without administrative privileges) to force the server to connect to arbitrary internal or external resources. The vulnerability lies in cookbook/integration/cookmate.py, within the Cookmate integration class. This vulnerability can be leveraged to scan internal network ports, access cloud instance metadata (e.g., AWS/GCP Metadata Service), or disclose the server's real IP address. This vulnerability is fixed in 2.5.1.	Patched by core rule	Y
CVE-2026-26005	ClipBucket v5 is an open source video sharing platform.	ClipBucket v5 is an open source video sharing platform. Prior to 5.5.3 - #45, in Clip Bucket V5, The Remote Play allows creating video entries that reference external video URLs without uploading the video files to the server. However, by specifying an internal network host in the video URL, an SSRF can be triggered, causing GET requests to be sent to internal servers. An attacker can exploit this to scan the internal network. Even a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		regular (non-privileged) user can carry out the attack.		
CVE-2026-26286	SillyTavern is a locally installed user interface that allows users to interact with text generation large language models, image generation engines, and text-to-speech voice models.	SillyTavern is a locally installed user interface that allows users to interact with text generation large language models, image generation engines, and text-to-speech voice models. In versions prior to 1.16.0, a Server-Side Request Forgery (SSRF) vulnerability in the asset download endpoint allows authenticated users to make arbitrary HTTP requests from the server and read the full response body, enabling access to internal services, cloud metadata, and private network resources. The vulnerability has been patched in the version 1.16.0 by introducing a whitelist domain check for asset download requests. It can be reviewed and customized by editing the `whitelistImportDomains` array in the `config.yaml` file.	Patched by core rule	Y
CVE-2026-2654	A weakness has been identified in huggingface smolagents 1.24.0.	A weakness has been identified in huggingface smolagents 1.24.0. Impacted is the function requests.get/requests.post of the component LocalPythonExecutor. Executing a manipulation can lead to server-side request forgery. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-27127	Craft is a content management system (CMS).	Craft is a content management system (CMS). In versions 4.5.0-RC1 through 4.16.18 and 5.0.0-RC1 through 5.8.22, the SSRF validation in Craft CMS,Äôs GraphQL Asset mutation performs DNS resolution separately from the HTTP request. This Time-of-Check-Time-of-Use (TOCTOU) vulnerability enables DNS rebinding attacks, where an attacker,Äôs DNS server returns different IP addresses for validation compared to the actual request. This is a bypass of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the security fix for CVE-2025-68437 that allows access to all blocked IPs, not just IPv6 endpoints. Exploitation requires GraphQL schema permissions for editing assets in the `<VolumeName>` volume and creating assets in the `<VolumeName>` volume. These permissions may be granted to authenticated users with appropriate GraphQL schema access and/or Public Schema (if misconfigured with write permissions). Versions 4.16.19 and 5.8.23 patch the issue.		
CVE-2026-27479	Wallos is an open-source, self-hostable personal subscription tracker.	Wallos is an open-source, self-hostable personal subscription tracker. Versions 4.6.0 and below contain a Server-Side Request Forgery (SSRF) vulnerability in the subscription and payment logo/icon upload functionality. The application validates the IP address of the provided URL before making the request, but allows HTTP redirects (CURLOPT_FOLLOWLOCATION = true), enabling an attacker to bypass the IP validation and access internal resources, including cloud instance metadata endpoints. The getLogoFromUrl() function validates the URL by resolving the hostname and checking if the resulting IP is in a private or reserved range using FILTER_FLAG_NO_PRIV_RANGE | FILTER_FLAG_NO_RES_RANGE. However, the subsequent cURL request is configured with CURLOPT_FOLLOWLOCATION = true and CURLOPT_MAXREDIRS = 3, which means the request will follow HTTP redirects without re-validating the destination IP. This issue has been fixed in version 4.6.1.	Patched by core rule	Y
CVE-2026-27696	changedetection.io is a free open source web page change detection tool.	changedetection.io is a free open source web page change detection tool. In versions prior to 0.54.1, changedetection.io is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		vulnerable to Server-Side Request Forgery (SSRF) because the URL validation function `is_safe_valid_url()` does not validate the resolved IP address of watch URLs against private, loopback, or link-local address ranges. An authenticated user (or any user when no password is configured, which is the default) can add a watch for internal network URLs. The application fetches these URLs server-side, stores the response content, and makes it viewable through the web UI ‚Äî enabling full data exfiltration from internal services. Version 0.54.1 contains a fix for the issue.		
CVE-2026-27730	esm.sh is a no-build content delivery network (CDN) for web development.	esm.sh is a no-build content delivery network (CDN) for web development. Versions up to and including 137 have an SSRF vulnerability (CWE-918) in esm.sh‚Äôs `/http(s)` fetch route. The service tries to block localhost/internal targets, but the validation is based on hostname string checks and can be bypassed using DNS alias domains. This allows an external requester to make the esm.sh server fetch internal localhost services. As of time of publication, no known patched versions exist.	Patched by core rule	Y
CVE-2026-3026	A vulnerability has been found in erzhongxmu JEEWMS 3.7.	A vulnerability has been found in erzhongxmu JEEWMS 3.7. Affected by this issue is some unknown functionality of the file /plug-in/ueditor/jsp/getRemoteImage.jsp of the component UEditor. The manipulation of the argument upfile leads to server-side request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-3052	A vulnerability was found in DataLinkDC dinky up to 1.2.5.	A vulnerability was found in DataLinkDC dinky up to 1.2.5. The impacted element is the function proxyUba of the file dinky-admin/src/main/java/org/dinky/controller/FlinkProxyCo	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		ntroller.java of the component Flink Proxy Controller. Performing a manipulation results in server-side request forgery. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2026-3163	A vulnerability has been found in SourceCodester Website Link Extractor 1.0.	A vulnerability has been found in SourceCodester Website Link Extractor 1.0. This vulnerability affects the function file_get_contents of the component URL Handler. The manipulation leads to server-side request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2020-37088	School ERP Pro 1.0 contains a file disclosure vulnerability that allows unauthenticated attackers to read arbitrary files by manipulating the 'document' parameter in download.php.	School ERP Pro 1.0 contains a file disclosure vulnerability that allows unauthenticated attackers to read arbitrary files by manipulating the 'document' parameter in download.php. Attackers can access sensitive configuration files by supplying directory traversal paths to retrieve system credentials and configuration information.	Patched by core rule	Y
CVE-2026-24897	Erugo is a self-hosted file-sharing platform.	Erugo is a self-hosted file-sharing platform. In versions up to and including 0.2.14, an authenticated low-privileged user can upload arbitrary files to any specified location due to insufficient validation of user‚Äësupplied paths when creating shares. By specifying a writable path within the public web root, an attacker can upload and execute arbitrary code on the server, resulting in remote code execution (RCE). This vulnerability allows a low-privileged user to fully compromise the affected Erugo instance. Version 0.2.15 fixes the issue.	Patched by core rule	Y

Path Traversal Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2020-36939	Cassandra Web 0.5.0 contains a directory traversal vulnerability that allows unauthenticated attackers to read arbitrary files by manipulating path traversal parameters.	Cassandra Web 0.5.0 contains a directory traversal vulnerability that allows unauthenticated attackers to read arbitrary files by manipulating path traversal parameters. Attackers can exploit the disabled Rack::Protection module to read sensitive system files like /etc/passwd and retrieve Apache Cassandra database credentials.	Patched by core rule	Y
CVE-2020-37015	Ruijie Networks Switch eWeb S29_RGOS 11.4 contains a directory traversal vulnerability that allows unauthenticated attackers to access sensitive configuration files by manipulating file path parameters.	Ruijie Networks Switch eWeb S29_RGOS 11.4 contains a directory traversal vulnerability that allows unauthenticated attackers to access sensitive configuration files by manipulating file path parameters. Attackers can exploit the /download.do endpoint with '../' sequences to retrieve system configuration files containing credentials and network settings.	Patched by core rule	Y
CVE-2026-23491	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments.	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. A path traversal vulnerability exists in the `get_file` method of the `Guest` module's `Get` controller in InvoicePlane up to and including through 1.6.3. The vulnerability allows unauthenticated attackers to read arbitrary files on the server by manipulating the input filename. This leads to the disclosure of sensitive information, including configuration files with database credentials. Version 1.6.4 fixes the issue.	Patched by core rule	Y
CVE-2026-24486	Python-Multipart is a streaming multipart parser for Python.	Python-Multipart is a streaming multipart parser for Python. Prior to version 0.0.22, a Path Traversal vulnerability exists when using non-default configuration options `UPLOAD_DIR` and `UPLOAD_KEEP_FILENAME=True`. An attacker can write uploaded files to arbitrary locations on the filesystem	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		by crafting a malicious filename. Users should upgrade to version 0.0.22 to receive a patch or, as a workaround, avoid using `UPLOAD_KEEP_FILENAME=True` in project configurations.		
CVE-2026-25635	calibre is an e-book manager.	calibre is an e-book manager. Prior to 9.2.0, Calibre's CHM reader contains a path traversal vulnerability that allows arbitrary file writes anywhere the user has write permissions. On Windows (haven't tested on other OS's), this can lead to Remote Code Execution by writing a payload to the Startup folder, which executes on next login. This vulnerability is fixed in 9.2.0.	Patched by core rule	Y
CVE-2026-25636	calibre is an e-book manager.	calibre is an e-book manager. In 9.1.0 and earlier, a path traversal vulnerability in Calibre's EPUB conversion allows a malicious EPUB file to corrupt arbitrary existing files writable by the Calibre process. During conversion, Calibre resolves CipherReference URI from META-INF/encryption.xml to an absolute filesystem path and opens it in read-write mode, even when it points outside the conversion extraction directory. This vulnerability is fixed in 9.2.0.	Patched by core rule	Y
CVE-2026-25760	Sliver is a command and control framework that uses a custom Wireguard netstack.	Sliver is a command and control framework that uses a custom Wireguard netstack. Prior to 1.6.11, a path traversal in the website content subsystem lets an authenticated operator read arbitrary files on the Sliver server host. This is an authenticated path traversal / arbitrary file read issue, and it can expose credentials, configs, and keys. This vulnerability is fixed in 1.6.11.	Patched by core rule	Y
CVE-2026-26064	calibre is a cross-platform e-book manager for viewing, converting, editing, and cataloging e-books.	calibre is a cross-platform e-book manager for viewing, converting, editing, and cataloging e-books. Versions 9.2.1 and below contain a Path Traversal vulnerability that allows arbitrary file writes anywhere the user has write permissions. On	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Windows, this leads to Remote Code Execution by writing a payload to the Startup folder, which executes on next login. Function extract_pictures only checks startswith('Pictures'), and does not sanitize '..' sequences. calibre's own ZipFile.extractall() in utils/zipfile.py does sanitize '..' via _get_targetpath(), but extract_pictures() bypasses this by using manual zf.read() + open(). This issue has been fixed in version 9.3.0.		
CVE-2026-26065	calibre is a cross-platform e-book manager for viewing, converting, editing, and cataloging e-books.	calibre is a cross-platform e-book manager for viewing, converting, editing, and cataloging e-books. Versions 9.2.1 and below are vulnerable to Path Traversal through PDB readers (both 132-byte and 202-byte header variants) that allow arbitrary file writes with arbitrary extension and arbitrary content anywhere the user has write permissions. Files are written in 'wb' mode, silently overwriting existing files. This can lead to potential code execution and Denial of Service through file corruption. This issue has been fixed in version 9.3.0.	Patched by core rule	Y

Cross-site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2018-25157	Phraseanet 4.0.3 contains a stored cross-site scripting vulnerability that allows authenticated users to inject malicious scripts through crafted file names during document uploads.	Phraseanet 4.0.3 contains a stored cross-site scripting vulnerability that allows authenticated users to inject malicious scripts through crafted file names during document uploads. Attackers can upload files with embedded SVG scripts that execute in the browser, potentially stealing cookies or redirecting users when the file is viewed.	Patched by core rule	Y
CVE-2019-25263	Zendesk SweetHawk Survey 1.6 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts through support ticket submissions.	Zendesk SweetHawk Survey 1.6 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts through support ticket submissions. Attackers can insert XSS payloads like script tags into ticket text that automatically execute when survey pages are loaded by other users.	Patched by core rule	Y
CVE-2019-25264	Snipe-IT 4.7.5 contains a persistent cross-site scripting vulnerability that allows authorized users to upload malicious SVG files with embedded JavaScript.	Snipe-IT 4.7.5 contains a persistent cross-site scripting vulnerability that allows authorized users to upload malicious SVG files with embedded JavaScript. Attackers can craft SVG files with script tags to execute arbitrary JavaScript when the accessory is viewed by other users.	Patched by core rule	Y
CVE-2019-25265	Online Inventory Manager 3.2 contains a stored cross-site scripting vulnerability in the group description field of the admin edit groups section.	Online Inventory Manager 3.2 contains a stored cross-site scripting vulnerability in the group description field of the admin edit groups section. Attackers can inject malicious JavaScript through the description field that will execute when the groups page is viewed, allowing potential cookie theft and client-side script execution.	Patched by core rule	Y
CVE-2019-25294	html5_snmp 1.11 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts through the 'Remark' parameter in add_router_operation.php.	html5_snmp 1.11 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts through the 'Remark' parameter in add_router_operation.php. Attackers can craft a POST request with a script payload in the Remark field to execute arbitrary JavaScript in victim browsers when the page is loaded.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2019-25301	Millhouse-Project 1.414 contains a persistent cross-site scripting vulnerability in the comment submission functionality that allows attackers to inject malicious scripts.	Millhouse-Project 1.414 contains a persistent cross-site scripting vulnerability in the comment submission functionality that allows attackers to inject malicious scripts. Attackers can post comments with embedded JavaScript through the 'content' parameter in add_comment_sql.php to execute arbitrary scripts in victim browsers.	Patched by core rule	Y
CVE-2019-25311	thesystem version 1.0 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts through multiple server data input fields.	thesystem version 1.0 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts through multiple server data input fields. Attackers can submit crafted script payloads in operating_system, system_owner, system_username, system_password, system_description, and server_name parameters to execute arbitrary JavaScript in victim browsers.	Patched by core rule	Y
CVE-2019-25312	InoERP 0.7.2 contains a persistent cross-site scripting vulnerability in the comment section that allows unauthenticated attackers to inject malicious scripts.	InoERP 0.7.2 contains a persistent cross-site scripting vulnerability in the comment section that allows unauthenticated attackers to inject malicious scripts. Attackers can submit comments with JavaScript payloads that execute in other users' browsers, potentially stealing cookies and session information.	Patched by core rule	Y
CVE-2019-25315	WordPress Server Log Viewer 1.0 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts through unfiltered log file paths.	WordPress Server Log Viewer 1.0 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts through unfiltered log file paths. Attackers can add log files with embedded XSS payloads that will execute when viewed in the WordPress admin interface.	Patched by core rule	Y
CVE-2019-25316	GOautodial 4.0 contains a persistent cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts through the event title parameter.	GOautodial 4.0 contains a persistent cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts through the event title parameter. Attackers can exploit the CreateEvent.php endpoint by sending crafted POST requests with XSS payloads	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to execute arbitrary JavaScript in victim browsers.		
