INDUSFACE™

MONTHLY BULLETIN · APRIL 2026

Zero-Day Vulnerability Coverage Report

Comprehensive AppTrana and Indusface WAS protection coverage across all newly disclosed zero-day vulnerabilities for April 2026.

509	100%	100%
TOTAL ZERO-DAYS	CORE RULE COVERAGE	WAS SCANNER COVERAGE

EXECUTIVE SUMMARY

April 2026 - Vulnerability Coverage Overview

AppTrana protected against 509 newly disclosed zero-day vulnerabilities across nine attack categories. The Indusface WAS scanner and AppTrana's core rules both delivered 100% coverage, with no custom rule patches required.

VULNERABILITY BREAKDOWN

VULNERABILITY CATEGORY	COUNT
Cross-Site Scripting	160
SQL Injection	109
Command Injection	85
SSRF	74
Code Injection	54
Malicious File Upload	9
Advanced Injection Types	9
Path Traversal	8
Remote Code Execution	1

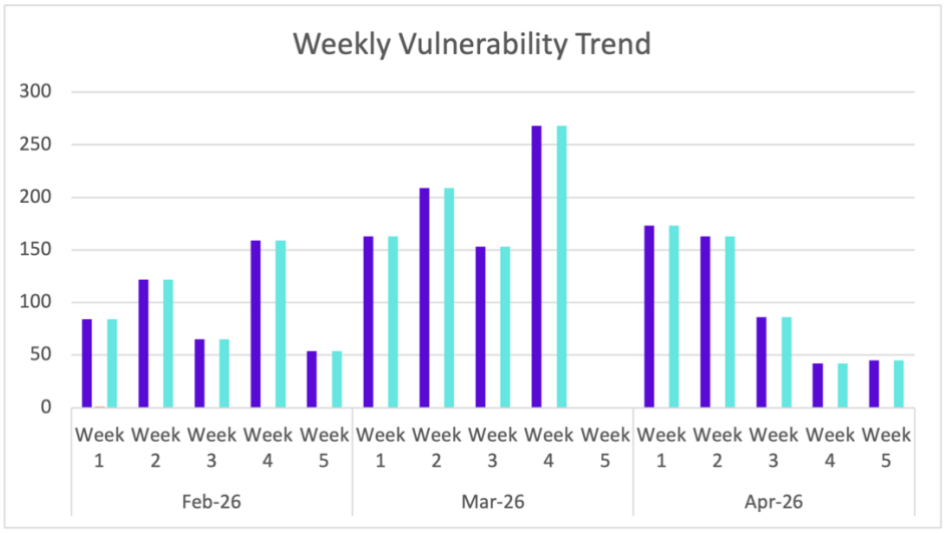
COVERAGE BY THE NUMBERS

COVERAGE METRIC	COUNT
Zero-day vulnerabilities protected through core rules	509
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities found by Indusface WAS	509