CVE-2019-25317	Kimai 2 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts into timesheet descriptions.	Kimai 2 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts into timesheet descriptions. Attackers can insert SVG-based XSS payloads in the description field to execute arbitrary JavaScript when the page is loaded and viewed by other users.	Patched by core rule	Y
CVE-2019-25323	Heatmiser Netmonitor v3.03 contains an HTML injection vulnerability in the outputSetup.htm page that allows attackers to inject malicious HTML code through the outputtitle parameter.	Heatmiser Netmonitor v3.03 contains an HTML injection vulnerability in the outputSetup.htm page that allows attackers to inject malicious HTML code through the outputtitle parameter. Attackers can craft specially formatted POST requests to the outputtitle parameter to execute arbitrary HTML and potentially manipulate the web interface's displayed content.	Patched by core rule	Y
CVE-2019-25324	RICOH Web Image Monitor 1.09 contains an HTML injection vulnerability in the address configuration CGI script that allows attackers to inject malicious HTML code.	RICOH Web Image Monitor 1.09 contains an HTML injection vulnerability in the address configuration CGI script that allows attackers to inject malicious HTML code. Attackers can exploit the entryNameIn and entryDisplayNameIn parameters to insert arbitrary HTML content, potentially enabling cross-site scripting attacks.	Patched by core rule	Y
CVE-2019-25356	Bematech (formerly Logic Controls, now Elgin) MP-4200 TH printer contains a cross-site scripting vulnerability in the admin configuration page.	Bematech (formerly Logic Controls, now Elgin) MP-4200 TH printer contains a cross-site scripting vulnerability in the admin configuration page. Attackers can inject malicious scripts via crafted POST requests with malformed 'admin' and 'person' parameters, allowing execution of arbitrary JavaScript in the context of an authenticated user's browser session.	Patched by core rule	Y
CVE-2019-25367	ArangoDB Community Edition 3.4.2-1 contains multiple cross-site scripting vulnerabilities in the Aardvark web admin interface (index.html) through search, user	ArangoDB Community Edition 3.4.2-1 contains multiple cross-site scripting vulnerabilities in the Aardvark web admin interface (index.html) through search, user	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	management, and API parameters.	management, and API parameters. Attackers can inject scripts via parameters in /_db/_system/_admin/aardvark/index.html to execute JavaScript in authenticated users' browsers.		
CVE-2019-25368	OPNsense 19.1 contains multiple cross-site scripting vulnerabilities in the diag_backup.php endpoint that allow attackers to inject malicious scripts through multiple parameters including GDrive_GDriveEmail, GDrive_GDriveFolderID, GDrive_GDriveBackupCount, Nextcloud_url, Nextcloud_user, Nextcloud_password, Nextcloud_password_encryption, and Nextcloud_backupdir.	OPNsense 19.1 contains multiple cross-site scripting vulnerabilities in the diag_backup.php endpoint that allow attackers to inject malicious scripts through multiple parameters including GDrive_GDriveEmail, GDrive_GDriveFolderID, GDrive_GDriveBackupCount, Nextcloud_url, Nextcloud_user, Nextcloud_password, Nextcloud_password_encryption, and Nextcloud_backupdir. Attackers can submit POST requests with script payloads in these parameters to execute arbitrary JavaScript in the context of authenticated administrator sessions.	Patched by core rule	Y
CVE-2019-25369	OPNsense 19.1 contains a stored cross-site scripting vulnerability in the system_advanced_sysctl.php endpoint that allows attackers to inject persistent malicious scripts via the tunable parameter.	OPNsense 19.1 contains a stored cross-site scripting vulnerability in the system_advanced_sysctl.php endpoint that allows attackers to inject persistent malicious scripts via the tunable parameter. Attackers can submit POST requests with script payloads that are stored and executed in the context of authenticated user sessions when the page is viewed.	Patched by core rule	Y
CVE-2019-25370	OPNsense 19.1 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input through multiple parameters.	OPNsense 19.1 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input through multiple parameters. Attackers can send POST requests to interfaces_vlan_edit.php with script payloads in the tag, descr, or vlanif parameters to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y
CVE-2019-25371	OPNsense 19.1 contains a reflected cross-site scripting vulnerability that allows unauthenticated	OPNsense 19.1 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	attackers to inject malicious scripts by exploiting insufficient input validation in the host parameter.	exploiting insufficient input validation in the host parameter. Attackers can submit crafted POST requests to the diag_ping.php endpoint with script payloads in the host parameter to execute arbitrary JavaScript in users' browsers.		
CVE-2019-25372	OPNsense 19.1 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by exploiting insufficient input validation in the host parameter.	OPNsense 19.1 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by exploiting insufficient input validation in the host parameter. Attackers can submit crafted payloads through POST requests to diag_traceroute.php to execute arbitrary JavaScript in the context of a user's browser session.	Patched by core rule	Y
CVE-2019-25373	OPNsense 19.1 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by submitting crafted input to the category parameter.	OPNsense 19.1 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by submitting crafted input to the category parameter. Attackers can send POST requests to firewall_rules_edit.php with script payloads in the category field to execute arbitrary JavaScript in the browsers of other users accessing firewall rule pages.	Patched by core rule	Y
CVE-2019-25374	OPNsense 19.1 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by exploiting the passthrough_networks parameter in vpn_ipsec_settings.php.	OPNsense 19.1 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by exploiting the passthrough_networks parameter in vpn_ipsec_settings.php. Attackers can craft POST requests with JavaScript payloads in the passthrough_networks parameter to execute arbitrary code in users' browsers.	Patched by core rule	Y
CVE-2019-25375	OPNsense 19.1 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting crafted input to the mailserver parameter.	OPNsense 19.1 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting crafted input to the mailserver parameter. Attackers can send POST requests to the monit interface with JavaScript payloads in the mailserver	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		parameter to execute arbitrary code in users' browsers.		
CVE-2019-25376	OPNsense 19.1 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting crafted payloads through the ignoreLogACL parameter.	OPNsense 19.1 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting crafted payloads through the ignoreLogACL parameter. Attackers can send POST requests to the proxy endpoint with JavaScript code in the ignoreLogACL parameter to execute arbitrary scripts in users' browsers.	Patched by core rule	Y
CVE-2019-25377	OPNsense 19.1 contains a reflected cross-site scripting vulnerability in the system_advanced_sysctl.php endpoint that allows attackers to inject malicious scripts via the value parameter.	OPNsense 19.1 contains a reflected cross-site scripting vulnerability in the system_advanced_sysctl.php endpoint that allows attackers to inject malicious scripts via the value parameter. Attackers can craft POST requests with script payloads in the value parameter to execute JavaScript in the context of authenticated user sessions.	Patched by core rule	Y
CVE-2019-25378	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple cross-site scripting vulnerabilities in the proxy.cgi endpoint that allow attackers to inject malicious scripts through parameters including CACHE_SIZE, MAX_SIZE, MIN_SIZE, MAX_OUTGOING_SIZE, and MAX_INCOMING_SIZE.	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple cross-site scripting vulnerabilities in the proxy.cgi endpoint that allow attackers to inject malicious scripts through parameters including CACHE_SIZE, MAX_SIZE, MIN_SIZE, MAX_OUTGOING_SIZE, and MAX_INCOMING_SIZE. Attackers can submit POST requests with script payloads to store or reflect arbitrary JavaScript code that executes in users' browsers when the proxy configuration page is accessed.	Patched by core rule	Y
CVE-2019-25379	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains stored and reflected cross-site scripting vulnerabilities in the urlfilter.cgi endpoint that allow attackers to inject malicious scripts.	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains stored and reflected cross-site scripting vulnerabilities in the urlfilter.cgi endpoint that allow attackers to inject malicious scripts. Attackers can submit POST requests with script payloads in the REDIRECT_PAGE or CHILDREN parameters to execute arbitrary JavaScript in user browsers.	Patched by core rule	Y
CVE-2019-25380	Smoothwall Express 3.1-	Smoothwall Express 3.1-SP4-	Patched by core	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	SP4-polar-x86_64-update9 contains multiple reflected cross-site scripting vulnerabilities in the dhcp.cgi script that allow attackers to inject malicious scripts through multiple parameters.	polar-x86_64-update9 contains multiple reflected cross-site scripting vulnerabilities in the dhcp.cgi script that allow attackers to inject malicious scripts through multiple parameters. Attackers can submit POST requests to dhcp.cgi with script payloads in parameters such as BOOT_SERVER, BOOT_FILE, BOOT_ROOT, START_ADDR, END_ADDR, DNS1, DNS2, NTP1, NTP2, WINS1, WINS2, DEFAULT_LEASE_TIME, MAX_LEASE_TIME, DOMAIN_NAME, NIS_DOMAIN, NIS1, NIS2, STATIC_HOST, STATIC_DESC, STATIC_MAC, and STATIC_IP to execute arbitrary JavaScript in user browsers.	rule	
CVE-2019-25381	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple reflected cross-site scripting vulnerabilities in the hosts.cgi script that allow attackers to inject malicious scripts through unvalidated parameters.	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple reflected cross-site scripting vulnerabilities in the hosts.cgi script that allow attackers to inject malicious scripts through unvalidated parameters. Attackers can submit POST requests to the hosts.cgi endpoint with script payloads in the IP, HOSTNAME, or COMMENT parameters to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y
CVE-2019-25382	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the NTP_SERVER parameter.	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the NTP_SERVER parameter. Attackers can send POST requests to the time.cgi endpoint with script payloads in the NTP_SERVER parameter to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y
CVE-2019-25383	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple reflected cross-site scripting vulnerabilities in the apcupsd.cgi script that allow attackers to inject malicious scripts through multiple POST parameters.	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple reflected cross-site scripting vulnerabilities in the apcupsd.cgi script that allow attackers to inject malicious scripts through multiple POST parameters. Attackers can submit crafted POST requests with script payloads in parameters like	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		BATTLEVEL, RTMIN, BATTDELAY, TO, ANNOY, UPSIP, UPSNAME, UPSPORT, POLLTIME, UPSUSER, NISPORT, UPSAUTH, EMAIL, FROM, CC, SMSEMAIL, SMTPSERVER, PORT, USER, and EMAIL_PASSWORD to execute arbitrary JavaScript in victim browsers.		
CVE-2019-25384	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple reflected cross-site scripting vulnerabilities in the portfw.cgi script that allow attackers to inject malicious scripts through unvalidated parameters.	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple reflected cross-site scripting vulnerabilities in the portfw.cgi script that allow attackers to inject malicious scripts through unvalidated parameters. Attackers can submit POST requests with script payloads in the EXT, SRC_PORT_SEL, SRC_PORT, DEST_IP, DEST_PORT_SEL, or COMMENT parameters to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y
CVE-2019-25385	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the MACHINE and MACHINECOMMENT parameters.	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the MACHINE and MACHINECOMMENT parameters. Attackers can send POST requests to the outgoing.cgi endpoint with script payloads to execute arbitrary JavaScript in users' browsers and steal session data.	Patched by core rule	Y
CVE-2019-25386	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple reflected cross-site scripting vulnerabilities in the dmzholes.cgi script that allow attackers to inject malicious scripts through unvalidated parameters.	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple reflected cross-site scripting vulnerabilities in the dmzholes.cgi script that allow attackers to inject malicious scripts through unvalidated parameters. Attackers can submit POST requests with script payloads in the SRC_IP, DEST_IP, or COMMENT parameters to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y
CVE-2019-25387	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting crafted input to the xtaccess.cgi	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	malicious scripts by submitting crafted input to the xtaccess.cgi endpoint.	endpoint. Attackers can inject script payloads through the EXT, DEST_PORT, or COMMENT parameters via POST requests to execute arbitrary JavaScript in victim browsers.		
CVE-2019-25388	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting crafted input to the ipblock.cgi endpoint.	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting crafted input to the ipblock.cgi endpoint. Attackers can inject script tags through the SRC_IP and COMMENT parameters in POST requests to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y
CVE-2019-25389	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the MACHINES parameter.	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the MACHINES parameter. Attackers can craft requests to the timedaccess.cgi endpoint with script payloads in the MACHINES parameter to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y
CVE-2019-25390	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple reflected cross-site scripting vulnerabilities in the interfaces.cgi script that allow attackers to inject malicious scripts through multiple parameters including GREEN_ADDRESS, GREEN_NETMASK, RED_DHCP_HOSTNAME, RED_ADDRESS, DNS1_OVERRIDE, DNS2_OVERRIDE, RED_MAC, RED_NETMASK, DEFAULT_GATEWAY, DNS1, and DNS2.	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple reflected cross-site scripting vulnerabilities in the interfaces.cgi script that allow attackers to inject malicious scripts through multiple parameters including GREEN_ADDRESS, GREEN_NETMASK, RED_DHCP_HOSTNAME, RED_ADDRESS, DNS1_OVERRIDE, DNS2_OVERRIDE, RED_MAC, RED_NETMASK, DEFAULT_GATEWAY, DNS1, and DNS2. Attackers can craft POST requests to interfaces.cgi with script payloads in these parameters to execute arbitrary JavaScript in the context of authenticated administrator sessions.	Patched by core rule	Y
CVE-2019-25392	Smoothwall Express 3.1-SP4-polar-x86_64-	Smoothwall Express 3.1-SP4-polar-x86_64-update9	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	update9 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the IP parameter.	contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the IP parameter. Attackers can send POST requests to the iptools.cgi endpoint with script payloads in the IP parameter to execute arbitrary JavaScript in victim browsers.		