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

VULNERABILITY TREND

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



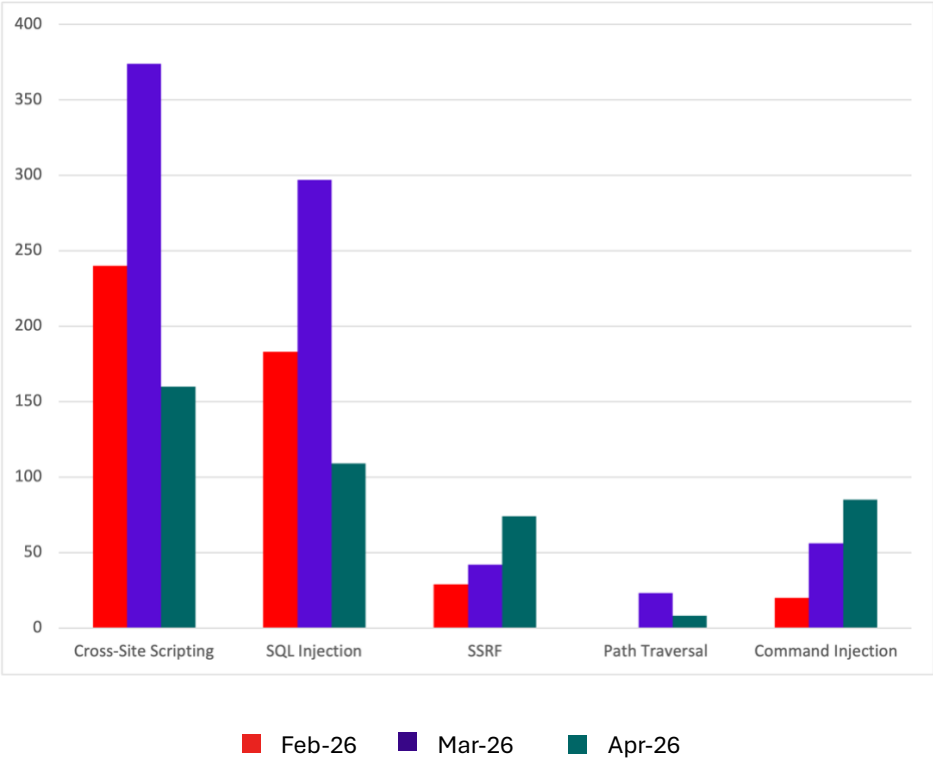
100%

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

100%

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

TOP FIVE VULNERABILITY CATEGORIES



VULNERABILITY DETAILS

Command Injection Vulnerabilities

Command injection vulnerabilities allow attackers to execute arbitrary OS commands by injecting shell metacharacters into unsanitized parameters. All 85 command injection CVEs identified in April 2026 are patched by AppTrana core rules.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-6992	Linksys MR9600 OS Command Injection	A vulnerability was identified in Linksys MR9600 2.0.6.206937. This affects the function BTRequestGetSmartConnectStatus of the file /etc/init.d/run_central2.sh of the component JNAP Action Handler. The manipulation of the argument pin leads to os command injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-33208	ToToLink A3300R Command Injection via interval	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the interval parameter to /cgi-bin/cstecgi.cgi.	Patched by core rule	Y
CVE-2026-41265	ToToLink A3300R Command Injection via week	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the week parameter to /cgi-bin/cstecgi.cgi.	Patched by core rule	Y
CVE-2026-31173	ToToLink A3300R Command Injection via recHour	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the recHour parameter to /cgi-bin/cstecgi.cgi.	Patched by core rule	Y
CVE-2026-31169	ToToLink A3300R Command Injection via mode	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the mode parameter to /cgi-bin/cstecgi.cgi.	Patched by core rule	Y
CVE-2026-31168	ToToLink A3300R Command Injection via hour	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the hour parameter to /cgi-bin/cstecgi.cgi.	Patched by core rule	Y
CVE-2026-31167	ToToLink A3300R Command Injection via dhcpMtu	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the dhcpMtu parameter to /cgi-bin/cstecgi.cgi.	Patched by core rule	Y
CVE-2026-31166	ToToLink A3300R Command Injection via ttlWay	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the ttlWay parameter to /cgi-bin/cstecgi.cgi.	Patched by core rule	Y
CVE-2026-31163	ToToLink A3300R Command Injection via stunServerAddr	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		allowing attackers to execute arbitrary commands via the stunServerAddr parameter to /cgi-bin/cstecgi.cgi.		
CVE-2026-31162	ToToLink A3300R Command Injection via stunPort	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the stunPort parameter to /cgi-bin/cstecgi.cgi.	Patched by core rule	Y
CVE-2026-31181	ToToLink A3300R Command Injection via stunMaxAlive	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the stunMaxAlive parameter to /cgi-bin/cstecgi.cgi.	Patched by core rule	Y
CVE-2026-31179	ToToLink A3300R Command Injection via stunMinAlive	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the stunMinAlive parameter to /cgi-bin/cstecgi.cgi.	Patched by core rule	Y
CVE-2026-31178	ToToLink A3300R Command Injection via stun_user	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the stun_user parameter to /cgi-bin/cstecgi.cgi.	Patched by core rule	Y
CVE-2026-31177	ToToLink A3300R Command Injection via stunEnable	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the stunEnable parameter to /cgi-bin/cstecgi.cgi.	Patched by core rule	Y
CVE-2026-31176	ToToLink A3300R Command Injection via informEnable	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the informEnable parameter to /cgi-bin/cstecgi.cgi.	Patched by core rule	Y
CVE-2026-31175	ToToLink A3300R Command Injection via user	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		user parameter to /cgi-bin/cstecgi.cgi.		
CVE-2026-31174	ToToLink A3300R Command Injection via url	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the url parameter to /cgi-bin/cstecgi.cgi.	Patched by core rule	Y
CVE-2026-31172	ToToLink A3300R Command Injection via pppoeServiceName	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the pppoeServiceName parameter to /cgi-bin/cstecgi.cgi.	Patched by core rule	Y
CVE-2026-31171	ToToLink A3300R Command Injection via pppoeMtu	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the pppoeMtu parameter to /cgi-bin/cstecgi.cgi.	Patched by core rule	Y
CVE-2026-31165	ToToLink A3300R Command Injection via provider	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the provider parameter to /cgi-bin/cstecgi.cgi.	Patched by core rule	Y
CVE-2026-31164	ToToLink A3300R Command Injection via password	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the password parameter to /cgi-bin/cstecgi.cgi.	Patched by core rule	Y
CVE-2026-31160	ToToLink A3300R Command Injection via stun-pass	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary commands via the stun-pass parameter to /cgi-bin/cstecgi.cgi.	Patched by core rule	Y
CVE-2026-31159	Tenda W30E Command Injection via usbPartitionName	Tenda W30E V2.0 V16.01.0.21 was found to contain a command injection vulnerability in the formSetUSBPartitionUmount function via the usbPartitionName parameter. This vulnerability allows	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attackers to execute arbitrary commands via a crafted request.		
CVE-2026-41208	Tenda W30E Command Injection via hostName	Tenda W30E V2.0 V16.01.0.21 was found to contain a command injection vulnerability in the do_ping_action function via the hostName parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted request.	Patched by core rule	Y
CVE-2026-41179	D-Link DIR-882 OS Command Injection via IPAddress	A vulnerability was found in D-Link DIR-882 1.01B02. Impacted is the function sprintf of the file prog.cgi of the component HNAP1 SetNetworkSettings Handler. The manipulation of the argument IPAddress results in os command injection. The attack may be performed from remote. The exploit has been made public and could be used. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2026-40517	Totolink N300RH OS Command Injection via FileName	A flaw has been found in Totolink N300RH 6.1c.1353_B20190305. Affected is the function setUpgradeUboot of the file upgrade.so. This manipulation of the argument FileName causes os command injection. The attack is possible to be carried out remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-41304	Trendnet TEW-657BRM Command Injection via policy_name (vpn_drop)	A vulnerability has been found in Trendnet TEW-657BRM 1.00.1. Affected by this issue is the function vpn_drop of the file /setup.cgi. The manipulation of the argument policy_name leads to os command injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-41064	Trendnet TEW-657BRM Command Injection via policy_name (vpn_connect)	A flaw has been found in Trendnet TEW-657BRM 1.00.1. Affected by this vulnerability is the function vpn_connect of the file /setup.cgi. Executing a manipulation of the argument policy_name can lead to os command injection. The attack can be executed remotely. The exploit has been published and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2026-40933	Trendnet TEW-657BRM Command Injection via c4_IPAddr	A vulnerability was detected in Trendnet TEW-657BRM 1.00.1. Affected is the function ping_test of the file /setup.cgi. Performing a manipulation of the argument c4_IPAddr results in os command injection. Remote exploitation of the attack is possible. The exploit is now public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2026-38835	Trendnet TEW-657BRM Command Injection via pcdb_list	A security vulnerability has been detected in Trendnet TEW-657BRM 1.00.1. This impacts the function Edit of the file /setup.cgi. Such manipulation of the argument pcdb_list leads to os command injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	Patched by core rule	Y
CVE-2026-38834	Trendnet TEW-657BRM Command Injection via wl_enrolee_pin	A weakness has been identified in Trendnet TEW-657BRM 1.00.1. This affects the function add_wps_client of the file /setup.cgi. This manipulation of the argument wl_enrolee_pin causes os command injection. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. This vulnerability only affects	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		products that are no longer supported by the maintainer.		
CVE-2026-39866	UTT Aggressive 520W RCE via formReleaseConnect	A remote command execution (RCE) vulnerability in the /goform/formReleaseConnect component of UTT Aggressive 520W v3v1.7.7-180627 allows attackers to execute arbitrary commands via a crafted string.	Patched by core rule	Y
CVE-2026-32311	UTT Aggressive HiPER 520W RCE via formDia	A remote command execution (RCE) vulnerability in the /goform/formDia component of UTT Aggressive HiPER 520W v3v1.7.7-180627 allows attackers to execute arbitrary commands via a crafted string.	Patched by core rule	Y
CVE-2026-35582	Roxy-WI Authenticated RCE via words Parameter	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. Prior to version 8.2.6.4, the /config/<service>/find-in-config endpoint in Roxy-WI fails to sanitize the user-supplied words parameter before embedding it into a shell command string that is subsequently executed on a remote managed server via SSH. An authenticated attacker can inject arbitrary shell metacharacters to break out of the intended grep command context and execute arbitrary OS commands with sudo privileges on the target server, resulting in full Remote Code Execution (RCE). Version 8.2.6.4 patches the issue.	Patched by core rule	Y
CVE-2026-30461	WWBN AVideo RCE via url Parameter in CloneSite	WWBN AVideo is an open source video platform. In versions 29.0 and below, the cloneServer.json.php endpoint in the CloneSite plugin constructs shell commands using user-controlled input (url parameter) without proper sanitization. The input is directly concatenated into a wget command executed via exec(), allowing command injection. An attacker can inject arbitrary shell commands by breaking out of the intended URL context using shell	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		metacharacters (e.g., ;). This leads to Remote Code Execution (RCE) on the server. Commit 473c609fc2defdea8b937b00e86ce88eba1f15bb contains a fix.		
CVE-2026-35196	WWBN AVideo Incomplete Sanitization Fix Bypass	WWBN AVideo is an open source video platform. In versions up to and including 29.0, an incomplete fix for AVideo's test.php adds escapeshellarg for wget but leaves the file_get_contents and curl code paths unsanitized, and the URL validation regex /^http/ accepts strings like httpevil[.]com. Commit 78bccae74634ead68aa6528d631c9ec4fd7aa536 contains an updated fix.	Patched by core rule	Y
CVE-2026-40288	FuelCMS Authenticated RCE via add_git_submodule	Daylight Studio FuelCMS v1.5.2 was discovered to contain an authenticated remote code execution (RCE) vulnerability via the /controllers/Installer.php and the function add_git_submodule.	Patched by core rule	Y
CVE-2026-6204	Chamilo LMS OS Command Injection via Course Code	Chamilo LMS is an open-source learning management system. In versions prior to 2.0.0-RC.3, an OS Command Injection vulnerability exists in the main/inc/ajax/gradebook.ajax.php endpoint within the export_all_certificates action, where the course code retrieved from the session variable $_SESSION['_cid'] via api_get_course_id() is concatenated directly into a shell_exec() command string without sanitization or escaping using escapeshellarg(). If an attacker can manipulate or poison their session data to inject shell metacharacters into the _cid variable, they can achieve arbitrary command execution on the underlying server. This issue has been fixed in version 2.0.0-RC.3.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-6158	LibreNMS Authenticated RCE via Binary Locations Config	LibreNMS versions before 26.3.0 are affected by an authenticated remote code execution vulnerability by abusing the Binary Locations config and the Netcommand feature. Successful exploitation requires administrative privileges. Exploitation could result in compromise of the underlying web server.	Patched by core rule	Y
CVE-2026-40111	Nginx UI IDOR Authorization Bypass	Nginx UI is a web user interface for the Nginx web server. In versions 2.3.3 and prior, Nginx-UI contains an Insecure Direct Object Reference (IDOR) vulnerability that allows any authenticated user to access, modify, and delete resources belonging to other users. The application's base Model struct lacks a user_id field, and all resource endpoints perform queries by ID without verifying user ownership, enabling complete authorization bypass in multi-user environments. At time of publication, there are no publicly available patches.	Patched by core rule	Y
CVE-2026-5974	Modoboa OS Command Injection via Domain Name	Modoboa is a mail hosting and management platform. Prior to version 2.7.1, exec_cmd() in modoboa/lib/sysutils.py always runs subprocess calls with shell=True. Since domain names flow directly into shell command strings without any sanitization, a Reseller or SuperAdmin can include shell metacharacters in a domain name to run arbitrary OS commands on the server. Version 2.7.1 patches the issue.	Patched by core rule	Y
CVE-2026-5973	Budibase Unauthenticated RCE via Bash Step Webhook	Budibase is an open-source low-code platform. Prior to version 3.33.4, an unauthenticated attacker can achieve Remote Code Execution (RCE) on the Budibase server by triggering an automation that contains a Bash step via the public webhook endpoint. No authentication is required to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		trigger the exploit. The process executes as root inside the container. This issue has been patched in version 3.33.4.		
CVE-2026-5972	Tianxin Behavior Management RCE via objClass Parameter	Tianxin Internet Behavior Management System contains a command injection vulnerability in the Reporter component endpoint that allows unauthenticated attackers to execute arbitrary commands by supplying a crafted objClass parameter containing shell metacharacters and output redirection. Attackers can exploit this vulnerability to write malicious PHP files into the web root and achieve remote code execution with the privileges of the web server process. This vulnerability has been fixed in version NACFirmware_4.0.0.7_20210716.180815_topsec_0_basic.bin.	Patched by core rule	Y
CVE-2026-40088	baserCMS OS Command Injection via Core Update	baserCMS is a website development framework. Prior to version 5.2.3, baserCMS contains an OS command injection vulnerability in the core update functionality. An authenticated administrator can execute arbitrary OS commands on the server due to improper handling of user-controlled input that is directly passed to exec() without sufficient validation or escaping. This issue has been patched in version 5.2.3.	Patched by core rule	Y
CVE-2026-31170	File Browser RCE via Malicious Filename in Hook System	File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. From 2.0.0 through 2.63.1, the hook system in File Browser which executes administrator-defined shell commands on file events such as upload, rename, and delete is vulnerable to OS command injection. Variable substitution for values like $FILE and $USERNAME is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		performed via os.Expand without sanitization. An attacker with file write permission can craft a malicious filename containing shell metacharacters, causing the server to execute arbitrary OS commands when the hook fires. This results in Remote Code Execution (RCE). This feature has been disabled by default for all installations from v2.33.8 onwards.		
CVE-2026-5844	Pi-hole FTL RCE via dhcp.hosts Newline Injection	FTLDNS (pihole-FTL) provides an interactive API and also generates statistics for Pi-hole's Web interface. From 6.0 to before 6.6, the Pi-hole FTL engine contains a Remote Code Execution (RCE) vulnerability in the DHCP hosts configuration parameter (dhcp.hosts). This vulnerability allows an authenticated attacker to inject arbitrary dnsmasq configuration directives through newline characters, ultimately achieving command execution on the underlying system. This vulnerability is fixed in 6.6.	Patched by core rule	Y
CVE-2026-35585	Pi-hole FTL RCE via dhcp.leaseTime Newline Injection	FTLDNS (pihole-FTL) provides an interactive API and also generates statistics for Pi-hole's Web interface. From 6.0 to before 6.6, the Pi-hole FTL engine contains a Remote Code Execution (RCE) vulnerability in the DHCP lease time configuration parameter (dhcp.leaseTime). This vulnerability allows an authenticated attacker to inject arbitrary dnsmasq configuration directives through newline characters, ultimately achieving command execution on the underlying system. This vulnerability is fixed in 6.6.	Patched by core rule	Y
CVE-2026-35581	Pi-hole FTL RCE via dns.cnameRecords Newline Injection	FTLDNS (pihole-FTL) provides an interactive API and also generates statistics for Pi-hole's Web interface. From 6.0 to before 6.6, the Pi-hole FTL engine contains a Remote Code	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Execution (RCE) vulnerability in the DNS CNAME records configuration parameter (dns.cnameRecords). This vulnerability allows an authenticated attacker to inject arbitrary dnsmasq configuration directives through newline characters, ultimately achieving command execution on the underlying system. This vulnerability is fixed in 6.6.		
CVE-2026-35580	Pi-hole FTL RCE via dns.upstreams Newline Injection	FTLDNS (pihole-FTL) provides an interactive API and also generates statistics for Pi-hole's Web interface. From 6.0 to before 6.6, the Pi-hole FTL engine contains a Remote Code Execution (RCE) vulnerability in the upstream DNS servers configuration parameter (dns.upstreams). This vulnerability allows an authenticated attacker to inject arbitrary dnsmasq configuration directives through newline characters, ultimately achieving command execution on the underlying system. This vulnerability is fixed in 6.6.	Patched by core rule	Y
CVE-2026-35521	Aperi'Solve Unauthenticated RCE via Password in expect Command	Aperi'Solve is an open-source steganalysis web platform. Prior to 3.2.1, when uploading a JPEG, a user can specify an optional password to accompany the JPEG. This password is then directly passed into an expect command, which is then subsequently passed into a bash -c command, without any form of sanitization or validation. An unauthenticated attacker can achieve root-level RCE inside the worker container with a single HTTP request. This vulnerability is fixed in 3.2.1.	Patched by core rule	Y
CVE-2026-35520	Flowise Prompt Injection to RCE via Airtable Agent	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, the specific flaw exists within the run method of the Airtable_Agents class. The issue results from the lack of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		proper sandboxing when evaluating an LLM generated python script. Using prompt injection techniques, an unauthenticated attacker with the ability to send prompts to a chatflow using the Airtable Agent node may convince an LLM to respond with a malicious python script that executes attacker controlled commands on the flowise server. This vulnerability is fixed in 3.1.0.		
CVE-2026-35518	Flowise Arbitrary Command Execution via MCP stdio Adapter	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, due to unsafe serialization of stdio commands in the MCP adapter, an authenticated attacker can add an MCP stdio server with an arbitrary command, achieving command execution. This vulnerability is fixed in 3.1.0.	Patched by core rule	Y
CVE-2026-35517	PraisonAI RCE via Untrusted YAML Workflow File	PraisonAI is a multi-agent teams system. In versions below 4.5.139 of PraisonAI and 1.5.140 of praisonaiagents, the workflow engine is vulnerable to arbitrary command and code execution through untrusted YAML files. When praisonai workflow run <file.yaml> loads a YAML file with type: job, the JobWorkflowExecutor in job_workflow.py processes steps that support run: (shell commands via subprocess.run()), script: (inline Python via exec()), and python: (arbitrary Python script execution) all without any validation, sandboxing, or user confirmation. This issue has been fixed in versions 4.5.139 of PraisonAI and 1.5.140 of praisonaiagents.	Patched by core rule	Y