CVE-2019-25393	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by exploiting insufficient input validation.	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by exploiting insufficient input validation. Attackers can submit POST requests to the smoothinfo.cgi endpoint with script payloads in the WRAP or SECTIONTITLE parameters to execute arbitrary JavaScript in victim browsers.	Patched by core rule	Y
CVE-2019-25394	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple stored cross-site scripting vulnerabilities in the modem.cgi script that allow attackers to inject malicious scripts through POST parameters.	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple stored cross-site scripting vulnerabilities in the modem.cgi script that allow attackers to inject malicious scripts through POST parameters. Attackers can submit crafted payloads in parameters like INIT, HANGUP, SPEAKER_ON, SPEAKER_OFF, TONE_DIAL, and PULSE_DIAL to execute arbitrary JavaScript in users' browsers when the stored data is retrieved.	Patched by core rule	Y
CVE-2019-25395	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple stored cross-site scripting vulnerabilities in the preferences.cgi script that allow attackers to inject malicious scripts through the HOSTNAME, KEYMAP, and OPENNESS parameters.	Smoothwall Express 3.1-SP4-polar-x86_64-update9 contains multiple stored cross-site scripting vulnerabilities in the preferences.cgi script that allow attackers to inject malicious scripts through the HOSTNAME, KEYMAP, and OPENNESS parameters. Attackers can submit POST requests with script payloads to preferences.cgi to store malicious code that executes in the browsers of users accessing the preferences page.	Patched by core rule	Y
CVE-2019-25396	IPFire 2.21 Core Update 127 contains a reflected cross-site scripting	IPFire 2.21 Core Update 127 contains a reflected cross-site scripting vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	vulnerability in the updatexlrator.cgi script that allows attackers to inject malicious scripts through POST parameters.	the updatexlrator.cgi script that allows attackers to inject malicious scripts through POST parameters. Attackers can submit crafted requests with script payloads in the MAX_DISK_USAGE or MAX_DOWNLOAD_RATE parameters to execute arbitrary JavaScript in users' browsers.		
CVE-2019-25397	IPFire 2.21 Core Update 127 contains multiple reflected cross-site scripting vulnerabilities in the hosts.cgi script that allow attackers to inject malicious scripts through unvalidated parameters.	IPFire 2.21 Core Update 127 contains multiple reflected cross-site scripting vulnerabilities in the hosts.cgi script that allow attackers to inject malicious scripts through unvalidated parameters. Attackers can submit POST requests with script payloads in the KEY1, IP, HOST, or DOM parameters to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y
CVE-2019-25398	IPFire 2.21 Core Update 127 contains multiple cross-site scripting vulnerabilities in the ovpnmain.cgi script that allow attackers to inject malicious scripts through VPN configuration parameters.	IPFire 2.21 Core Update 127 contains multiple cross-site scripting vulnerabilities in the ovpnmain.cgi script that allow attackers to inject malicious scripts through VPN configuration parameters. Attackers can submit POST requests with script payloads in parameters like VPN_IP, DMTU, ccdname, ccdsubnet, DOVPN_SUBNET, DHCP_DOMAIN, DHCP_DNS, DHCP_WINS, ROUTES_PUSH, FRAGMENT, KEEPALIVE_1, and KEEPALIVE_2 to execute arbitrary JavaScript in administrator browsers.	Patched by core rule	Y
CVE-2019-25399	IPFire 2.21 Core Update 127 contains multiple stored cross-site scripting vulnerabilities in the extrahd.cgi script that allow attackers to inject malicious scripts through the FS, PATH, and UUID parameters.	IPFire 2.21 Core Update 127 contains multiple stored cross-site scripting vulnerabilities in the extrahd.cgi script that allow attackers to inject malicious scripts through the FS, PATH, and UUID parameters. Attackers can submit POST requests with script payloads in these parameters to execute arbitrary JavaScript in the context of authenticated administrator sessions.	Patched by core rule	Y
CVE-2019-25400	IPFire 2.21 Core Update 127 contains multiple reflected cross-site scripting vulnerabilities in the fwhosts.cgi script	IPFire 2.21 Core Update 127 contains multiple reflected cross-site scripting vulnerabilities in the fwhosts.cgi script that allow	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	that allow attackers to inject malicious scripts through multiple parameters including HOSTNAME, IP, SUBNET, NETREMARK, HOSTREMARK, newhost, grp_name, remark, SRV_NAME, SRV_PORT, SRVGRP_NAME, SRVGRP_REMARK, and updatesrvgrp.	attackers to inject malicious scripts through multiple parameters including HOSTNAME, IP, SUBNET, NETREMARK, HOSTREMARK, newhost, grp_name, remark, SRV_NAME, SRV_PORT, SRVGRP_NAME, SRVGRP_REMARK, and updatesrvgrp. Attackers can submit POST requests with script payloads in these parameters to execute arbitrary JavaScript in the context of authenticated users' browsers.		
CVE-2019-25402	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting crafted input to the username parameter.	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting crafted input to the username parameter. Attackers can send POST requests to the login endpoint with script payloads in the username field to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y
CVE-2019-25403	Comodo Dome Firewall 2.7.0 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by submitting crafted input to the comment parameter.	Comodo Dome Firewall 2.7.0 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by submitting crafted input to the comment parameter. Attackers can inject JavaScript code through the admin_profiles endpoint that executes in the browsers of other users who view the affected page.	Patched by core rule	Y
CVE-2019-25404	Comodo Dome Firewall 2.7.0 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by submitting crafted input through admin management parameters.	Comodo Dome Firewall 2.7.0 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by submitting crafted input through admin management parameters. Attackers can inject script payloads in the admin_name, name, and surname parameters via POST requests to the /korugan/admins endpoint, which are stored and executed when administrators access the interface.	Patched by core rule	Y
CVE-2019-25405	Comodo Dome Firewall 2.7.0 contains a stored cross-site scripting vulnerability that allows	Comodo Dome Firewall 2.7.0 contains a stored cross-site scripting vulnerability that allows attackers to inject	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	attackers to inject malicious scripts by submitting crafted input to the newLicense parameter.	malicious scripts by submitting crafted input to the newLicense parameter. Attackers can send POST requests to the license activation endpoint with script payloads in the newLicense field to execute arbitrary JavaScript in administrators' browsers.		
CVE-2019-25406	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the organization parameter.	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the organization parameter. Attackers can send POST requests to the korugan/cmclient endpoint with script payloads in the organization parameter to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y
CVE-2019-25407	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the backup schedule interface.	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the backup schedule interface. Attackers can send POST requests to the backupschedule endpoint with JavaScript code in the BACKUP_RCPTTO parameter to execute arbitrary scripts in users' browsers.	Patched by core rule	Y
CVE-2019-25408	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the netmask_addr parameter.	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the netmask_addr parameter. Attackers can send POST requests to the netwizard2 endpoint with script payloads in the netmask_addr parameter to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y
CVE-2019-25409	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the destination parameter.	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the destination parameter. Attackers can send POST requests to the routing endpoint with script payloads in the destination parameter to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2019-25410	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts through the source and destination parameters.	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts through the source and destination parameters. Attackers can submit POST requests to the policy routing endpoint with script payloads in these parameters to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y
CVE-2019-25411	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the GATEWAY_GREEN parameter.	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the GATEWAY_GREEN parameter. Attackers can send POST requests to the DHCP configuration endpoint with script payloads to execute arbitrary JavaScript in administrator browsers.	Patched by core rule	Y
CVE-2019-25412	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting unsanitized input through the NTP_SERVER_LIST parameter.	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting unsanitized input through the NTP_SERVER_LIST parameter. Attackers can send POST requests to the /korugan/time endpoint with script payloads in the NTP_SERVER_LIST parameter to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y
CVE-2019-25413	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the ID parameter.	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the ID parameter. Attackers can craft requests to the /manage/ips/rules/ endpoint with script payloads in the ID parameter to execute arbitrary JavaScript in victim browsers.	Patched by core rule	Y
CVE-2019-25414	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the ID parameter. Attackers can	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	manipulating the ID parameter.	craft requests to the /manage/ips/appid/ endpoint with script payloads in the ID parameter to execute arbitrary JavaScript in victim browsers.		
CVE-2019-25415	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting unsanitized input to the hotspot_permanent_users endpoint.	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting unsanitized input to the hotspot_permanent_users endpoint. Attackers can send POST requests with JavaScript payloads in the MACADDRESSES parameter to execute arbitrary scripts in users' browsers.	Patched by core rule	Y
CVE-2019-25416	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input through the device parameter.	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input through the device parameter. Attackers can send POST requests to the QoS devices management endpoint with script payloads in the device parameter to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y
CVE-2019-25417	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the protocol parameter.	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the protocol parameter. Attackers can send POST requests to the QoS rules management endpoint with JavaScript payloads in the protocol parameter to execute arbitrary code in administrator browsers.	Patched by core rule	Y
CVE-2019-25418	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the FWADDRESSES parameter.	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the FWADDRESSES parameter. Attackers can send POST requests to the /korugan/fwgroups endpoint with script payloads to execute arbitrary JavaScript in users' browsers and steal session data.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2019-25419	Comodo Dome Firewall 2.7.0 contains a stored cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the schedule endpoint.	Comodo Dome Firewall 2.7.0 contains a stored cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the schedule endpoint. Attackers can submit POST requests with JavaScript payloads in the SCHNAME parameter to execute arbitrary code in administrators' browsers when the schedule page is accessed.	Patched by core rule	Y
CVE-2019-25420	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the snat endpoint.	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the snat endpoint. Attackers can send POST requests with JavaScript payloads in the port or snat_to_ip parameters to execute arbitrary scripts in users' browsers.	Patched by core rule	Y
CVE-2019-25421	Comodo Dome Firewall 2.7.0 contains multiple cross-site scripting vulnerabilities that allow attackers to inject malicious scripts through the policyfw endpoint.	Comodo Dome Firewall 2.7.0 contains multiple cross-site scripting vulnerabilities that allow attackers to inject malicious scripts through the policyfw endpoint. Attackers can submit POST requests with JavaScript payloads in the mac, target, and remark parameters to execute arbitrary code in administrator browsers or store persistent scripts in the application.	Patched by core rule	Y
CVE-2019-25422	Comodo Dome Firewall 2.7.0 contains cross-site scripting vulnerabilities that allow attackers to inject malicious scripts through the vpnfw endpoint.	Comodo Dome Firewall 2.7.0 contains cross-site scripting vulnerabilities that allow attackers to inject malicious scripts through the vpnfw endpoint. Attackers can submit POST requests with script payloads in the target parameter for reflected XSS or the remark parameter for stored XSS to execute arbitrary JavaScript in administrator browsers.	Patched by core rule	Y
CVE-2019-25423	Comodo Dome Firewall 2.7.0 contains multiple reflected cross-site scripting vulnerabilities in the /korugan/proxyconfig endpoint that allow attackers to inject malicious scripts through POST parameters.	Comodo Dome Firewall 2.7.0 contains multiple reflected cross-site scripting vulnerabilities in the /korugan/proxyconfig endpoint that allow attackers to inject malicious scripts through POST parameters. Attackers can submit crafted POST	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		requests with JavaScript payloads in parameters like PROXY_PORT, VISIBLE_HOSTNAME, ADMIN_MAIL_ADDRESS, CACHE_MEM, MAX_SIZE, MIN_SIZE, and DST_NOCACHE to execute arbitrary scripts in administrator browsers.		
CVE-2019-25424	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting unsanitized input to the EXCEPTIONSITELIST parameter.	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting unsanitized input to the EXCEPTIONSITELIST parameter. Attackers can craft POST requests to the https_exceptions endpoint with script payloads to execute arbitrary JavaScript in users' browsers and steal session data.	Patched by core rule	Y
CVE-2019-25425	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the VIRUS_ADMIN parameter.	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the VIRUS_ADMIN parameter. Attackers can send POST requests to the smtpconfig endpoint with script payloads to execute arbitrary JavaScript in the context of an administrator's browser session.	Patched by core rule	Y
CVE-2019-25426	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the dnsmasq endpoint.	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the dnsmasq endpoint. Attackers can send POST requests with script payloads in the TRANSPARENT_SOURCE_BYPASS or TRANSPARENT_DESTINATION_BYPASS parameters to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y
CVE-2019-25427	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the antispyware endpoint.	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the antispyware endpoint. Attackers can send POST requests with JavaScript payloads in the DNSMASQ_WHITELIST or	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		DNSMASQ_BLACKLIST parameters to execute arbitrary code in users' browsers.		
CVE-2019-25428	Comodo Dome Firewall 2.7.0 contains multiple reflected cross-site scripting vulnerabilities in the openvpn_users endpoint that allow attackers to inject malicious scripts through POST parameters.	Comodo Dome Firewall 2.7.0 contains multiple reflected cross-site scripting vulnerabilities in the openvpn_users endpoint that allow attackers to inject malicious scripts through POST parameters. Attackers can submit crafted POST requests with script payloads in the username, remotenets, explicitroutes, static_ip, custom_dns, or custom_domain parameters to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y
CVE-2019-25429	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the openvpn_advanced endpoint.	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted input to the openvpn_advanced endpoint. Attackers can inject JavaScript code through the GLOBAL_NETWORKS and GLOBAL_DNS parameters via POST requests to execute arbitrary scripts in users' browsers.	Patched by core rule	Y
CVE-2019-25430	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting crafted input to the username parameter.	Comodo Dome Firewall 2.7.0 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by submitting crafted input to the username parameter. Attackers can send POST requests to the vpn_users endpoint with script payloads in the username field to execute arbitrary JavaScript in victim browsers.	Patched by core rule	Y
CVE-2019-25445	Fiverr Clone Script 1.2.2 contains a cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the keyword parameter.	Fiverr Clone Script 1.2.2 contains a cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the keyword parameter. Attackers can craft URLs with script tags in the keyword parameter of search-results.php to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y
CVE-2019-25448	OrientDB 3.0.17 contains a stored cross-site	OrientDB 3.0.17 contains a stored cross-site scripting	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	scripting vulnerability that allows authenticated attackers to inject malicious scripts by creating users with script payloads in the name parameter.	vulnerability that allows authenticated attackers to inject malicious scripts by creating users with script payloads in the name parameter. Attackers can send POST requests to the document endpoint with JavaScript code in the name field to execute arbitrary scripts when users view the application.		