CVE-2026-35463	PraisonAI Command Injection via hooks.json shell=True	PraisonAIAgents is a multi-agent teams system. Prior to 1.5.128, the memory hooks executor in praisonaiagents passes a user-controlled command string directly to subprocess.run() with	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		shell=True at src/praisonai-agents/praisonaiagents/memory/hooks.py. No sanitization is performed and shell metacharacters are interpreted by /bin/sh before the intended command executes. An agent that gains file-write access through prompt injection can overwrite .praisonai/hooks.json and have its payload execute silently at every subsequent lifecycle event without further user interaction. This vulnerability is fixed in 1.5.128.		
CVE-2021-4473	PraisonAI Shell Metacharacter Injection via execute_command	PraisonAI is a multi-agent teams system. Prior to 4.5.121, the execute_command function and workflow shell execution are exposed to user-controlled input via agent workflows, YAML definitions, and LLM-generated tool calls, allowing attackers to inject arbitrary shell commands through shell metacharacters. This vulnerability is fixed in 4.5.121.	Patched by core rule	Y
CVE-2026-5709	PraisonAI SubprocessSandbox Escape via sh/bash	PraisonAI is a multi-agent teams system. Prior to version 4.5.97, SubprocessSandbox in all modes (BASIC, STRICT, NETWORK_ISOLATED) calls subprocess.run() with shell=True and relies solely on string-pattern matching to block dangerous commands. The blocklist does not include sh or bash as standalone executables, allowing trivial sandbox escape in STRICT mode via sh -c '<command>'. This issue has been patched in version 4.5.97.	Patched by core rule	Y
CVE-2026-5707	PraisonAI run_python Backtick and Dollar Substitution Escape	PraisonAI is a multi-agent teams system. Prior to version 1.5.90, run_python() in praisonai constructs a shell command string by interpolating user-controlled code into python3 -c "<code>" and passing it to subprocess.run(..., shell=True). The escaping logic only handles \ and ", leaving $() and backtick	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		substitutions unescaped, allowing arbitrary OS command execution before Python is invoked. This issue has been patched in version 1.5.90.		
CVE-2026-35022	PraisonAI MCP CLI Injection via anyio.open_process	PraisonAI is a multi-agent teams system. From version 4.5.15 to before version 4.5.69, the --mcp CLI argument is passed directly to shlex.split() and forwarded through the call chain to anyio.open_process() with no validation, allowlist check, or sanitization at any hop, allowing arbitrary OS command execution as the process user. This issue has been patched in version 4.5.69.	Patched by core rule	Y
CVE-2026-35021	MetaGPT OS Command Injection via Bash.run	A vulnerability was determined in FoundationAgents MetaGPT up to 0.8.1. The affected element is the function Bash.run in the library metagpt/tools/libs/terminal.py. This manipulation causes os command injection. The attack is possible to be carried out remotely. The project was informed of the problem early through a pull request but has not reacted yet.	Patched by core rule	Y
CVE-2026-35020	MetaGPT OS Command Injection via get_mime_type	A vulnerability was found in FoundationAgents MetaGPT up to 0.8.1. Impacted is the function get_mime_type of the file metagpt/utils/common.py. The manipulation results in os command injection. The attack can be executed remotely. The exploit has been made public and could be used. The project was informed of the problem early through a pull request but has not reacted yet.	Patched by core rule	Y
CVE-2026-35043	MetaGPT OS Command Injection via Terminal.run_command	A vulnerability has been found in FoundationAgents MetaGPT up to 0.8.1. This issue affects the function Terminal.run_command in the library metagpt/tools/libs/terminal.py. The manipulation leads to os command injection. Remote exploitation of the attack is	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		possible. The exploit has been disclosed to the public and may be used. The identifier of the patch is d04ffc8dc67903e8b327f78ec121df5e190ffc7b.		
CVE-2026-34977	OpenHands Command Injection via git/diff path Parameter	OpenHands is software for AI-driven development. Starting in version 1.5.0, a Command Injection vulnerability exists in the get_git_diff() method at openhands/runtime/utils/git_handler.py:134. The path parameter from the /api/conversations/{conversation_id}/git/diff API endpoint is passed unsanitized to a shell command, allowing authenticated attackers to execute arbitrary commands in the agent sandbox. Version 1.5.0 fixes the issue.	Patched by core rule	Y
CVE-2026-34940	KubeAI Shell Injection via Ollama Model URL Startup Probe	KubeAI is an AI inference operator for kubernetes. Prior to 0.23.2, the ollamaStartupProbeScript() function in internal/modelcontroller/engine_ollama.go constructs a shell command string using fmt.Sprintf with unsanitized model URL components (ref, modelParam). This shell command is executed via bash -c as a Kubernetes startup probe. An attacker who can create or update Model custom resources can inject arbitrary shell commands that execute inside model server pods. This vulnerability is fixed in 0.23.2.	Patched by core rule	Y
CVE-2026-31067	Paperclip Agent Privilege Escalation via provisionCommand	Paperclip is a Node.js server and React UI that orchestrates a team of AI agents to run a business. Versions of @paperclipai/server prior to 2026.416.0 contain a privilege escalation vulnerability that allows an attacker with an Agent API key to execute arbitrary OS commands on the Paperclip server host. The vulnerability occurs because agents are allowed to update	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		their own adapterConfig via the /agents/:id API endpoint. The configuration field adapterConfig.workspaceStrategy.provisionCommand is later executed by the server runtime. This vulnerability allows remote code execution on the server host. @paperclipai/server version 2026.416.0 fixes the issue.		
CVE-2026-31059	BentoML Cloud Deployment RCE via system_packages f-string	BentoML is a Python library for building online serving systems optimized for AI apps and model inference. Prior to 1.4.38, the cloud deployment path in src/bentoml/_internal/cloud/deployment.py was not included in the fix for CVE-2026-33744. Line 1648 interpolates system_packages directly into a shell command using an f-string without any quoting. The generated script is uploaded to BentoCloud as setup.sh and executed on the cloud build infrastructure during deployment, making this a remote code execution on the CI/CD tier. This vulnerability is fixed in 1.4.38.	Patched by core rule	Y
CVE-2026-34955	Flowsint Docker Container Escape via org_to_asn Transform	Flowsint is an open-source OSINT graph exploration tool designed for cybersecurity investigation, transparency, and verification. Flowsint allows a user to create investigations, which are used to manage sketches and analyses. The nodes can have automated processes execute on them called 'transformers'. A remote attacker can create a sketch, then trigger the 'org_to_asn' transform on an organization node to execute arbitrary OS commands as root on the host machine via shell metacharacters and a docker container escape. Commit b52cbbb904c8013b74308d58af88bc7dbb1b055c appears to remove the code that causes this issue.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-34937	Rclone Unauthenticated RCE via bearer_token_command in RC Endpoint	Rclone is a command-line program to sync files and directories to and from different cloud storage providers. Starting in version 1.48.0 and prior to version 1.73.5, the RC endpoint operations/fsinfo is exposed without AuthRequired: true and accepts attacker-controlled fs input. Because rc.GetFs(...) supports inline backend definitions, an unauthenticated attacker can instantiate an attacker-controlled backend on demand. For the WebDAV backend, bearer_token_command is executed during backend initialization, making single-request unauthenticated local command execution possible on reachable RC deployments without global HTTP authentication. Version 1.73.5 patches the issue.	Patched by core rule	Y
CVE-2026-34935	PinchTab PowerShell Injection via Crafted Profile Name	PinchTab is a standalone HTTP server that gives AI agents direct control over a Chrome browser. PinchTab v0.8.4 contains a Windows-only command injection issue in the orphaned Chrome cleanup path. When an instance is stopped, the Windows cleanup routine builds a PowerShell -Command string using a needle derived from the profile path. In v0.8.4, that string interpolation escapes backslashes but does not safely neutralize other PowerShell metacharacters. If an attacker can launch an instance using a crafted profile name and then trigger the cleanup path, they may be able to execute arbitrary PowerShell commands on the Windows host. Version 0.8.5 contains a patch for the issue.	Patched by core rule	Y
CVE-2026-35216	OneUptime Playwright Sandbox Escape via _browserType.launchServer	OneUptime is an open-source monitoring and observability platform. Prior to version 10.0.35, a low-privileged authenticated user (ProjectMember) can achieve	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remote command execution on the Probe container/host by abusing Synthetic Monitor Playwright script execution. Synthetic monitor code is executed in VMRunner.runCodeInNodeVM with a live Playwright page object in context. The sandbox relies on a denylist of blocked properties/methods, but it is incomplete. Specifically, _browserType and launchServer are not blocked, so attacker code can traverse page.context().browser()._browserType.launchServer(...) and spawn arbitrary processes. Version 10.0.35 contains a patch.		
CVE-2025-64340	FastMCP Server Name Injection via cmd.exe Wrapper on Windows	FastMCP is the standard framework for building MCP applications. Prior to version 3.2.0, server names containing shell metacharacters (e.g., &) can cause command injection on Windows when passed to fastmcp install claude-code or fastmcp install gemini-cli. These install paths use subprocess.run() with a list argument, but on Windows the target CLIs often resolve to .cmd wrappers that are executed through cmd.exe, which interprets metacharacters in the flattened command string. This issue has been patched in version 3.2.0.	Patched by core rule	Y
CVE-2026-5355	MLflow Command Injection via model_uri in enable_mlserver	A command injection vulnerability exists in mlflow/mlflow when serving a model with enable_mlserver=True. The model_uri is embedded directly into a shell command executed via bash -c without proper sanitization. If the model_uri contains shell metacharacters, such as $() or backticks, it allows for command substitution and execution of attacker-controlled commands. This vulnerability affects the latest version of mlflow/mlflow	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and can lead to privilege escalation if a higher-privileged service serves models from a directory writable by lower-privileged users.		
CVE-2026-5354	MLflow RCE via python_env.yaml Dependency Interpolation	A command injection vulnerability exists in MLflow's model serving container initialization code, specifically in the _install_model_dependencies_to_env() function. When deploying a model with env_manager=LOCAL, MLflow reads dependency specifications from the model artifact's python_env.yaml file and directly interpolates them into a shell command without sanitization. This allows an attacker to supply a malicious model artifact and achieve arbitrary command execution on systems that deploy the model. The vulnerability affects versions 3.8.0 and is fixed in version 3.8.2.	Patched by core rule	Y
CVE-2026-5353	AWS RES Authenticated RCE via FileBrowser API	Unsanitized input in the FileBrowser API in AWS Research and Engineering Studio (RES) version 2024.10 through 2025.12.01 might allow a remote authenticated actor to execute arbitrary commands on the cluster-manager EC2 instance via crafted input when using the FileBrowser functionality. To remediate this issue, users are advised to upgrade to RES version 2026.03 or apply the corresponding mitigation patch to their existing environment.	Patched by core rule	Y
CVE-2026-5352	AWS RES Authenticated RCE via Virtual Desktop Session Name	Unsanitized input in an OS command in the virtual desktop session name handling in AWS Research and Engineering Studio (RES) version 2025.03 through 2025.12.01 might allow a remote authenticated actor to execute arbitrary commands as root on the virtual desktop host via a crafted session name. To	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		remediate this issue, users are advised to upgrade to RES version 2026.03 or apply the corresponding mitigation patch to their existing environment.		
CVE-2026-5351	Anthropic Claude Code OS Command Injection via apiKeyHelper	Anthropic Claude Code CLI and Claude Agent SDK contain an OS command injection vulnerability in authentication helper execution where helper configuration values are executed using shell=true without input validation. Attackers who can influence authentication settings can inject shell metacharacters through parameters like apiKeyHelper, awsAuthRefresh, awsCredentialExport, and gcpAuthRefresh to execute arbitrary commands with the privileges of the user or automation environment, enabling credential theft and environment variable exfiltration.	Patched by core rule	Y
CVE-2026-33641	Anthropic Claude Code OS Command Injection via Prompt Editor File Path	Anthropic Claude Code CLI and Claude Agent SDK contain an OS command injection vulnerability in the prompt editor invocation utility that allows attackers to execute arbitrary commands by crafting malicious file paths. Attackers can inject shell metacharacters such as $() or backtick expressions into file paths that are interpolated into shell commands executed via execSync. Although the file path is wrapped in double quotes, POSIX shell semantics do not prevent command substitution within double quotes, allowing injected expressions to be evaluated and resulting in arbitrary command execution with the privileges of the user running the CLI.	Patched by core rule	Y
CVE-2026-34243	Anthropic Claude Code OS Command Injection via TERMINAL Variable	Anthropic Claude Code CLI and Claude Agent SDK contain an OS command injection vulnerability in the command	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		lookup helper and deep-link terminal launcher that allows local attackers to execute arbitrary commands by manipulating the TERMINAL environment variable. Attackers can inject shell metacharacters into the TERMINAL variable which are interpreted by /bin/sh when the command lookup helper constructs and executes shell commands with shell=true. The vulnerability can be triggered during normal CLI execution as well as via the deep-link handler path, resulting in arbitrary command execution with the privileges of the user running the CLI.		
CVE-2026-0596	Emissary Shell Injection via IN_FILE_ENDING/OUT_FILE_ENDING Config	Emissary is a P2P based data-driven workflow engine. In versions 8.42.0 and below, Executrix.getCommand() is vulnerable to OS command injection because it interpolates temporary file paths into a /bin/sh -c shell command string without any escaping or input validation. The IN_FILE_ENDING and OUT_FILE_ENDING configuration keys flow directly into these paths, allowing a place author who can write or modify a .cfg file to inject arbitrary shell metacharacters that execute OS commands in the JVM process's security context. This issue has been fixed in version 8.43.0.	Patched by core rule	Y
CVE-2026-21861	Emissary Shell Injection via PLACE_NAME Insufficient Sanitization	Emissary is a P2P based data-driven workflow engine. Prior to 8.39.0, the Executrix utility class constructed shell commands by concatenating configuration-derived values including the PLACE_NAME parameter with insufficient sanitization. Only spaces were replaced with underscores, allowing shell metacharacters (;, |, $, `, (,), etc.) to pass through into /bin/sh -c command execution. This vulnerability is fixed in 8.39.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-33030	Emissary GitHub Actions workflow_dispatch Input Injection	Emissary is a P2P based data-driven workflow engine. Prior to 8.39.0, GitHub Actions workflow files contained shell injection points where user-controlled workflow_dispatch inputs were interpolated directly into shell commands via ${{ }} expression syntax. An attacker with repository write access could inject arbitrary shell commands, leading to repository poisoning and supply chain compromise affecting all downstream users. This vulnerability is fixed in 8.39.0.	Patched by core rule	Y
CVE-2025-15379	Lawnchair GitHub Actions Command Injection via release_update.yml	Lawnchair is a free, open-source home app for Android. Prior to commit fcba413f55dd47f8a3921445252849126c6266b2, command injection in release_update.yml workflow dispatch input allows arbitrary code execution. Commit fcba413f55dd47f8a3921445252849126c6266b2 patches the issue.	Patched by core rule	Y
CVE-2026-33718	wenxian GitHub Actions Shell Injection via issue_comment.body	wenxian is a tool to generate BIBTEX files from given identifiers (DOI, PMID, arXiv ID, or paper title). In versions 0.3.1 and prior, a GitHub Actions workflow uses untrusted user input from issue_comment.body directly inside a shell command, allowing potential command injection and arbitrary code execution on the runner. At time of publication, there are no publicly available patches.	Patched by core rule	Y
CVE-2026-33623	radare2 Command Injection via PDB Symbol Name Newline	radare2 prior to 6.1.4 contains a command injection vulnerability in the PDB parser's print_gvars() function that allows attackers to execute arbitrary commands by crafting a malicious PDB file with newline characters in symbol names. Attackers can inject arbitrary radare2 commands through unsanitized symbol name interpolation in the flag	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		rename command, which are then executed when a user runs the idp command against the malicious PDB file, enabling arbitrary OS command execution through radare2's shell execution operator.		
CVE-2026-33396	Glances OS Command Execution via Config Backtick Parsing	Glances is an open-source system cross-platform monitoring tool. Prior to version 4.5.3, Glances supports dynamic configuration values in which substrings enclosed in backticks are executed as system commands during configuration parsing. This behavior occurs in Config.get_value() and is implemented without validation or restriction of the executed commands. If an attacker can modify or influence configuration files, arbitrary commands will execute automatically with the privileges of the Glances process during startup or configuration reload. This issue has been patched in version 4.5.3.	Patched by core rule	Y
CVE-2026-27602	pyLoad Privilege Escalation via AntiVirus Plugin avfile Path	pyLoad is a free and open-source download manager written in Python. In 0.5.0b3.dev96 and earlier, the ADMIN_ONLY_OPTIONS protection mechanism restricts security-critical configuration values to admin-only access. However, this protection is only applied to core config options, not to plugin config options. The AntiVirus plugin stores an executable path (avfile) in its config, which is passed directly to subprocess.Popen(). A non-admin user with SETTINGS permission can change this path to achieve remote code execution.	Patched by core rule	Y