CVE-2019-25449	OrientDB 3.0.17 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted JSON payloads to the document endpoint.	OrientDB 3.0.17 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by submitting crafted JSON payloads to the document endpoint. Attackers can send POST requests to /document/demodb/-1:-1 with script tags in the name parameter to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y
CVE-2019-25453	phpMoAdmin 1.1.5 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the newdb parameter.	phpMoAdmin 1.1.5 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the newdb parameter. Attackers can craft URLs with JavaScript payloads in the newdb parameter of moadmin.php to execute arbitrary code in users' browsers when they visit the malicious link.	Patched by core rule	Y
CVE-2019-25454	phpMoAdmin 1.1.5 contains a stored cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the collection parameter.	phpMoAdmin 1.1.5 contains a stored cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the collection parameter. Attackers can send GET requests to moadmin.php with script payloads in the collection parameter during collection creation to execute arbitrary JavaScript in users' browsers.	Patched by core rule	Y
CVE-2020-36954	Xeroneit Library Management System 3.1 contains a stored cross-site scripting vulnerability in the Book Category feature that allows administrators to inject malicious scripts.	Xeroneit Library Management System 3.1 contains a stored cross-site scripting vulnerability in the Book Category feature that allows administrators to inject malicious scripts. Attackers can insert a payload in the Category Name field to execute arbitrary JavaScript code	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		when the page is loaded.		
CVE-2020-36955	Grav CMS 1.6.30 with Admin Plugin 1.9.18 contains a persistent cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts through the page title field.	Grav CMS 1.6.30 with Admin Plugin 1.9.18 contains a persistent cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts through the page title field. Attackers can create a new page with a malicious script in the title, which will be executed when the page is viewed in the admin panel or on the site.	Patched by core rule	Y
CVE-2020-36956	Openfire 4.6.0 contains a stored cross-site scripting vulnerability in the nodejs plugin that allows attackers to inject malicious scripts through the 'path' parameter.	Openfire 4.6.0 contains a stored cross-site scripting vulnerability in the nodejs plugin that allows attackers to inject malicious scripts through the 'path' parameter. Attackers can craft a payload with script tags to execute arbitrary JavaScript in the context of administrative users viewing the nodejs configuration page.	Patched by core rule	Y
CVE-2020-36960	Forma LMS 2.3 contains a stored cross-site scripting vulnerability that allows attackers to inject malicious scripts into user profile first and last name fields.	Forma LMS 2.3 contains a stored cross-site scripting vulnerability that allows attackers to inject malicious scripts into user profile first and last name fields. Attackers can craft scripts like '<script>alert(document.cookie)</script>' to execute arbitrary JavaScript when the profile is viewed by other users.	Patched by core rule	Y
CVE-2020-36966	Dolibarr 11.0.3 contains a persistent cross-site scripting vulnerability in LDAP synchronization settings that allows attackers to inject malicious scripts through multiple parameters.	Dolibarr 11.0.3 contains a persistent cross-site scripting vulnerability in LDAP synchronization settings that allows attackers to inject malicious scripts through multiple parameters. Attackers can exploit the host, slave, and port parameters in /dolibarr/admin/ldap.php to execute arbitrary JavaScript and potentially steal user cookie information.	Patched by core rule	Y
CVE-2020-36978	Froxlor Server Management Panel 0.10.16 contains a persistent cross-site scripting vulnerability in customer registration input fields.	Froxlor Server Management Panel 0.10.16 contains a persistent cross-site scripting vulnerability in customer registration input fields. Attackers can inject malicious scripts through username, name, and firstname parameters to execute code when	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		administrators view customer traffic modules.		
CVE-2020-36988	PDW File Browser version 1.3 contains stored and reflected cross-site scripting vulnerabilities that allow authenticated attackers to inject malicious scripts through file rename and path parameters.	PDW File Browser version 1.3 contains stored and reflected cross-site scripting vulnerabilities that allow authenticated attackers to inject malicious scripts through file rename and path parameters. Attackers can craft malicious URLs or rename files with XSS payloads to execute arbitrary JavaScript in victims' browsers when they access the file browser.	Patched by core rule	Y
CVE-2020-36993	LimeSurvey 4.3.10 contains a stored cross-site scripting vulnerability in the Survey Menu functionality of the administration panel.	LimeSurvey 4.3.10 contains a stored cross-site scripting vulnerability in the Survey Menu functionality of the administration panel. Attackers can inject malicious SVG scripts through the Surveymenu[title] and Surveymenu[parent_id] parameters to execute arbitrary JavaScript in administrative contexts.	Patched by core rule	Y
CVE-2020-36996	PHPFusion 9.03.50 contains a persistent cross-site scripting vulnerability in the print.php page that fails to properly sanitize user-submitted message content.	PHPFusion 9.03.50 contains a persistent cross-site scripting vulnerability in the print.php page that fails to properly sanitize user-submitted message content. Attackers can inject malicious JavaScript through forum messages that will execute when the print page is generated, allowing script execution in victim browsers.	Patched by core rule	Y
CVE-2020-36998	Forma.lms The E-Learning Suite 2.3.0.2 contains a persistent cross-site scripting vulnerability in multiple course and profile parameters.	Forma.lms The E-Learning Suite 2.3.0.2 contains a persistent cross-site scripting vulnerability in multiple course and profile parameters. Attackers can inject malicious scripts in course code, name, description fields, and email parameter to execute arbitrary JavaScript without proper input sanitization.	Patched by core rule	Y
CVE-2020-37003	Sellacious eCommerce 4.6 contains a persistent cross-site scripting vulnerability in the Manage Your Addresses module that allows attackers to inject malicious scripts.	Sellacious eCommerce 4.6 contains a persistent cross-site scripting vulnerability in the Manage Your Addresses module that allows attackers to inject malicious scripts. Attackers can exploit multiple address input fields like full name, company, and address to execute persistent script code that	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		can hijack user sessions and manipulate application modules.		
CVE-2020-37014	Tryton 5.4 contains a persistent cross-site scripting vulnerability in the user profile name input that allows remote attackers to inject malicious scripts.	Tryton 5.4 contains a persistent cross-site scripting vulnerability in the user profile name input that allows remote attackers to inject malicious scripts. Attackers can exploit the vulnerability by inserting script payloads in the name field, which execute in the frontend and backend user interfaces.	Patched by core rule	Y
CVE-2020-37018	GOautodial 4.0 contains a persistent cross-site scripting vulnerability that allows authenticated agents to inject malicious scripts through message subjects.	GOautodial 4.0 contains a persistent cross-site scripting vulnerability that allows authenticated agents to inject malicious scripts through message subjects. Attackers can craft messages with embedded JavaScript that will execute when an administrator reads the message, potentially stealing session cookies or executing client-side attacks.	Patched by core rule	Y
CVE-2020-37019	Orchard Core RC1 contains a persistent cross-site scripting vulnerability that allows remote attackers to inject malicious scripts through blog post creation.	Orchard Core RC1 contains a persistent cross-site scripting vulnerability that allows remote attackers to inject malicious scripts through blog post creation. Attackers can create blog posts with embedded JavaScript in the MarkdownBodyPart.Source parameter to execute arbitrary scripts in victim browsers.	Patched by core rule	Y
CVE-2020-37022	OpenZ ERP 3.6.60 contains a persistent cross-site scripting vulnerability in the Employee module's name and description parameters.	OpenZ ERP 3.6.60 contains a persistent cross-site scripting vulnerability in the Employee module's name and description parameters. Attackers can inject malicious scripts through POST requests to , enabling session hijacking and manipulation of application modules.	Patched by core rule	Y
CVE-2020-37044	OpenCTI 3.3.1 is vulnerable to a reflected cross-site scripting (XSS) attack via the /graphql endpoint.	OpenCTI 3.3.1 is vulnerable to a reflected cross-site scripting (XSS) attack via the /graphql endpoint. An attacker can inject arbitrary JavaScript code by sending a crafted GET request with a malicious payload in the query string, leading to execution of JavaScript in the victim's browser. For example, a request to /graphql?'"--	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		></style></scRipt><scRipt>alert('Raif_Berkay')</scRipt> will trigger an alert. This vulnerability was discovered by Raif Berkay Dincel and confirmed on Linux Mint and Windows 10.		
CVE-2020-37072	Victor CMS 1.0 contains a stored cross-site scripting vulnerability in the 'comment_author' POST parameter that allows attackers to inject malicious scripts.	Victor CMS 1.0 contains a stored cross-site scripting vulnerability in the 'comment_author' POST parameter that allows attackers to inject malicious scripts. Attackers can submit crafted JavaScript payloads through the comment submission form to execute arbitrary code in victim browsers.	Patched by core rule	Y
CVE-2020-37087	Easy Transfer Wifi Transfer v1.7 for iOS contains a persistent cross-site scripting vulnerability that allows remote attackers to inject malicious scripts by manipulating the oldPath, newPath, and path parameters in Create Folder and Move/Edit functions.	Easy Transfer Wifi Transfer v1.7 for iOS contains a persistent cross-site scripting vulnerability that allows remote attackers to inject malicious scripts by manipulating the oldPath, newPath, and path parameters in Create Folder and Move/Edit functions. Attackers can exploit improper input validation via POST requests to execute arbitrary JavaScript in the context of the mobile web application.	Patched by core rule	Y
CVE-2020-37103	DotNetNuke 9.5 contains a persistent cross-site scripting vulnerability that allows normal users to upload malicious XML files with executable scripts through journal tools.	DotNetNuke 9.5 contains a persistent cross-site scripting vulnerability that allows normal users to upload malicious XML files with executable scripts through journal tools. Attackers can upload XML files with XHTML namespace scripts to execute arbitrary JavaScript in users' browsers, potentially bypassing CSRF protections and performing more damaging attacks.	Patched by core rule	Y
CVE-2020-37111	60CycleCMS 2.5.2 contains a cross-site scripting (XSS) vulnerability in news.php that allows attackers to inject malicious scripts through GET parameters.	60CycleCMS 2.5.2 contains a cross-site scripting (XSS) vulnerability in news.php that allows attackers to inject malicious scripts through GET parameters. Attackers can craft malicious URLs with XSS payloads targeting the 'etsu' and 'ltsu' parameters to execute arbitrary scripts in victim's browsers. This issue does not involve SQL injection.	Patched by core rule	Y
CVE-2020-37148	P5 FNIP-8x16A/FNIP-4xSH versions 1.0.20 and	P5 FNIP-8x16A/FNIP-4xSH versions 1.0.20 and 1.0.11	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	1.0.11 suffer from a stored cross-site scripting vulnerability.	suffer from a stored cross-site scripting vulnerability. Input passed to several GET/POST parameters is not properly sanitized before being returned to the user, allowing attackers to execute arbitrary HTML and script code in a user's browser session in the context of the affected site. This can be exploited by submitting crafted input to the label modification functionality, such as the 'lab4' parameter in config.html.		
CVE-2020-37152	PHP-Fusion 9.03.50 panels.php is vulnerable to cross-site scripting (XSS) via the 'panel_content' POST parameter.	PHP-Fusion 9.03.50 panels.php is vulnerable to cross-site scripting (XSS) via the 'panel_content' POST parameter. The application fails to properly sanitize user input before rendering it in the browser, allowing attackers to inject arbitrary JavaScript. This can be exploited by submitting crafted input to the 'panel_content' field in panels.php, resulting in execution of malicious scripts in the context of the affected site.	Patched by core rule	Y
CVE-2020-37153	ASTPP 4.0.1 contains multiple vulnerabilities including cross-site scripting and command injection in SIP device configuration and plugin management interfaces.	ASTPP 4.0.1 contains multiple vulnerabilities including cross-site scripting and command injection in SIP device configuration and plugin management interfaces. Attackers can exploit these flaws to inject system commands, hijack administrator sessions, and potentially execute arbitrary code with root permissions through cron task manipulation.	Patched by core rule	Y
CVE-2021-47912	PHP Melody version 3.0 contains multiple non-persistent cross-site scripting vulnerabilities in categories, import, and user import files.	PHP Melody version 3.0 contains multiple non-persistent cross-site scripting vulnerabilities in categories, import, and user import files. Attackers can inject malicious scripts through unvalidated parameters to execute client-side attacks and potentially hijack user sessions.	Patched by core rule	Y
CVE-2021-47913	PHP Melody 3.0 contains a persistent cross-site scripting vulnerability in the video editor that allows privileged users to	PHP Melody 3.0 contains a persistent cross-site scripting vulnerability in the video editor that allows privileged users to inject	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	inject malicious scripts.	malicious scripts. Attackers can exploit the WYSIWYG editor to execute persistent scripts, potentially leading to session hijacking and application manipulation.		
CVE-2021-47914	PHP Melody version 3.0 contains a persistent cross-site scripting vulnerability in the edit-video.php submitted parameter that allows remote attackers to inject malicious script code.	PHP Melody version 3.0 contains a persistent cross-site scripting vulnerability in the edit-video.php submitted parameter that allows remote attackers to inject malicious script code. Attackers can exploit this vulnerability to execute arbitrary JavaScript, potentially leading to session hijacking, persistent phishing, and manipulation of application modules.	Patched by core rule	Y
CVE-2021-47917	Simple CMS 2.1 contains a persistent cross-site scripting vulnerability in user input parameters that allows remote attackers to inject malicious script code.	Simple CMS 2.1 contains a persistent cross-site scripting vulnerability in user input parameters that allows remote attackers to inject malicious script code. Attackers can exploit the newUser and editUser modules to inject persistent scripts that execute on user list preview, potentially leading to session hijacking and application manipulation.	Patched by core rule	Y
CVE-2021-47919	Simple CMS 2.1 contains a non-persistent cross-site scripting vulnerability in the preview.php file's id parameter.	Simple CMS 2.1 contains a non-persistent cross-site scripting vulnerability in the preview.php file's id parameter. Attackers can inject malicious script code through a GET request to execute arbitrary scripts and potentially hijack user sessions or perform phishing attacks.	Patched by core rule	Y
CVE-2025-13672	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in OpenText,Ñ¢ Web Site Management Server allows Reflected XSS.	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in OpenText,Ñ¢ Web Site Management Server allows Reflected XSS. The vulnerability could allow injecting malicious JavaScript inside URL parameters that was then rendered with the preview of the page, so that malicious scripts could be executed on the client side. This issue affects Web Site Management Server: 16.7.0, 16.7.1.	Patched by core rule	Y
CVE-2025-15386	The Responsive Lightbox & Gallery WordPress plugin before 2.6.1 is	The Responsive Lightbox & Gallery WordPress plugin before 2.6.1 is vulnerable to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	vulnerable to an Unauthenticated Stored-XSS attack due to flawed regex replacement rules that can be abused by posting a comment with a malicious link when lightbox for comments are enabled and then approved.	an Unauthenticated Stored-XSS attack due to flawed regex replacement rules that can be abused by posting a comment with a malicious link when lightbox for comments are enabled and then approved.		
CVE-2025-15396	The Library Viewer WordPress plugin before 3.2.0 does not sanitise and escape some parameters before outputting them back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	The Library Viewer WordPress plugin before 3.2.0 does not sanitise and escape some parameters before outputting them back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	Patched by core rule	Y
CVE-2025-15583	A weakness has been identified in detronetdip E-commerce 1.0.0.	A weakness has been identified in detronetdip E-commerce 1.0.0. This affects the function get_safe_value of the file utility/function.php. Executing a manipulation can lead to cross site scripting. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	Patched by core rule	Y
CVE-2025-65717	An issue in Visual Studio Code Extensions Live Server v5.7.9 allows attackers to exfiltrate files via user interaction with a crafted HTML page.	An issue in Visual Studio Code Extensions Live Server v5.7.9 allows attackers to exfiltrate files via user interaction with a crafted HTML page.	Patched by core rule	Y
CVE-2025-67491	OpenEMR is a free and open source electronic health records and medical practice management application.	OpenEMR is a free and open source electronic health records and medical practice management application. Versions 5.0.0.5 through 7.0.3.4 have a stored cross-site scripting vulnerability in the ub04 helper of the billing interface. The variable `$data` is passed in a click event handler enclosed in single quotes without proper sanitization. Thus, despite `json_encode` a malicious user can still inject a payload such as ` ac' ><img src=x onerror=alert(document.cookie)> ` to trigger the bug. This vulnerability allows low	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		privileged users to embed malicious JS payloads on the server and perform stored XSS attack. This, in turn makes it possible for malicious users to steal the session cookies and perform unauthorized actions impersonating administrators. Version 7.0.4 patches the issue.		
CVE-2025-69231	OpenEMR is a free and open source electronic health records and medical practice management application.	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0, a stored cross-site scripting vulnerability in the GAD-7 anxiety assessment form allows authenticated users with clinician privileges to inject malicious JavaScript that executes when other users view the form. This enables session hijacking, account takeover, and privilege escalation from clinician to administrator. Version 8.0.0 fixes the issue.	Patched by core rule	Y
CVE-2025-69749	Cross Site Scripting vulnerability in tale v.2.0.5 allows an attacker to execute arbitrary code.	Cross Site Scripting vulnerability in tale v.2.0.5 allows an attacker to execute arbitrary code.	Patched by core rule	Y
CVE-2025-70091	A cross-site scripting (XSS) vulnerability in the Customers function of OpenSourcePOS v3.4.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Phone Number parameter.	A cross-site scripting (XSS) vulnerability in the Customers function of OpenSourcePOS v3.4.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Phone Number parameter.	Patched by core rule	Y
CVE-2025-70092	A cross-site scripting (XSS) vulnerability in the Item Kits function of OpenSourcePOS v3.4.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Item Name parameter.	A cross-site scripting (XSS) vulnerability in the Item Kits function of OpenSourcePOS v3.4.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Item Name parameter.	Patched by core rule	Y
CVE-2025-70094	A cross-site scripting (XSS) vulnerability in the Generate Item Barcode function of OpenSourcePOS v3.4.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Item Category parameter.	A cross-site scripting (XSS) vulnerability in the Generate Item Barcode function of OpenSourcePOS v3.4.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Item Category parameter.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-70095	A cross-site scripting (XSS) vulnerability in the item management and sales invoice function of OpenSourcePOS v3.4.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload.	A cross-site scripting (XSS) vulnerability in the item management and sales invoice function of OpenSourcePOS v3.4.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload.	Patched by core rule	Y
CVE-2025-70296	A stored HTML injection vulnerability in the Recipe Notes rendering component in Mealie 3.3.1 allows remote authenticated users to inject arbitrary HTML, resulting in user interface redressing within the recipe view.	A stored HTML injection vulnerability in the Recipe Notes rendering component in Mealie 3.3.1 allows remote authenticated users to inject arbitrary HTML, resulting in user interface redressing within the recipe view.	Patched by core rule	Y
CVE-2025-70297	A stored cross-site scripting (XSS) vulnerability in the recipe asset upload and media serving component in Mealie 3.3.1 allows remote authenticated users to inject arbitrary web script or HTML via an uploaded SVG file that is served as image/svg+xml and rendered by a victim s browser.	A stored cross-site scripting (XSS) vulnerability in the recipe asset upload and media serving component in Mealie 3.3.1 allows remote authenticated users to inject arbitrary web script or HTML via an uploaded SVG file that is served as image/svg+xml and rendered by a victim s browser.	Patched by core rule	Y
CVE-2025-70368	Worklenz version 2.1.5 contains a Stored Cross-Site Scripting (XSS) vulnerability in the Project Updates feature.	Worklenz version 2.1.5 contains a Stored Cross-Site Scripting (XSS) vulnerability in the Project Updates feature. An attacker can submit a malicious payload in the Updates text field which is then rendered in the reporting view without proper sanitization. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	Patched by core rule	Y
CVE-2025-70791	Cross Site Scripting vulnerability in the "/admin/order/abandoned" endpoint of Microweber 2.0.19.	Cross Site Scripting vulnerability in the "/admin/order/abandoned" endpoint of Microweber 2.0.19. An attacker can manipulate the "orderDirection" parameter in a crafted URL and lure a user with admin privileges into visiting it, achieving JavaScript code execution in the victim's browser. The issue was reported to the developers and fixed in version 2.0.20.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2025-70792	Cross Site Scripting vulnerability in the "/admin/category/create" endpoint of Microweber 2.0.19.	Cross Site Scripting vulnerability in the "/admin/category/create" endpoint of Microweber 2.0.19. An attacker can manipulate the "rel_id" parameter in a crafted URL and lure a user with admin privileges into visiting it, achieving JavaScript code execution in the victim's browser. The issue was reported to the developers and fixed in version 2.0.20.	Patched by core rule	Y
CVE-2025-70849	Arbitrary File Upload in podinfo thru 6.9.0 allows unauthenticated attackers to upload arbitrary files via crafted POST request to the /store endpoint.	Arbitrary File Upload in podinfo thru 6.9.0 allows unauthenticated attackers to upload arbitrary files via crafted POST request to the /store endpoint. The application renders uploaded content without a restrictive Content-Security-Policy (CSP) or adequate Content-Type validation, leading to Stored Cross-Site Scripting (XSS).	Patched by core rule	Y
CVE-2025-70958	Multiple reflected cross-site scripting (XSS) vulnerabilities in the installation module of Subrion CMS v4.2.1 allows attackers to execute arbitrary Javascript in the context of the user's browser via injecting a crafted payload into the dbuser, dbpwd, and dbname parameters.	Multiple reflected cross-site scripting (XSS) vulnerabilities in the installation module of Subrion CMS v4.2.1 allows attackers to execute arbitrary Javascript in the context of the user's browser via injecting a crafted payload into the dbuser, dbpwd, and dbname parameters.	Patched by core rule	Y
CVE-2025-70959	A stored cross-site scripting (XSS) vulnerability in the Jobs module of Tendenci CMS v15.3.7 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload.	A stored cross-site scripting (XSS) vulnerability in the Jobs module of Tendenci CMS v15.3.7 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload.	Patched by core rule	Y
CVE-2025-70960	A stored cross-site scripting (XSS) vulnerability in the Forums module of Tendenci CMS v15.3.7 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload.	A stored cross-site scripting (XSS) vulnerability in the Forums module of Tendenci CMS v15.3.7 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload.	Patched by core rule	Y
CVE-2025-71179	Creativeitem Academy LMS 7.0 contains reflected Cross-Site Scripting (XSS) vulnerabilities via the	Creativeitem Academy LMS 7.0 contains reflected Cross-Site Scripting (XSS) vulnerabilities via the search parameter to the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	search parameter to the /academy/blogs endpoint, and the string parameter to the /academy/course_bundles/search/query endpoint.	/academy/blogs endpoint, and the string parameter to the /academy/course_bundles/search/query endpoint. These vulnerabilities are distinct from the patch for CVE-2023-4119, which only fixed XSS in query and sort_by parameters to the /academy/home/courses endpoint.		
CVE-2025-9208	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in OpenText,Ñ¢ Web Site Management Server allows Stored XSS.	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in OpenText,Ñ¢ Web Site Management Server allows Stored XSS. The vulnerability could execute malicious scripts on the client side when the download query parameter is removed from the file URL, allowing attackers to compromise user sessions and data. This issue affects Web Site Management Server: 16.7.X, 16.8, 16.8.1.	Patched by core rule	Y
CVE-2026-0521	A reflected cross-site scripting (XSS) vulnerability in the PDF export functionality of the TYDAC AG MAP+ solution allows unauthenticated attackers to craft a malicious URL, that if visited by a victim, will execute arbitrary JavaScript in the victim's context.	A reflected cross-site scripting (XSS) vulnerability in the PDF export functionality of the TYDAC AG MAP+ solution allows unauthenticated attackers to craft a malicious URL, that if visited by a victim, will execute arbitrary JavaScript in the victim's context. Such a URL could be delivered through various means, for instance, by sending a link or by tricking victims to visit a page crafted by the attacker. This issue was verified in MAP+: 3.4.0.	Patched by core rule	Y
CVE-2026-1337	Insufficient escaping of unicode characters in query log in Neo4j Enterprise and Community editions prior to 2026.01 can lead to XSS if the user opens the logs in a tool that treats them as HTML.	Insufficient escaping of unicode characters in query log in Neo4j Enterprise and Community editions prior to 2026.01 can lead to XSS if the user opens the logs in a tool that treats them as HTML. There is no security impact on Neo4j products, but this advisory is released as a precaution to treat the logs as plain text if using versions prior to 2026.01. Proof of concept exploit: https://github.com/JoakimBulow/CVE-2026-1337	Patched by core rule	Y
CVE-2026-1421	A vulnerability has been found in code-projects Online Examination	A vulnerability has been found in code-projects Online Examination System	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	System 1.0.	1.0. Affected is an unknown function of the component Add Pages. Such manipulation leads to cross site scripting. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.		
CVE-2026-1520	A vulnerability was identified in rethinkdb up to 2.4.3.	A vulnerability was identified in rethinkdb up to 2.4.3. Affected by this issue is some unknown functionality of the component Secondary Index Handler. Such manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-1598	A vulnerability was found in Bdtask Bhojon All-In-One Restaurant Management System up to 20260116.	A vulnerability was found in Bdtask Bhojon All-In-One Restaurant Management System up to 20260116. Impacted is an unknown function of the file /dashboard/home/profile of the component User Information Module. Performing a manipulation of the argument fullname results in cross site scripting. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-1700	A weakness has been identified in projectworlds House Rental and Property Listing 1.0.	A weakness has been identified in projectworlds House Rental and Property Listing 1.0. This vulnerability affects unknown code of the file /app/sms.php. This manipulation of the argument Message causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-1744	A vulnerability was found in D-Link DSL-6641K N8.TR069.20131126.	A vulnerability was found in D-Link DSL-6641K N8.TR069.20131126. Affected by this issue is the function doSubmitPPP of the file sp_pppoe_user.js. The manipulation of the argument Username results in cross site scripting. The	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attack may be launched remotely. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.		
CVE-2026-1971	A vulnerability has been found in Edimax BR-6288ACL up to 1.12.	A vulnerability has been found in Edimax BR-6288ACL up to 1.12. Impacted is the function wiz_WISP24gmanual of the file wiz_WISP24gmanual.asp. Such manipulation of the argument manualssid leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor confirms that the affected product is end-of-life. They confirm that they "will issue a consolidated Security Advisory on our official support website." This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2026-2064	A vulnerability was identified in Portabilis i-Educar up to 2.10.	A vulnerability was identified in Portabilis i-Educar up to 2.10. Affected by this vulnerability is an unknown functionality of the file /intranet/meusdadod.php of the component User Data Page. Such manipulation of the argument File leads to cross site scripting. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-2149	A vulnerability was detected in SourceCodester/Patrick Mvuma Patients Waiting Area Queue Management System 1.0.	A vulnerability was detected in SourceCodester/Patrick Mvuma Patients Waiting Area Queue Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /appointments.php. The manipulation of the argument patient_id results in cross site scripting. It is possible to launch the attack remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-2150	A flaw has been found in SourceCodester/Patrick Mvuma Patients Waiting	A flaw has been found in SourceCodester/Patrick Mvuma Patients Waiting	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Area Queue Management System 1.0.	Area Queue Management System 1.0. Affected by this issue is some unknown functionality of the file /checkin.php. This manipulation of the argument patient_id causes cross site scripting. The attack can be initiated remotely. The exploit has been published and may be used.		
CVE-2026-2154	A vulnerability was identified in SourceCodester/Patrick Mvuma Patients Waiting Area Queue Management System 1.0.	A vulnerability was identified in SourceCodester/Patrick Mvuma Patients Waiting Area Queue Management System 1.0. Impacted is an unknown function of the file /registration.php of the component Patient Registration Module. The manipulation of the argument First Name leads to cross site scripting. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2026-2156	A weakness has been identified in code-projects Online Student Management System 1.0.	A weakness has been identified in code-projects Online Student Management System 1.0. The impacted element is an unknown function of the file /admin/announcement/index.php?view=add of the component Announcement Management Module. This manipulation causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-2159	A flaw has been found in SourceCodester Simple Responsive Tourism Website 1.0.	A flaw has been found in SourceCodester Simple Responsive Tourism Website 1.0. Affected is an unknown function of the file /tourism/classes/Master.php?f=register of the component Registration. Executing a manipulation of the argument firstname/lastname/username can lead to cross site scripting. It is possible to launch the attack remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-2160	A vulnerability has been found in SourceCodester Simple Responsive Tourism Website 1.0.	A vulnerability has been found in SourceCodester Simple Responsive Tourism Website 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 /tourism/classes/Master.php?f=save_package. The manipulation of the argument Title leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2026-2200	A weakness has been identified in heyewei JFinalCMS 5.0.0.	A weakness has been identified in heyewei JFinalCMS 5.0.0. This affects an unknown function of the file /admin/admin/save of the component API Endpoint. Executing a manipulation can lead to cross site scripting. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-2214	A weakness has been identified in code-projects for Plugin 1.0.	A weakness has been identified in code-projects for Plugin 1.0. This affects an unknown part of the file /Administrator/PHP/AdminAddAlbum.php. This manipulation of the argument txtalbum causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-2222	A weakness has been identified in code-projects Online Reviewer System 1.0.	A weakness has been identified in code-projects Online Reviewer System 1.0. Affected by this vulnerability is an unknown functionality of the file /system/system/admins/manage/users/btn_functions.php. Executing a manipulation of the argument firstname can lead to cross site scripting. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-2224	A vulnerability was detected in code-projects Online Reviewer System 1.0.	A vulnerability was detected in code-projects Online Reviewer System 1.0. This affects an unknown part of the file /system/system/admins/manage/users/btn_functions.php. The manipulation of the argument firstname results in cross site scripting. It is possible to launch the attack	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remotely. The exploit is now public and may be used.		