VULNERABILITY DETAILS

Path Traversal Vulnerabilities

Path traversal vulnerabilities allow attackers to access or overwrite files outside the intended directory by exploiting insufficient validation of user-supplied file paths. All 8 path traversal CVEs in April 2026 are covered by AppTrana core rules.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-6940	radare2 Path Traversal via Absolute Project Path	radare2 prior to 6.1.4 contains a path traversal vulnerability in project deletion that allows local attackers to recursively delete arbitrary directories by supplying absolute paths that escape the configured dir.projects root directory. Attackers can craft absolute paths to project marker files outside the project storage boundary to cause recursive deletion of attacker-chosen directories with permissions of the radare2 process, resulting in integrity and availability loss.	Patched by core rule	Y
CVE-2026-3689	OpenClaw Canvas Path Traversal Information Disclosure	OpenClaw Canvas Path Traversal Information Disclosure Vulnerability. This vulnerability allows remote attackers to disclose sensitive information on affected installations of OpenClaw. Authentication is required to exploit this vulnerability. The specific flaw exists within the handling of the path parameters provided to the canvas gateway endpoint. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of the service account. Was ZDI-CAN-29312.	Patched by core rule	Y
CVE-2026-35484	text-generation-webui Unauthenticated Path	text-generation-webui is an open-source web interface for running Large Language	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Traversal via load_preset()	Models. Prior to 4.3, an unauthenticated path traversal vulnerability in load_preset() allows reading any .yaml file on the server filesystem. The parsed YAML key-value pairs (including passwords, API keys, connection strings) are returned in the API response. This vulnerability is fixed in 4.3.		
CVE-2026-34591	Poetry Arbitrary File Write via Crafted Wheel ../ Paths	Poetry is a dependency manager for Python. From version 1.4.0 to before version 2.3.3, a crafted wheel can contain ../ paths that Poetry writes to disk without containment checks, allowing arbitrary file write with the privileges of the Poetry process. It is reachable from untrusted package artifacts during normal install flows. This issue has been patched in version 2.3.3.	Patched by core rule	Y
CVE-2026-30285	Earn Crypto v2.60.0 Arbitrary File Overwrite via Path Traversal	An arbitrary file overwrite vulnerability in Zora: Post, Trade, Earn Crypto v2.60.0 allows attackers to overwrite critical internal files via the file import process, leading to arbitrary code execution or information exposure.	Patched by core rule	Y
CVE-2026-34070	LangChain Arbitrary File Read via load_prompt() Path Traversal	LangChain is a framework for building agents and LLM-powered applications. Prior to version 1.2.22, multiple functions in langchain_core.prompts.loading read files from paths embedded in deserialized config dicts without validating against directory traversal or absolute path injection. When an application passes user-influenced prompt configurations to load_prompt() or load_prompt_from_config(), an attacker can read arbitrary files on the host filesystem, constrained only by file-extension checks (.txt for	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		templates, .json/.yaml for examples). This issue has been patched in version 1.2.22.		
CVE-2026-29871	awesome-llm-apps FastAPI stream-audio Endpoint Path Traversal	A path traversal vulnerability exists in the awesome-llm-apps project in commit e46690f99c3f08be80a9877fab52acacf7ab8251 (2026-01-19) in the Beifong AI News and Podcast Agent backend in FastAPI backend, stream-audio endpoint, in file routers/podcast_router.py, in function stream_audio. The stream-audio endpoint accepts a user-controlled path parameter that is concatenated into a filesystem path without proper validation or restriction. An unauthenticated remote attacker can exploit this vulnerability to read arbitrary files from the server filesystem, potentially disclosing sensitive information such as configuration files and credentials.	Patched by core rule	Y
CVE-2026-33528	GoDoxy Authenticated Path Traversal via filename Parameter	GoDoxy is a reverse proxy and container orchestrator for self-hosters. Prior to version 0.27.5, the file content API endpoint at /api/v1/file/content is vulnerable to path traversal. The filename query parameter is passed directly to path.Join(common.ConfigBasePath, filename) where ConfigBasePath = config (a relative path). No sanitization or validation is applied beyond checking that the field is non-empty. An authenticated attacker can use ../ sequences to read or write files outside the intended config/ directory, including TLS private keys, OAuth refresh tokens, and any file accessible to the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		container's UID. Version 0.27.5 fixes the issue.		