CVE-2026-23476	FacturaScripts is open-source enterprise resource planning and accounting software.	FacturaScripts is open-source enterprise resource planning and accounting software. Prior to 2025.8, there a reflected XSS bug in FacturaScripts. The problem is in how error messages get displayed. Twig's | raw filter is used, which skips HTML escaping. When triggering a database error (like passing a string where an integer is expected), the error message includes the input and gets rendered without sanitization. This vulnerability is fixed in 2025.8.	Patched by core rule	Y
CVE-2026-23997	FacturaScripts is open-source enterprise resource planning and accounting software.	FacturaScripts is open-source enterprise resource planning and accounting software. In 2025.71 and earlier, a Stored Cross-Site Scripting (XSS) vulnerability was discovered in the Observations field. The flaw occurs in the History view, where historical data is rendered without proper HTML entity encoding. This allows an attacker to execute arbitrary JavaScript in the browser of viewing the history by administrators.	Patched by core rule	Y
CVE-2026-24045	Docmost is open-source collaborative wiki and documentation software.	Docmost is open-source collaborative wiki and documentation software. From g and before 0.25.0, the public share page functionality in Docmost does not properly HTML-escape page titles before inserting them into meta tags and the title tag. This allows Stored Cross-Site Scripting (XSS) attacks, where an attacker can execute arbitrary JavaScript in the context of any user who opens a shared page link. This vulnerability is fixed in 0.25.0.	Patched by core rule	Y
CVE-2026-24476	Shaarli is a personal bookmarking service.	Shaarli is a personal bookmarking service. Prior to version 0.16.0, crafting a malicious tag which starting with `"` prematurely ends the `<input>` tag on the start page and allows an attacker to add arbitrary html leading to a possible XSS attack. Version 0.16.0 fixes the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		issue.		
CVE-2026-24490	MobSF is a mobile application security testing tool used.	MobSF is a mobile application security testing tool used. Prior to version 4.4.5, a Stored Cross-site Scripting (XSS) vulnerability in MobSF's Android manifest analysis allows an attacker to execute arbitrary JavaScript in the context of a victim's browser session by uploading a malicious APK. The \`android:host\` attribute from \`<data android:scheme="android_secret_code">\` elements is rendered in HTML reports without sanitization, enabling session hijacking and account takeover. Version 4.4.5 fixes the issue.	Patched by core rule	Y
CVE-2026-24665	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system.	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system. Prior to version 4.2, a stored Cross-Site Scripting (XSS) vulnerability allows authenticated students to inject malicious JavaScript into uploaded assignment files, which is executed when instructors view the submission. This issue has been patched in version 4.2.	Patched by core rule	Y
CVE-2026-24671	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system.	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system. Prior to version 4.2, a Stored Cross-Site Scripting (XSS) vulnerability allows authenticated high-privileged users (teachers or administrators) to inject malicious JavaScript into multiple user-controllable input fields across the application, which is executed when other users access affected pages. This issue has been patched in version 4.2.	Patched by core rule	Y
CVE-2026-24672	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system.	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system. Prior to version 4.2, a Stored Cross-Site Scripting (XSS) vulnerability allows authenticated students to inject malicious JavaScript into user profile fields, which is executed when users with viewing privileges access	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		affected application pages. This issue has been patched in version 4.2.		
CVE-2026-24674	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system.	The Open eClass platform (formerly known as GUnet eClass) is a complete course management system. Prior to version 4.2, a Reflected Cross-Site Scripting (XSS) vulnerability allows remote attackers to execute arbitrary JavaScript in the context of authenticated users by crafting malicious URLs and tricking victims into visiting them. This issue has been patched in version 4.2.	Patched by core rule	Y
CVE-2026-24743	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments.	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. A Stored Cross-Site Scripting (XSS) vulnerability occurs in the upload Invoice Logo functions of InvoicePlane version 1.7.0. The Upload Invoice Logo function allows the application to upload svg files. Although administrator privileges are required to exploit it, this is still considered a critical vulnerability as it can cause actions such as unauthorized modification of application data, creation of persistent backdoors through stored malicious scripts, and full compromise of the application's integrity. Version 1.7.1 patches the issue.	Patched by core rule	Y
CVE-2026-24744	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments.	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. A Stored Cross-Site Scripting (XSS) vulnerability occurs in the Edit Invoices functions of InvoicePlane version 1.7.0. When editing invoices, the application does not validate user input at the \`invoice_number\` parameter. Although administrator privileges are required to exploit it, this is still considered a critical vulnerability as it can cause actions such as unauthorized modification of application data, creation of persistent backdoors through stored malicious scripts, and full compromise of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		application's integrity. Version 1.7.1 patches the issue.		
CVE-2026-24745	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments.	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. A Stored Cross-Site Scripting (XSS) vulnerability occurs in the upload Login Logo functions of InvoicePlane version 1.7.0. In the Upload Login Logo, the application allows uploading svg files. Although administrator privileges are required to exploit it, this is still considered a critical vulnerability as it can cause actions such as unauthorized modification of application data, creation of persistent backdoors through stored malicious scripts, and full compromise of the application's integrity. Version 1.7.1 patches the issue.	Patched by core rule	Y
CVE-2026-24746	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments.	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. A Stored Cross-Site Scripting (XSS) vulnerability occurs in the Edit Quotes functions of InvoicePlane version 1.7.0. In the Editing Quotes function, the application does not validate user input at the quote_number parameter. Although administrator privileges are required to exploit it, this is still considered a critical vulnerability as it can cause actions such as unauthorized modification of application data, creation of persistent backdoors through stored malicious scripts, and full compromise of the application's integrity. Version 1.7.1 patches the issue.	Patched by core rule	Y
CVE-2026-24769	NocoDB is software for building databases as spreadsheets.	NocoDB is software for building databases as spreadsheets. Prior to version 0.301.0, a stored cross-site scripting (XSS) vulnerability exists in NocoDB,Äôs attachment handling mechanism. Authenticated users can upload malicious SVG files containing embedded JavaScript, which are later rendered inline and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		executed in the browsers of other users who view the attachment. Because the malicious payload is stored server-side and executed under the application,Äôs origin, successful exploitation can lead to account compromise, data exfiltration and unauthorized actions performed on behalf of affected users. Version 0.301.0 patches the issue.		
CVE-2026-24855	ChurchCRM is an open-source church management system.	ChurchCRM is an open-source church management system. Versions prior to 6.7.2 have a Stored Cross-Site Scripting (XSS) vulnerability occurs in Create Events in Church Calendar. Users with low privileges can create XSS payloads in the Description field. This payload is stored in the database, and when other users view that event (including the admin), the payload is triggered, leading to account takeover. Version 6.7.2 fixes the vulnerability.	Patched by core rule	Y
CVE-2026-24903	OrcaStatLLM Researcher is an LLM Based Research Paper Generator.	OrcaStatLLM Researcher is an LLM Based Research Paper Generator. A Stored Cross-Site Scripting (XSS) vulnerability was discovered in the Log Message in the Session Page in OrcaStatLLM-Researcher that allows attackers to inject and execute arbitrary JavaScript code in victims' browsers through malicious research topic inputs.	Patched by core rule	Y
CVE-2026-25154	LocalSend is a free, open-source app that allows users to share files and messages with nearby devices over their local network without needing an internet connection.	LocalSend is a free, open-source app that allows users to share files and messages with nearby devices over their local network without needing an internet connection. In versions up to and including 1.17.0, when a user initiates a "Share via Link" session, the LocalSend application starts a local HTTP server to host the selected files. The client-side logic for this web interface is contained in \`app/assets/web/main.js\`. Note that at [0], the \`handleFilesDisplay\` function constructs the HTML for the file list by iterating over the files received from the server. Commit	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		8f3cec85aa29b2b13fed9b2f8e499e1ac9b0504c contains a patch.		
CVE-2026-25230	FileRise is a self-hosted web file manager / WebDAV server.	FileRise is a self-hosted web file manager / WebDAV server. Prior to 3.3.0, an HTML Injection vulnerability allows an authenticated user to modify the DOM and add e.g. form elements that call certain endpoints or link elements that redirect the user on active interaction. This vulnerability is fixed in 3.3.0.	Patched by core rule	Y
CVE-2026-2545	A weakness has been identified in LigeroSmart up to 6.1.26.	A weakness has been identified in LigeroSmart up to 6.1.26. Impacted is an unknown function of the file /otrs/index.pl?Action=AgentTicketSearch. This manipulation of the argument Profile causes cross site scripting. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	Patched by core rule	Y
CVE-2026-2546	A security vulnerability has been detected in LigeroSmart up to 6.1.26.	A security vulnerability has been detected in LigeroSmart up to 6.1.26. The affected element is an unknown function of the file /otrs/index.pl. Such manipulation of the argument SortBy leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	Patched by core rule	Y
CVE-2026-2547	A vulnerability was detected in LigeroSmart up to 6.1.26.	A vulnerability was detected in LigeroSmart up to 6.1.26. The impacted element is the function AgentDashboard of the file /otrs/index.pl. Performing a manipulation of the argument Subaction results in cross site scripting. Remote exploitation of the attack is possible. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-25482	Craft Commerce is an ecommerce platform for Craft CMS.	Craft Commerce is an ecommerce platform for Craft CMS. In versions from 4.0.0-RC1 to 4.10.0 and from 5.0.0 to 5.5.1, a stored DOM XSS vulnerability exists in the "Recent Orders" dashboard widget. The Order Status Name is rendered via JavaScript string concatenation without proper escaping, allowing script execution when any admin visits the dashboard. This issue has been patched in versions 4.10.1 and 5.5.2.	Patched by core rule	Y
CVE-2026-25483	Craft Commerce is an ecommerce platform for Craft CMS.	Craft Commerce is an ecommerce platform for Craft CMS. In versions from 4.0.0-RC1 to 4.10.0 and from 5.0.0 to 5.5.1, a stored XSS vulnerability exists in Craft Commerce,Äôs Order Status History Message. The message is rendered using the |md filter, which permits raw HTML, enabling malicious script execution. If a user has database backup utility permissions (which do not require an elevated session), an attacker can exfiltrate the entire database, including all user credentials, customer PII, order history, and 2FA recovery codes. This issue has been patched in versions 4.10.1 and 5.5.2.	Patched by core rule	Y
CVE-2026-25484	Craft Commerce is an ecommerce platform for Craft CMS.	Craft Commerce is an ecommerce platform for Craft CMS. In versions from 4.0.0-RC1 to 4.10.0 and from 5.0.0 to 5.5.1, there is a Stored XSS via Product Type names. The name is not sanitized when displayed in user permissions settings. The vulnerable input (source) is in Commerce (Product Type settings), but the sink is in CMS user permissions settings. This issue has been patched in versions 4.10.1 and 5.5.2.	Patched by core rule	Y
CVE-2026-25485	Craft Commerce is an ecommerce platform for Craft CMS.	Craft Commerce is an ecommerce platform for Craft CMS. In versions from 4.0.0-RC1 to 4.10.0 and from 5.0.0 to 5.5.1, a stored XSS vulnerability in Craft Commerce allows attackers to execute malicious JavaScript in an administrator,Äôs browser.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		This occurs because the Shipping Categories (Name & Description) fields in the Store Management section are not properly sanitized before being displayed in the admin panel. This issue has been patched in versions 4.10.1 and 5.5.2.		
CVE-2026-25486	Craft Commerce is an ecommerce platform for Craft CMS.	Craft Commerce is an ecommerce platform for Craft CMS. From version 5.0.0 to 5.5.1, a stored XSS vulnerability in Craft Commerce allows attackers to execute malicious JavaScript in an administrator‚Äôs browser. This occurs because the Shipping Methods Name field in the Store Management section is not properly sanitized before being displayed in the admin panel. This issue has been patched in version 5.5.2.	Patched by core rule	Y
CVE-2026-25487	Craft Commerce is an ecommerce platform for Craft CMS.	Craft Commerce is an ecommerce platform for Craft CMS. In versions from 4.0.0-RC1 to 4.10.0 and from 5.0.0 to 5.5.1, a stored XSS vulnerability in Craft Commerce allows attackers to execute malicious JavaScript in an administrator's browser. This occurs because the Tax Rates 'Name' field in the Store Management section is not properly sanitized before being displayed in the admin panel. This issue has been patched in versions 4.10.1 and 5.5.2.	Patched by core rule	Y
CVE-2026-25488	Craft Commerce is an ecommerce platform for Craft CMS.	Craft Commerce is an ecommerce platform for Craft CMS. In versions from 4.0.0-RC1 to 4.10.0 and from 5.0.0 to 5.5.1, a stored XSS vulnerability in Craft Commerce allows attackers to execute malicious JavaScript in an administrator‚Äôs browser. This occurs because the Tax Categories (Name & Description) fields in the Store Management section are not properly sanitized before being displayed in the admin panel. This issue has been patched in versions 4.10.1 and 5.5.2.	Patched by core rule	Y
CVE-2026-25489	Craft Commerce is an ecommerce platform for	Craft Commerce is an ecommerce platform for	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Craft CMS.	Craft CMS. In versions from 4.0.0-RC1 to 4.10.0 and from 5.0.0 to 5.5.1, a stored XSS vulnerability in Craft Commerce allows attackers to execute malicious JavaScript in an administrator‚Äôs browser. This occurs because the Name & Description fields in Tax Zones are not properly sanitized before being displayed in the admin panel. This issue has been patched in versions 4.10.1 and 5.5.2.		
CVE-2026-25490	Craft Commerce is an ecommerce platform for Craft CMS.	Craft Commerce is an ecommerce platform for Craft CMS. In versions from 4.0.0-RC1 to 4.10.0 and from 5.0.0 to 5.5.1, a stored XSS vulnerability in Craft Commerce allows attackers to execute malicious JavaScript in an administrator‚Äôs browser. This occurs because the 'Address Line 1' field in Inventory Locations is not properly sanitized before being displayed in the admin panel. This issue has been patched in versions 4.10.1 and 5.5.2.	Patched by core rule	Y
CVE-2026-25491	Craft is a platform for creating digital experiences.	Craft is a platform for creating digital experiences. From 5.0.0-RC1 to 5.8.21, Craft has a stored XSS via Entry Type names. The name is not sanitized when displayed in the Entry Types list. This vulnerability is fixed in 5.8.22.	Patched by core rule	Y
CVE-2026-25496	Craft is a platform for creating digital experiences.	Craft is a platform for creating digital experiences. In Craft versions 4.0.0-RC1 through 4.16.17 and 5.0.0-RC1 through 5.8.21, a stored XSS vulnerability exists in the Number field type settings. The Prefix and Suffix fields are rendered using the |md|raw Twig filter without proper escaping, allowing script execution when the Number field is displayed on users' profiles. This issue is patched in versions 4.16.18 and 5.8.22.	Patched by core rule	Y
CVE-2026-25500	Rack is a modular Ruby web server interface.	Rack is a modular Ruby web server interface. Prior to versions 2.2.22, 3.1.20, and 3.2.5, `Rack::Directory` generates an HTML directory index where each file entry	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		is rendered as a clickable link. If a file exists on disk whose basename starts with the `javascript:` scheme (e.g. `javascript:alert(1)`), the generated index contains an anchor whose `href` is exactly `javascript:alert(1)`. Clicking the entry executes JavaScript in the browser (demonstrated with `alert(1)`). Versions 2.2.22, 3.1.20, and 3.2.5 fix the issue.		
CVE-2026-25516	NiceGUI is a Python-based UI framework.	NiceGUI is a Python-based UI framework. The ui.markdown() component uses the markdown2 library to convert markdown content to HTML, which is then rendered via innerHTML. By default, markdown2 allows raw HTML to pass through unchanged. This means that if an application renders user-controlled content through ui.markdown(), an attacker can inject malicious HTML containing JavaScript event handlers. Unlike other NiceGUI components that render HTML (ui.html(), ui.chat_message(), ui.interactive_image()), the ui.markdown() component does not provide or require a sanitize parameter, leaving applications vulnerable to XSS attacks. This vulnerability is fixed in 3.7.0.	Patched by core rule	Y
CVE-2026-25522	Craft Commerce is an ecommerce platform for Craft CMS.	Craft Commerce is an ecommerce platform for Craft CMS. In versions from 4.0.0-RC1 to 4.10.0 and from 5.0.0 to 5.5.1, a stored XSS vulnerability in Craft Commerce allows attackers to execute malicious JavaScript in an administrator‚Äôs browser. This occurs because the Shipping Zone (Name & Description) fields in the Store Management section are not properly sanitized before being displayed in the admin panel. This issue has been patched in versions 4.10.1 and 5.5.2.	Patched by core rule	Y
CVE-2026-2557	A vulnerability was detected in cskefu up to 8.0.1.	A vulnerability was detected in cskefu up to 8.0.1. Impacted is the function Upload of the file com/cskefu/cc/controller/resource/MediaController.java	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		of the component File Upload. The manipulation results in cross site scripting. The attack may be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2026-25578	Navidrome is an open source web-based music collection server and streamer.	Navidrome is an open source web-based music collection server and streamer. Prior to version 0.60.0, a cross-site scripting vulnerability in the frontend allows a malicious attacker to inject code through the comment metadata of a song to exfiltrate user credentials. This issue has been patched in version 0.60.0.	Patched by core rule	Y
CVE-2026-25581	SCEditor is a lightweight WYSIWYG BBCode and XHTML editor.	SCEditor is a lightweight WYSIWYG BBCode and XHTML editor. Prior to 3.2.1, if an attacker has the ability control configuration options passed to sceditor.create(), like emoticons, charset, etc. then it's possible for them to trigger an XSS attack due to lack of sanitisation of configuration options. This vulnerability is fixed in 3.2.1.	Patched by core rule	Y
CVE-2026-25594	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments.	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. A Stored Cross-Site Scripting (XSS) vulnerability exists in InvoicePlane 1.7.0 via the Family Name field. The \`family_name\` value is rendered without HTML encoding inside the family dropdown on the product form. When an administrator creates a family with a malicious name, the payload executes in the browser of any administrator who visits the product form. Version 1.7.1 patches the issue.	Patched by core rule	Y
CVE-2026-25595	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments.	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. A Stored Cross-Site Scripting (XSS) vulnerability exists in InvoicePlane 1.7.0 via the Invoice Number field. An authenticated administrator can inject malicious JavaScript that executes	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		when any administrator views the affected invoice or visits the dashboard. Version 1.7.1 patches the issue.		
CVE-2026-25596	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments.	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. A Stored Cross-Site Scripting (XSS) vulnerability exists in InvoicePlane 1.7.0 via the Product Unit Name fields. An authenticated administrator can inject malicious JavaScript that executes when any administrator views an invoice containing a product with the malicious unit. Version 1.7.1 patches the issue.	Patched by core rule	Y
CVE-2026-25647	Lute is a structured Markdown engine supporting Go and JavaScript.	Lute is a structured Markdown engine supporting Go and JavaScript. Lute 1.7.6 and earlier (as used in SiYuan before) has a Stored Cross-Site Scripting (XSS) vulnerability in the Markdown rendering engine. An attacker can inject malicious JavaScript into a Markdown text/note. When another user clicks the rendered content, the script executes in the context of their session.	Patched by core rule	Y
CVE-2026-25648	Versions of the Traccar open-source GPS tracking system starting with 6.11.1 contain an issue in which authenticated users can execute arbitrary JavaScript in the context of other users' browsers by uploading malicious SVG files as device images.	Versions of the Traccar open-source GPS tracking system starting with 6.11.1 contain an issue in which authenticated users can execute arbitrary JavaScript in the context of other users' browsers by uploading malicious SVG files as device images. The application accepts SVG file uploads without sanitization and serves them with the `image/svg+xml` Content-Type, allowing embedded JavaScript to execute when victims view the image. As of time of publication, it is unclear whether a fix is available.	Patched by core rule	Y
CVE-2026-25802	New API is a large language mode (LLM) gateway and artificial intelligence (AI) asset management system.	New API is a large language mode (LLM) gateway and artificial intelligence (AI) asset management system. Prior to version 0.10.8-alpha.9, a potential unsafe operation occurs in component `MarkdownRenderer.jsx`,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		allowing for Cross-Site Scripting(XSS) when the model outputs items containing `<script>` tag. Version 0.10.8-alpha.9 fixes the issue.		
CVE-2026-26023	Dify is an open-source LLM app development platform.	Dify is an open-source LLM app development platform. Prior to 1.13.0, a cross site scripting vulnerability has been found in the web application chat frontend when using echarts. User or llm inputs containing echarts containing a specific javascript payload will be executed. This vulnerability is fixed in 1.13.0.	Patched by core rule	Y
CVE-2026-26059	ChurchCRM is an open-source church management system.	ChurchCRM is an open-source church management system. In versions prior to 6.8.2, it was possible for an authenticated user with permission to edit groups to store a JavaScript payload that would execute when the group was viewed in the Group View. Version 6.8.2 fixes this issue.	Patched by core rule	Y
CVE-2026-26188	Solspace Freeform plugin for Craft CMS 5.x is a super flexible form-building tool.	Solspace Freeform plugin for Craft CMS 5.x is a super flexible form-building tool. An authenticated, low-privilege user (able to create/edit forms) can inject arbitrary HTML/JS into the Craft Control Panel (CP) builder and integrations views. User-controlled form labels and integration metadata are rendered with dangerouslySetInnerHTML without sanitization, leading to stored XSS that executes when any admin views the builder/integration screens. This vulnerability is fixed in 5.14.7.	Patched by core rule	Y
CVE-2026-26192	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline.	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to version 0.7.0, aanually modifying chat history allows setting the `html` property within document metadata. This causes the frontend to enter a code path that treats document contents as HTML, and render them in an iFrame when the citation is previewed. This allows stored XSS via a weaponized document payload in a chat.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The payload also executes when the citation is viewed on a shared chat. Version 0.7.0 fixes the issue.		
CVE-2026-26193	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline.	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to version 0.6.44, aanually modifying chat history allows setting the `embeds` property on a response message, the content of which is loaded into an iFrame with a sandbox that has `allow-scripts` and `allow-same-origin` set, ignoring the "iframe Sandbox Allow Same Origin" configuration. This enables stored XSS on the affected chat. This also triggers when the chat is in the shared format. The result is a shareable link containing the payload that can be distributed to any other users on the instance. Version 0.6.44 fixes the issue.	Patched by core rule	Y
CVE-2026-2622	A vulnerability was detected in Blossom up to 1.17.1.	A vulnerability was detected in Blossom up to 1.17.1. This vulnerability affects the function content of the file blossom-backend/backend/src/main/java/com/blossom/backend/server/article/draft/ArticleController.java of the component Article Title Handler. The manipulation results in cross site scripting. The attack can be launched remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-26281	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments.	InvoicePlane is a self-hosted open source application for managing invoices, clients, and payments. A stored cross-site scripting (XSS) vulnerability in the Sumex invoice view allows an authenticated user with client and invoice management privileges to execute arbitrary JavaScript in the browser of any user viewing the invoice. This can lead to session hijacking, data theft, or other malicious actions on behalf of the victim user. Version 1.7.1 patches the issue.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-26464	Stored Cross-Site Scripting (XSS) was found in the /admin/edit_user.php page of Society Management System Portal V1.0, which allows remote attackers to inject and store arbitrary JavaScript code that is executed in users' browsers.	Stored Cross-Site Scripting (XSS) was found in the /admin/edit_user.php page of Society Management System Portal V1.0, which allows remote attackers to inject and store arbitrary JavaScript code that is executed in users' browsers. This vulnerability can be exploited via the name parameter in a POST HTTP request, leading to execution of malicious scripts when the affected content is viewed by other users, including administrators.	Patched by core rule	Y
CVE-2026-26723	Cross Site Scripting vulnerability in Key Systems Inc Global Facilities Management Software v.	Cross Site Scripting vulnerability in Key Systems Inc Global Facilities Management Software v. 20230721a allows a remote attacker to execute arbitrary code via the function parameter.	Patched by core rule	Y
CVE-2026-26724	Cross Site Scripting vulnerability in Key Systems Inc Global Facilities Management Software v.	Cross Site Scripting vulnerability in Key Systems Inc Global Facilities Management Software v. 20230721a allows a remote attacker to execute arbitrary code via the selectgroup and gn parameters on the /?Function=Groups endpoint.	Patched by core rule	Y
CVE-2026-26987	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool.	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool. Versions 25.12.0 and below are vulnerable to Reflected XSS attacks via email field. This issue has been fixed in version 26.2.0.	Patched by core rule	Y
CVE-2026-26989	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool.	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool. Versions 25.12.0 and below are affected by a Stored Cross-Site Scripting (XSS) vulnerability in the Alert Rules workflow. An attacker with administrative privileges can inject malicious scripts that execute in the browser context of any user who accesses the Alert Rules page. This issue has been fixed in version 26.2.0.	Patched by core rule	Y
CVE-2026-26991	LibreNMS is an auto-discovering	LibreNMS is an auto-discovering	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	PHP/MySQL/SNMP based network monitoring tool.	PHP/MySQL/SNMP based network monitoring tool. In versions 26.1.1 and below, the device group name is not sanitized, allowing attackers with admin privileges to perform Stored Cross-Site Scripting (XSS) attacks. When a user adds a device group, an HTTP POST request is sent to the Request-URI "/device-groups". The name of the newly created device group is stored in the value of the name parameter. After the device group is created, the entry is displayed along with relevant buttons such as Rediscover Devices, Edit, and Delete. This issue has been fixed in version 26.2.0.		
CVE-2026-26992	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool.	LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool. In versions 26.1.1 and below, the port group name is not sanitized, allowing attackers with admin privileges to perform Stored Cross-Site Scripting (XSS) attacks. When a user adds a port group, an HTTP POST request is sent to the Request-URI "/port-groups". The name of the newly created port group is stored in the value of the name parameter. After the port group is created, the entry is displayed along with relevant buttons such as Edit and Delete. This issue has been fixed in version 26.2.0.	Patched by core rule	Y
CVE-2026-27009	OpenClaw is a personal AI assistant.	OpenClaw is a personal AI assistant. Prior to version 2026.2.15, a atored XSS issue in the OpenClaw Control UI when rendering assistant identity (name/avatar) into an inline `<script>` tag without script-context-safe escaping. A crafted value containing `</script>` could break out of the script tag and execute attacker-controlled JavaScript in the Control UI origin. Version 2026.2.15 removed inline script injection and serve bootstrap config from a JSON endpoint and added a restrictive Content Security Policy for the Control UI	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		(`script-src 'self'`, no inline scripts).		