VULNERABILITY DETAILS

SQL Injection Vulnerabilities

SQL injection vulnerabilities exploit insufficient input sanitization to manipulate database queries, enabling data exfiltration, authentication bypass, and in some cases remote code execution. All 109 SQL injection CVEs in April 2026 are patched by AppTrana core rules.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-33078	Roxy-WI SQL Injection via server_ip in haproxy_section_save	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. Versions prior to 8.2.6.4 have a SQL injection vulnerability in the haproxy_section_save function in app/routes/config/routes.py. The server_ip parameter, sourced from the URL path, is passed unsanitized through multiple function calls and ultimately interpolated into a SQL query string using Python string formatting, allowing attackers to execute arbitrary SQL commands. Version 8.2.6.4 fixes the issue.	Patched by core rule	Y
CVE-2025-50229	Jizhicms SQL Injection in Product Editing Module	Jizhicms v2.5.4 is vulnerable to SQL injection in the product editing module.	Patched by core rule	Y
CVE-2026-41460	SocialEngine SQL Injection via text Parameter in get-memberall	SocialEngine versions 7.8.0 and prior contain a SQL injection vulnerability in the /activity/index/get-memberall endpoint where user-supplied input passed via the text parameter is not sanitized before being incorporated into a SQL query. An unauthenticated remote attacker can exploit this vulnerability to read arbitrary data from the database, reset administrator account passwords, and gain unauthorized access to the Packages Manager in the Admin Panel, potentially enabling remote code execution.	Patched by core rule	Y
CVE-2026-35588	Glances CQL Injection via Cassandra Export Module Config	Glances is an open-source system cross-platform monitoring tool. Prior to version 4.5.4, the Cassandra export module (glances/exports/glances_cassandra/__init__.py) interpolates	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		keyspace, table, and replication_factor configuration values directly into CQL statements without validation. A user with write access to glances.conf can redirect all monitoring data to an attacker-controlled Cassandra keyspace. Version 4.5.4 contains a fix.		
CVE-2026-40900	DataEase SQL Injection via previewSql Stacked Queries	DataEase is an open-source data visualization and analytics platform. Versions 2.10.20 and below contain a SQL injection vulnerability in the /de2api/datasetData/previewSql endpoint. The user-supplied SQL is wrapped in a subquery without validation that the input is a single SELECT statement. Combined with the JDBC blocklist bypass that allows enabling allowMultiQueries=true, an attacker can break out of the subquery and execute arbitrary stacked SQL statements. An authenticated attacker with access to valid datasource credentials can achieve full read and write access to the underlying database. This issue has been fixed in version 2.10.21.	Patched by core rule	Y
CVE-2026-33207	DataEase SQL Injection via tableName in getTableField Endpoint	DataEase is an open-source data visualization and analytics platform. Versions 2.10.20 and below contain a SQL injection vulnerability in the /datasource/getTableField endpoint. The getTableFiledSql method in CalciteProvider.java incorporates the tableName parameter directly into SQL query strings using String.format without parameterization or sanitization. Although DatasourceServer.java validates that the table name exists in the datasource, an attacker can bypass this by first registering an API datasource with a malicious deTableName. An authenticated attacker can execute arbitrary SQL commands, enabling error-based extraction of sensitive	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		database information. This issue has been fixed in version 2.10.21.		
CVE-2026-33122	DataEase SQL Injection via deTableName in Datasource Update	DataEase is an open-source data visualization and analytics platform. Versions 2.10.20 and below contain a SQL injection vulnerability in the API datasource update process. When a new table definition is added during a datasource update via /de2api/datasource/update, the deTableName field from the user-submitted configuration is passed to DatasourceSyncManage.createEngineTable, where it is substituted into a CREATE TABLE statement template without any sanitization or identifier escaping. An authenticated attacker can inject arbitrary SQL commands by crafting a deTableName that breaks out of identifier quoting, enabling error-based SQL injection. This issue has been fixed in version 2.10.21.	Patched by core rule	Y
CVE-2026-33121	DataEase SQL Injection via deTableName in Datasource Save	DataEase is an open-source data visualization and analytics platform. Versions 2.10.20 and below contain a SQL injection vulnerability in the API datasource saving process. The deTableName field from the Base64-encoded datasource configuration is used to construct a DDL statement via simple string replacement without any sanitization or escaping of the table name. An authenticated attacker can inject arbitrary SQL commands by crafting a deTableName that breaks out of identifier quoting, enabling error-based SQL injection that can extract database information such as the MySQL version. This issue has been fixed in version 2.10.21.	Patched by core rule	Y
CVE-2026-33084	DataEase Blind SQL Injection via sort Parameter in enumValueObj	DataEase is an open-source data visualization and analytics platform. Versions 2.10.20 and below contain a SQL injection vulnerability in the sort parameter of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/de2api/datasetData/enumValueObj endpoint. The DatasetDataManage service layer directly transfers the user-supplied sort value to the sorting metadata DTO, which is passed to Order2SQLObj where it is incorporated into the SQL ORDER BY clause without any whitelist validation, and then executed via CalciteProvider. An authenticated attacker can inject arbitrary SQL commands through the sort parameter, enabling time-based blind SQL injection. This issue has been fixed in version 2.10.21.		
CVE-2026-33083	DataEase Blind SQL Injection via orderDirection in Dataset Endpoints	DataEase is an open-source data visualization and analytics platform. Versions 2.10.20 and below contain a SQL injection vulnerability in the orderDirection parameter used in dataset-related endpoints including /de2api/datasetData/enumValueDs and /de2api/datasetTree/exportDataset. The Order2SQLObj class directly assigns the raw user-supplied orderDirection value into the SQL query without any validation or whitelist enforcement, and the value is rendered into the ORDER BY clause via StringTemplate before being executed against the database. An authenticated attacker can inject arbitrary SQL commands through the sorting direction field, enabling time-based blind data extraction and denial of service. This issue has been fixed in version 2.10.21.	Patched by core rule	Y
CVE-2026-33082	DataEase Blind SQL Injection via expressionTree in Dataset Export	DataEase is an open source data visualization analysis tool. Versions 2.10.20 and below contain a SQL injection vulnerability in the dataset export functionality. The expressionTree parameter in POST /de2api/datasetTree/exportDataset is deserialized into a filtering object and passed to WhereTree2Str.transFilterTrees for SQL translation, where user-supplied	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		controlled values in like filter terms are directly concatenated into SQL fragments without sanitization. An attacker can inject arbitrary SQL commands by escaping the string literal in the filter value, enabling blind SQL injection through techniques such as time-based extraction. This issue has been fixed in version 2.10.21.		
CVE-2025-65135	School Management System Blind SQL Injection via fromdate Parameter	In manikandan580 School-management-system 1.0, a time-based blind SQL injection vulnerability exists in /studentms/admin/between-date-reprtsdetails.php through the fromdate POST parameter.	Patched by core rule	Y
CVE-2025-65133	School Management System SQL Injection via Crafted HTTP Request	A SQL injection vulnerability exists in the School Management System (version 1.0) by manikandan580. An unauthenticated or authenticated remote attacker can supply a crafted HTTP request to the affected endpoint to manipulate SQL query logic and extract sensitive database information.	Patched by core rule	Y
CVE-2026-40315	PraisonAI SQL Identifier Injection via table_prefix in SQLiteConversationStore	PraisonAI is a multi-agent teams system. Prior to 4.5.133, there is an SQL identifier injection vulnerability in SQLiteConversationStore where the table_prefix configuration value is directly concatenated into SQL queries via f-strings without any validation or sanitization. Since SQL identifiers cannot be safely parameterized, an attacker who controls the table_prefix value (e.g., through from_yaml or from_dict configuration input) can inject arbitrary SQL fragments that alter query structure. This enables unauthorized data access, such as reading internal SQLite tables like sqlite_master, and manipulation of query results through techniques like UNION-based injection. This issue has been fixed in version 4.5.133.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-36947	Sourcecodester Repair Shop SQL Injection in view_service.php	Sourcecodester Computer and Mobile Repair Shop Management System v1.0 is vulnerable to SQL Injection in the file /rsms/admin/services/view_service.php.	Patched by core rule	Y
CVE-2026-36946	Sourcecodester Repair Shop SQL Injection in view_details.php	Sourcecodester Computer and Mobile Repair Shop Management System v1.0 is vulnerable to SQL injection in the file /rsms/admin/inquiries/view_details.php.	Patched by core rule	Y
CVE-2026-36923	Sourcecodester Cab Management SQL Injection in view_booking.php	Sourcecodester Cab Management System 1.0 is vulnerable to SQL Injection in the file /cms/admin/bookings/view_booking.php.	Patched by core rule	Y
CVE-2026-36922	Sourcecodester Cab Management SQL Injection in view_category.php	Sourcecodester Cab Management System v1.0 is vulnerable to SQL injection in the file /cms/admin/categories/view_category.php.	Patched by core rule	Y
CVE-2026-36920	Sourcecodester Online Reviewer SQL Injection in questions-view.php	Sourcecodester Online Reviewer System v1.0 is vulnerable to SQL Injection in the file /system/system/admins/assessments/examproper/questions-view.php.	Patched by core rule	Y
CVE-2026-36919	Sourcecodester Online Reviewer SQL Injection in exam-update.php	Sourcecodester Online Reviewer System v1.0 is vulnerable to SQL Injection in the file /system/system/admins/assessments/examproper/exam-update.php.	Patched by core rule	Y
CVE-2026-36874	Sourcecodester Library System SQL Injection in load_student.php	Sourcecodester Basic Library System v1.0 is vulnerable to SQL Injection in /librarysystem/load_student.php.	Patched by core rule	Y
CVE-2026-36873	Sourcecodester Library System SQL Injection in load_admin.php	Sourcecodester Basic Library System v1.0 is vulnerable to SQL Injection in /librarysystem/load_admin.php.	Patched by core rule	Y
CVE-2026-36872	Sourcecodester Library System SQL Injection in load_book.php	Sourcecodester Basic Library System v1.0 is vulnerable to SQL Injection in /librarysystem/load_book.php.	Patched by core rule	Y
CVE-2026-3830	Product Filter for WooCommerce WordPress Plugin SQL Injection	The Product Filter for WooCommerce by WBW WordPress plugin before 3.1.3 does not sanitize and escape a	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		parameter before using it in a SQL statement, allowing unauthenticated users to perform SQL injection attacks.		
CVE-2025-15441	Form Maker by 10Web WordPress Plugin SQL Injection via MySQL Mapping	The Form Maker by 10Web WordPress plugin before 1.15.38 does not properly prepare SQL queries when the MySQL Mapping feature is in use, which could make SQL Injection attacks possible in certain contexts.	Patched by core rule	Y
CVE-2019-25713	MyT-PM SQL Injection via Charge[group_total] Parameter	MyT-PM 1.5.1 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the Charge[group_total] parameter. Attackers can submit crafted POST requests to the /charge/admin endpoint with error-based, time-based blind, or stacked query payloads to extract sensitive database information or manipulate data.	Patched by core rule	Y
CVE-2019-25710	Dolibarr ERP SQL Injection via rowid in admin dict.php	Dolibarr ERP-CRM 8.0.4 contains an SQL injection vulnerability in the rowid parameter of the admin dict.php endpoint that allows attackers to execute arbitrary SQL queries. Attackers can inject malicious SQL code through the rowid POST parameter to extract sensitive database information using error-based SQL injection techniques.	Patched by core rule	Y
CVE-2019-25707	eBrigade ERP SQL Injection via id Parameter in pdf.php	eBrigade ERP 4.5 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the id parameter. Attackers can send GET requests to pdf.php with crafted SQL payloads in the id parameter to extract sensitive database information including table names and schema details.	Patched by core rule	Y
CVE-2019-25703	ImpressCMS Blind SQL Injection via bid Parameter	ImpressCMS 1.3.11 contains a time-based blind SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through the bid	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		parameter. Attackers can send POST requests to the admin.php endpoint with malicious bid values containing SQL commands to extract sensitive database information.		
CVE-2019-25699	Newsbull Haber Script SQL Injection via search Parameter	Newsbull Haber Script 1.0.0 contains multiple SQL injection vulnerabilities in the search parameter that allow authenticated attackers to extract database information through time-based, blind, and boolean-based injection techniques. Attackers can inject malicious SQL code through the search parameter in endpoints like /admin/comment/records, /admin/category/records, /admin/news/records, and /admin/menu/childs.	Patched by core rule	Y
CVE-2019-25697	CMSsite SQL Injection via cat_id Parameter in category.php	CMSsite 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the cat_id parameter. Attackers can send GET requests to category.php with malicious cat_id values to extract sensitive database information including usernames and credentials.	Patched by core rule	Y
CVE-2018-25257	Adianti Framework SQL Injection via name Field in SystemProfileForm	Adianti Framework 5.5.0 and 5.6.0 contains an SQL injection vulnerability that allows authenticated users to manipulate database queries by injecting SQL code through the name field in SystemProfileForm. Attackers can submit crafted SQL statements in the profile edit endpoint to modify user credentials and gain administrative access.	Patched by core rule	Y
CVE-2026-36236	SourceCodester Engineers Online Portal SQL Injection via new_password	SourceCodester Engineers Online Portal v1.0 is vulnerable to SQL Injection in update_password.php via the new_password parameter.	Patched by core rule	Y
CVE-2026-36235	itsourcecode Online Student Enrollment SQL Injection via subjcode in scheduleSubList.php	A SQL injection vulnerability was found in the scheduleSubList.php file of itsourcecode Online Student Enrollment System v1.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		The reason for this issue is that the subjcode parameter is directly embedded into the SQL query via string interpolation without any sanitization or validation.		
CVE-2026-36234	itsourcecode Online Student Enrollment SQL Injection via coursename in newCourse.php	itsourcecode Online Student Enrollment System v1.0 is vulnerable to SQL Injection in newCourse.php via the coursename parameter.	Patched by core rule	Y
CVE-2026-36233	itsourcecode Online Student Enrollment SQL Injection via subjcode in assignInstructorSubjects.php	A SQL injection vulnerability was found in the assignInstructorSubjects.php file of itsourcecode Online Student Enrollment System v1.0. The reason for this issue is that attackers can inject malicious code via the parameter subjcode and use it directly in SQL queries without the need for appropriate cleaning or validation.	Patched by core rule	Y