CVE-2026-27013	Fabric.js is a Javascript HTML5 canvas library.	Fabric.js is a Javascript HTML5 canvas library. Prior to version 7.2.0, Fabric.js applies `escapeXml()` to text content during SVG export (`src/shapes/Text/TextSVGExportMixin.ts:186`) but fails to apply it to other user-controlled string values that are interpolated into SVG attribute markup. When attacker-controlled JSON is loaded via `loadFromJSON()` and later exported via `toSVG()`, the unescaped values break out of XML attributes and inject arbitrary SVG elements including event handlers. Any application that accepts user-supplied JSON (via `loadFromJSON()`, collaborative sharing, import features, CMS plugins) and renders the `toSVG()` output in a browser context (SVG preview, export download rendered in-page, email template, embed) is vulnerable to stored XSS. An attacker can execute arbitrary JavaScript in the victim's browser session. Version 7.2.0 contains a fix.	Patched by core rule	Y
CVE-2026-27147	GetSimple CMS is a content management system.	GetSimple CMS is a content management system. All versions of GetSimple CMS are vulnerable to XSS through SVG file uploads. Authenticated users can upload SVG files via the administrative upload functionality, but they are not properly sanitized or restricted, allowing an attacker to embed malicious JavaScript. When the uploaded SVG file is accessed, the script executes in the browser. This issue does not have a fix at the time of publication.	Patched by core rule	Y
CVE-2026-27176	MajorDoMo (aka Major Domestic Module) contains a reflected cross-site scripting (XSS) vulnerability in command.php.	MajorDoMo (aka Major Domestic Module) contains a reflected cross-site scripting (XSS) vulnerability in command.php. The $qry parameter is rendered directly into the HTML page without sanitization via htmlspecialchars(), both in an input field value attribute and in a paragraph element. An attacker can inject	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		arbitrary JavaScript by crafting a URL with malicious content in the qry parameter.		
CVE-2026-27177	MajorDoMo (aka Major Domestic Module) contains a stored cross-site scripting (XSS) vulnerability via the /objects/?op=set endpoint, which is intentionally unauthenticated for IoT device integration.	MajorDoMo (aka Major Domestic Module) contains a stored cross-site scripting (XSS) vulnerability via the /objects/?op=set endpoint, which is intentionally unauthenticated for IoT device integration. User-supplied property values are stored raw in the database without sanitization. When an administrator views the property editor in the admin panel, the stored values are rendered without escaping in both a paragraph tag (SOURCE field) and a textarea element (VALUE field). The XSS fires on page load without requiring any click from the admin. Additionally, the session cookie lacks the HttpOnly flag, enabling session hijack via document.cookie exfiltration. An attacker can enumerate properties via the unauthenticated /api.php/data/ endpoint and poison any property with malicious JavaScript.	Patched by core rule	Y
CVE-2026-27178	MajorDoMo (aka Major Domestic Module) contains a stored cross-site scripting (XSS) vulnerability through method parameter injection into the shoutbox.	MajorDoMo (aka Major Domestic Module) contains a stored cross-site scripting (XSS) vulnerability through method parameter injection into the shoutbox. The /objects/?method= endpoint allows unauthenticated execution of stored methods with attacker-controlled parameters. Default methods such as ThisComputer.VolumeLevelChanged pass the user-supplied VALUE parameter directly into the say() function, which stores the message raw in the shouts database table without escaping. The shoutbox widget renders stored messages without sanitization in both PHP rendering code and HTML templates. Because the dashboard widget auto-refreshes every 3 seconds, the injected script executes automatically when any administrator loads the dashboard, enabling session	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		hijack through cookie exfiltration.		
CVE-2026-27612	Repostat is a React component to fetch and display GitHub repository info.	Repostat is a React component to fetch and display GitHub repository info. Prior to version 1.0.1, the `RepoCard` component is vulnerable to Reflected Cross-Site Scripting (XSS). The vulnerability occurs because the component uses React's `dangerouslySetInnerHTML` to render the repository name (`repo` prop) during the loading state without any sanitization. If a developer using this package passes unvalidated user input directly into the `repo` prop (for example, reading it from a URL query parameter), an attacker can execute arbitrary JavaScript in the context of the user's browser. In version 1.0.1, the use of dangerouslySetInnerHTML has been removed, and the repo prop is now safely rendered using standard React JSX data binding, which automatically escapes HTML entities.	Patched by core rule	Y
CVE-2026-27614	Bugsink is a self-hosted error tracking tool.	Bugsink is a self-hosted error tracking tool. In versions prior to 2.0.13, an unauthenticated attacker who can submit events to a Bugsink project can store arbitrary JavaScript in an event. The payload executes only if a user explicitly views the affected Stacktrace in the web UI. When Pygments returns more lines than it was given (a known upstream quirk that triggers with Ruby heredoc-style input), `_pygmentize_lines()` in `theme/templatetags/issues.py:75-77` falls back to returning the raw input lines. `mark_safe()` at line 111-113 is then applied unconditionally - including to those unsanitized raw lines. Since DSN endpoints are public by Sentry protocol, no account is needed to inject. The payload sits in the database until an admin looks at the event. Successful exploitation requires that the attacker to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		be able to submit events to the project (i.e. knows the DSN or can access a client that uses it), the Bugsink ingest endpoint is reachable to the attacker, and an administrator explicitly views the crafted event in the UI. Under those conditions, the attacker can execute JavaScript in the administrator‚Äôs browser and act with that user‚Äôs privileges within Bugsink. Version 2.0.13 fixes the vulnerability.		
CVE-2026-27621	TypiCMS is a multilingual content management system based on the Laravel framework.	TypiCMS is a multilingual content management system based on the Laravel framework. A Stored Cross-Site Scripting (XSS) vulnerability exists in the file upload module of TypiCMS prior to version 16.1.7. The application allows users with file upload permissions to upload SVG files. While there is a MIME type validation, the content of the SVG file is not sanitized. An attacker can upload a specially crafted SVG file containing malicious JavaScript code. When another user (such as an administrator) views or accesses this file through the application, the script executes in their browser, leading to a compromise of that user's session. The issue is exacerbated by a bug in the SVG parsing logic, which can cause a 500 error if the uploaded SVG does not contain a `viewBox` attribute. However, this does not mitigate the XSS vulnerability, as an attacker can easily include a valid `viewBox` attribute in their malicious payload. Version 16.1.7 of TypiCMS Core fixes the issue.	Patched by core rule	Y
CVE-2026-27627	Karakeep is a elf-hostable bookmark-everything app.	Karakeep is a elf-hostable bookmark-everything app. In version 0.30.0, when the Reddit metascraper plugin returns `readableContentHtml`, the HTML parsing subprocess uses it directly without running it through DOMPurify. Every other content source in the crawler goes through	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Readability + DOMPurify, but the Reddit path skips both. Since this content ends up in `dangerouslySetInnerHTML` in the reader view, any malicious HTML in the Reddit response gets executed in the user's browser. Version 0.31.0 contains a patch for this issue.		
CVE-2026-27645	changedetection.io is a free open source web page change detection tool.	changedetection.io is a free open source web page change detection tool. In versions prior to 0.54.1, the RSS single-watch endpoint reflects the UUID path parameter directly in the HTTP response body without HTML escaping. Since Flask returns text/html by default for plain string responses, the browser parses and executes injected JavaScript. Version 0.54.1 contains a fix for the issue.	Patched by core rule	Y
CVE-2026-27742	Bludit version 3.16.2 contains a stored cross-site scripting (XSS) vulnerability in the post content functionality.	Bludit version 3.16.2 contains a stored cross-site scripting (XSS) vulnerability in the post content functionality. The application performs client-side sanitation of content input but does not enforce equivalent sanitation on the server side. An authenticated user can inject arbitrary JavaScript into the content field of a post, which is stored and later rendered to other users without proper output encoding. When viewed, the injected script executes in the context of the victim‚Äôs browser, allowing session hijacking, credential theft, content manipulation, or other actions within the user‚Äôs privileges.	Patched by core rule	Y
CVE-2026-27822	RustFS is a distributed object storage system built in Rust.	RustFS is a distributed object storage system built in Rust. Prior to version 1.0.0-alpha.83, a Stored Cross-Site Scripting (XSS) vulnerability in the RustFS Console allows an attacker to execute arbitrary JavaScript in the context of the management console. By bypassing the PDF preview logic, an attacker can steal administrator credentials from `localStorage`, leading to full account takeover and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		system compromise. Version 1.0.0-alpha.83 fixes the issue.		
CVE-2026-2825	A vulnerability has been found in rachelos WeRSS we-mp-rss up to 1.4.8.	A vulnerability has been found in rachelos WeRSS we-mp-rss up to 1.4.8. This impacts the function fix_html of the file tools/fix.py of the component Article Module. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-2897	A security vulnerability has been detected in funadmin up to 7.1.0-rc4.	A security vulnerability has been detected in funadmin up to 7.1.0-rc4. This vulnerability affects unknown code of the file app/backend/view/index/index.html of the component Backend Interface. The manipulation of the argument Value leads to cross site scripting. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-2932	A security flaw has been discovered in YiFang CMS up to 2.0.5.	A security flaw has been discovered in YiFang CMS up to 2.0.5. The impacted element is the function update of the file app/db/admin/D_adPosition.php of the component Extended Management Module. Performing a manipulation of the argument name/index results in cross site scripting. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y
CVE-2026-2933	A weakness has been identified in YiFang CMS up to 2.0.5.	A weakness has been identified in YiFang CMS up to 2.0.5. This affects the function update of the file app/db/admin/D_adManage.php of the component Extended Management Module. Executing a manipulation of the argument Name can lead to cross site scripting. The attack may be performed from remote. The exploit has	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		been made available to the public and could be used for attacks.		
CVE-2026-2934	A security vulnerability has been detected in YiFang CMS up to 2.0.5.	A security vulnerability has been detected in YiFang CMS up to 2.0.5. This impacts the function update of the file app/db/admin/D_friendLinkGroup.php of the component Extended Management Module. The manipulation of the argument Name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-2939	A vulnerability was found in itsourcecode Student Management System 1.0.	A vulnerability was found in itsourcecode Student Management System 1.0. The impacted element is an unknown function of the file /add_student/ of the component Add Student Module. The manipulation results in cross site scripting. It is possible to launch the attack remotely. The exploit has been made public and could be used.	Patched by core rule	Y
CVE-2026-2946	A security vulnerability has been detected in rymcu forest up to 0.0.5.	A security vulnerability has been detected in rymcu forest up to 0.0.5. Affected by this issue is the function XssUtils.replaceHtmlCode of the file src/main/java/com/rymcu/forest/util/XssUtils.java of the component Article Content/Comments/Portfolio. The manipulation leads to cross site scripting. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-2947	A vulnerability was detected in rymcu forest up to 0.0.5.	A vulnerability was detected in rymcu forest up to 0.0.5. This affects the function updateUserInfo of the file - src/main/java/com/rymcu/forest/web/api/user/UserInfoController.java of the component User Profile Handler. The manipulation results in cross site scripting. The attack can be executed remotely. The exploit is now public and may be used. The vendor was contacted early	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		about this disclosure but did not respond in any way.		
CVE-2026-2965	A security flaw has been discovered in 07FLYCMS, 07FLY-CMS and 07FlyCRM up to 1.2.9.	A security flaw has been discovered in 07FLYCMS, 07FLY-CMS and 07FlyCRM up to 1.2.9. The affected element is an unknown function of the file /admin/SysModule/edit.html of the component System Extension Module. Performing a manipulation of the argument Title results in cross site scripting. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. This product is published under multiple names. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-2971	A vulnerability was found in a466350665 Smart-SSO up to 2.1.1.	A vulnerability was found in a466350665 Smart-SSO up to 2.1.1. Affected by this issue is some unknown functionality of the file smart-sso-server/src/main/resources/templates/login.html of the component Login. Performing a manipulation of the argument redirectUri results in cross site scripting. The attack is possible to be carried out remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-2972	A vulnerability was determined in a466350665 Smart-SSO up to 2.1.1.	A vulnerability was determined in a466350665 Smart-SSO up to 2.1.1. This affects the function Save of the file smart-sso-server/src/main/java/openjoe/smart/sso/server/controller/admin/UserController.java of the component Role Edit Page. Executing a manipulation can lead to cross site scripting. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-3027	A vulnerability was found in erzhongxmu JEEWMS up to 3.7.	A vulnerability was found in erzhongxmu JEEWMS up to 3.7. This affects an unknown	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		part of the file src/main/webapp/plug-in/ueditor/jsp/getContent.jsp of the component UEditor. The manipulation of the argument myEditor results in cross site scripting. The attack can be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2026-3028	A vulnerability was determined in erzhongxmu JEEWMS up to 3.7.	A vulnerability was determined in erzhongxmu JEEWMS up to 3.7. This vulnerability affects the function doAdd of the file src/main/java/com/jeecg/demo/controller/JeecgListDemoController.java. This manipulation of the argument Name causes cross site scripting. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	Patched by core rule	Y
CVE-2026-3043	A flaw has been found in itsourcecode Event Management System 1.0.	A flaw has been found in itsourcecode Event Management System 1.0. The impacted element is an unknown function of the file /admin/navbar.php. Executing a manipulation of the argument page can lead to cross site scripting. The attack may be performed from remote. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-3050	A flaw has been found in horilla-opensource horilla up to 1.0.2.	A flaw has been found in horilla-opensource horilla up to 1.0.2. Impacted is an unknown function of the file static/assets/js/global.js of the component Leads Module. This manipulation of the argument Notes causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been published and may be used. Upgrading to version 1.0.3 is recommended to address this issue. Patch name: fc5c8e55988e89273012491b5f097b762b474546. It is suggested to upgrade the affected component.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-3070	A vulnerability was detected in SourceCodester Modern Image Gallery App 1.0.	A vulnerability was detected in SourceCodester Modern Image Gallery App 1.0. Affected by this vulnerability is an unknown functionality of the file upload.php. The manipulation of the argument filename results in cross site scripting. The attack may be launched remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-3170	A vulnerability was detected in SourceCodester/Patrick Mvuma Patients Waiting Area Queue Management System 1.0.	A vulnerability was detected in SourceCodester/Patrick Mvuma Patients Waiting Area Queue Management System 1.0. Affected is an unknown function of the file /patient-search.php. The manipulation of the argument First Name/Last Name results in cross site scripting. The attack can be executed remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-3171	A flaw has been found in SourceCodester/Patrick Mvuma Patients Waiting Area Queue Management System 1.0.	A flaw has been found in SourceCodester/Patrick Mvuma Patients Waiting Area Queue Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /queue.php. This manipulation of the argument firstname/lastname causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been published and may be used.	Patched by core rule	Y

INDUSFACE™

Indusface is a leading application security SaaS company, securing over 6,500 customers across 95 countries with its award-winning platform. Backed by leading institutional investors, Indusface is a category leader in cloud WAAP, with repeated recognition from top analysts and industry platforms including Gartner, Forrester, GigaOm, and G2.

The industry's only AI-powered, all-in-one AppSec platform helps businesses discover, detect, remediate, and protect web applications and APIs at internet scale, backed by a 100% uptime guarantee.

Gartner
Peer Insights
Customers'
Choice 2024™

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

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

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