CVE-2026-36232	itsourcecode Online Student Enrollment SQL Injection via classId in instructorClasses.php	A SQL injection vulnerability was found in the instructorClasses.php file of itsourcecode Online Student Enrollment System v1.0. The reason for this issue is that the classId parameter from $_GET['classId'] is directly concatenated into the SQL query without any sanitization or validation.	Patched by core rule	Y
CVE-2023-54359	WordPress adivaha Travel Plugin Blind SQL Injection via pid Parameter	WordPress adivaha Travel Plugin 2.3 contains a time-based blind SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the pid GET parameter. Attackers can send requests to the /mobile-app/v3/ endpoint with crafted pid values using XOR-based payloads to extract sensitive database information or cause denial of service.	Patched by core rule	Y
CVE-2026-39342	ChurchCRM SQL Injection via searchwhat in QueryView.php	ChurchCRM is an open-source church management system. Prior to 7.1.0, the searchwhat parameter via QueryView.php with the QueryID=15 is vulnerable to a SQL injection. The authenticated user requires	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		access to Data/Reports > Query Menu and access to the Advanced Search query. This vulnerability is fixed in 7.1.0.		
CVE-2026-39318	ChurchCRM SQL Injection via Field Parameter in Row Operation Endpoints	ChurchCRM is an open-source church management system. Versions prior to 7.1.0 have an SQL injection vulnerability in the endpoints /GroupPropsFormRowOps.php, /PersonCustomFieldsRowOps.php, and /FamilyCustomFieldsRowOps.php. A user has to be authenticated. These users can inject arbitrary SQL statements through the Field parameter and thus modify tables from the database. This vulnerability is fixed in 7.1.0.	Patched by core rule	Y
CVE-2026-4079	SQL Chart Builder WordPress Plugin SQL Injection via Dynamic Filter	The SQL Chart Builder WordPress plugin before 2.3.8 does not properly escape user input as it is concatenated to SQL queries, making it possible for attackers to conduct SQL Injection attacks against the dynamic filter functionality.	Patched by core rule	Y
CVE-2026-35395	WeGIA SQL Injection via id_memorando in DespachoDAO.php	WeGIA is a Web manager for charitable institutions. Prior to 3.6.9, WeGIA contains a SQL injection vulnerability in dao/memorando/DespachoDAO.php. The id_memorando parameter is extracted from $_REQUEST without validation and directly interpolated into SQL queries, allowing any authenticated user to execute arbitrary SQL commands against the database. This vulnerability is fixed in 3.6.9.	Patched by core rule	Y
CVE-2026-35184	EcclesiaCRM SQL Injection via custom and value Parameters in queryview.php	EcclesiaCRM is CRM Software for church management. Prior to 8.0.0, there is a SQL injection vulnerability in v2/templates/query/queryview.php via the custom and value parameters. This vulnerability is fixed in 8.0.0.	Patched by core rule	Y
CVE-2026-35470	OpenSTAManager SQL Injection via righe Parameter in confronta_righe.php	OpenSTAManager is an open source management software for technical assistance and invoicing. Prior to 2.10.2,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		confronta_righe.php files across different modules in OpenSTAManager contain an SQL Injection vulnerability. The righe parameter received via $_GET['righe'] is directly concatenated into an SQL query without any sanitization, parameterization or validation. An authenticated attacker can inject arbitrary SQL statements to extract sensitive data from the database. This vulnerability is fixed in 2.10.2.		
CVE-2019-25704	Kados R10 GreenBee SQL Injection via filter_user_mail Parameter	Kados R10 GreenBee contains an SQL injection vulnerability that allows attackers to manipulate database queries by injecting SQL code through the filter_user_mail parameter. Attackers can send crafted requests with malicious SQL statements to extract sensitive database information or modify data.	Patched by core rule	Y
CVE-2019-25702	Kados R10 GreenBee SQL Injection via id_project Parameter	Kados R10 GreenBee contains an SQL injection vulnerability that allows attackers to manipulate database queries by injecting SQL code through the id_project parameter. Attackers can send crafted requests with malicious SQL statements in the id_project parameter to extract sensitive database information or modify data.	Patched by core rule	Y
CVE-2019-25700	Kados R10 GreenBee SQL Injection via sort_direction Parameter	Kados R10 GreenBee contains an SQL injection vulnerability that allows attackers to manipulate database queries by injecting SQL code through the sort_direction parameter. Attackers can submit malicious SQL statements in the sort_direction parameter to extract sensitive database information or modify data.	Patched by core rule	Y
CVE-2019-25698	Kados R10 GreenBee SQL Injection via id_to_delete Parameter	Kados R10 GreenBee contains an SQL injection vulnerability that allows attackers to manipulate database queries by injecting SQL code through the id_to_delete parameter. Attackers can send crafted requests with malicious SQL statements in the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		id_to_delete field to extract or modify sensitive database information.		
CVE-2019-25696	Kados R10 GreenBee SQL Injection via language_tag Parameter	Kados R10 GreenBee contains an SQL injection vulnerability that allows attackers to manipulate database queries by injecting SQL code through the language_tag parameter. Attackers can submit malicious SQL statements in the language_tag parameter to extract sensitive database information or modify data.	Patched by core rule	Y
CVE-2019-25694	Kados R10 GreenBee Unauthenticated SQL Injection via user2reset Parameter	Kados R10 GreenBee contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the user2reset parameter. Attackers can send crafted requests with malicious SQL payloads to extract sensitive database information or modify data.	Patched by core rule	Y
CVE-2019-25692	Kados R10 GreenBee SQL Injection via id_to_modify Parameter	Kados R10 GreenBee contains an SQL injection vulnerability that allows attackers to manipulate database queries by injecting SQL code through the id_to_modify parameter. Attackers can send crafted requests with malicious SQL statements in the id_to_modify field to extract sensitive database information or modify data.	Patched by core rule	Y
CVE-2019-25690	Kados R10 GreenBee SQL Injection via mng_profile_id Parameter	Kados R10 GreenBee contains an SQL injection vulnerability that allows attackers to manipulate database queries by injecting SQL code through the mng_profile_id parameter. Attackers can send crafted requests with malicious SQL payloads in the mng_profile_id parameter to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25688	Kados R10 GreenBee Unauthenticated SQL Injection via menu_lev1 Parameter	Kados R10 GreenBee contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the menu_lev1 parameter. Attackers can send crafted requests with	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		malicious SQL payloads in the menu_lev1 parameter to extract sensitive database information or modify database contents.		
CVE-2019-25684	OpenDocMan SQL Injection via where Parameter in search.php	OpenDocMan 1.3.4 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the where parameter. Attackers can send GET requests to search.php with malicious SQL payloads in the where parameter to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25680	Advance Gift Shop Pro Script SQL Injection via search Parameter	Advance Gift Shop Pro Script 2.0.3 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the search parameter. Attackers can submit crafted SQL payloads in the s parameter of search requests to extract sensitive database information including version details and other data.	Patched by core rule	Y
CVE-2019-25675	eDirectory SQL Injection via key Parameter Enabling Auth Bypass	eDirectory contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to bypass administrator authentication and disclose sensitive files by injecting SQL code into parameters. Attackers can exploit the key parameter in the login endpoint with union-based SQL injection to authenticate as administrator, then leverage authenticated file disclosure vulnerabilities in language_file.php to read arbitrary PHP files from the server.	Patched by core rule	Y
CVE-2019-25674	CMSsite SQL Injection via post Parameter in post.php	CMSsite 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the post parameter. Attackers can send GET requests to post.php with malicious post values to extract sensitive database information or perform time-based blind SQL injection attacks.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2019-25672	PilusCart SQL Injection via send Parameter in Comment Submission	PilusCart 1.4.1 contains a SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the send parameter. Attackers can submit POST requests to the comment submission endpoint with RLIKE-based boolean SQL injection payloads to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25669	qdPM SQL Injection via search_by_extrafields[] Parameter	qdPM 9.1 contains an SQL injection vulnerability that allows attackers to manipulate database queries by injecting SQL code through the search_by_extrafields[] parameter. Attackers can send POST requests to the users endpoint with malicious search_by_extrafields[] values to trigger SQL syntax errors and extract database information.	Patched by core rule	Y
CVE-2019-25668	News Website Script SQL Injection via News ID Parameter	News Website Script 2.0.5 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the news ID parameter. Attackers can send GET requests to index.php/show/news/ with malicious SQL statements to extract sensitive database information.	Patched by core rule	Y
CVE-2019-25664	SuiteCRM Blind SQL Injection via record Parameter in Users DetailView	SuiteCRM 7.10.7 contains a time-based SQL injection vulnerability in the record parameter of the Users module DetailView action that allows authenticated attackers to manipulate database queries. Attackers can append SQL code to the record parameter in GET requests to the index.php endpoint to extract sensitive database information through time-based blind SQL injection techniques.	Patched by core rule	Y
CVE-2019-25663	SuiteCRM SQL Injection via parentTab Parameter in Email Module	SuiteCRM 7.10.7 contains a SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		parentTab parameter. Attackers can send GET requests to the email module with malicious parentTab values using boolean-based SQL injection techniques to extract sensitive database information.		
CVE-2019-25662	ResourceSpace SQL Injection via ref Parameter in watched_searches.php	ResourceSpace 8.6 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the ref parameter. Attackers can send GET requests to the watched_searches.php endpoint with crafted SQL payloads to extract sensitive database information including usernames and credentials.	Patched by core rule	Y
CVE-2026-34934	PraisonAI SQL Injection via Malicious Thread ID in get_all_user_threads	PraisonAI is a multi-agent teams system. Prior to version 4.5.90, the get_all_user_threads function constructs raw SQL queries using f-strings with unescaped thread IDs fetched from the database. An attacker stores a malicious thread ID via update_thread. When the application loads the thread list, the injected payload executes and grants full database access. This issue has been patched in version 4.5.90.	Patched by core rule	Y
CVE-2026-34788	Emlog SQL Injection via updateTagName() in tag_model.php	Emlog is an open source website building system. In versions 2.6.2 and prior, a SQL injection vulnerability exists in include/model/tag_model.php at line 168. The updateTagName() function directly interpolates user input into the SQL query string without using parameterized queries or proper escaping, making it vulnerable to SQL injection attacks. At time of publication, there are no publicly available patches.	Patched by core rule	Y
CVE-2026-34612	Kestra SQL Injection to RCE via PostgreSQL COPY TO PROGRAM	Kestra is an open-source, event-driven orchestration platform. Prior to version 1.3.7, Kestra contains a SQL Injection vulnerability that leads to Remote Code Execution (RCE) in the GET /api/v1/main/flows/search	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		endpoint. The injected payload is executed by PostgreSQL using COPY ... TO PROGRAM ..., which runs arbitrary OS commands on the host. This issue has been patched in version 1.3.7.		
CVE-2026-27885	Piwigo SQL Injection via Activity List API Endpoint	Piwigo is an open source photo gallery application for the web. Prior to version 16.3.0, a SQL Injection vulnerability was discovered in Piwigo affecting the Activity List API endpoint. This vulnerability allows an authenticated administrator to extract sensitive data from the database, including user credentials, email addresses, and all stored content. This issue has been patched in version 16.3.0.	Patched by core rule	Y
CVE-2026-27834	Piwigo SQL Injection via filter Parameter in pwg.users.getList API	Piwigo is an open source photo gallery application for the web. Prior to version 16.3.0, a SQL Injection vulnerability exists in the pwg.users.getList Web Service API method. The filter parameter is directly concatenated into a SQL query without proper sanitization, allowing authenticated administrators to execute arbitrary SQL commands. This issue has been patched in version 16.3.0.	Patched by core rule	Y
CVE-2026-27634	Piwigo Unauthenticated SQL Injection via Date Filter Parameters	Piwigo is an open source photo gallery application for the web. Prior to version 16.3.0, the four date filter parameters (f_min_date_available, f_max_date_available, f_min_date_created, f_max_date_created) in ws_std_image_sql_filter() are concatenated directly into SQL without any escaping or type validation. This could result in an unauthenticated attacker reading the full database, including user password hashes. This issue has been patched in version 16.3.0.	Patched by core rule	Y
CVE-2026-34825	NocoBase SQL Injection via Template Variables in Workflow SQL Node	NocoBase is an AI-powered no-code/low-code platform for building business applications and enterprise solutions. Prior to version 2.0.30, NocoBase plugin-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		workflow-sql substitutes template variables directly into raw SQL strings via getParsedValue() without parameterization or escaping. Any user who triggers a workflow containing a SQL node with template variables from user-controlled data can inject arbitrary SQL. This issue has been patched in version 2.0.30.		
CVE-2026-35168	OpenSTAManager SQL Injection via Arbitrary SQL Execution in Aggiornamenti Module	OpenSTAManager is an open source management software for technical assistance and invoicing. Prior to version 2.10.2, the Aggiornamenti (Updates) module in OpenSTAManager contains a database conflict resolution feature (op=risolvi-conflitti-database) that accepts a JSON array of SQL statements via POST and executes them directly against the database without any validation, allowlist, or sanitization. An authenticated attacker with access to the Aggiornamenti module can execute arbitrary SQL statements including CREATE, DROP, ALTER, INSERT, UPDATE, DELETE, SELECT INTO OUTFILE, and any other SQL command supported by the MySQL server. This issue has been patched in version 2.10.2.	Patched by core rule	Y
CVE-2026-28805	OpenSTAManager Blind SQL Injection via options[stato] Parameter	OpenSTAManager is an open source management software for technical assistance and invoicing. Prior to version 2.10.2, multiple AJAX select handlers in OpenSTAManager are vulnerable to Time-Based Blind SQL Injection through the options[stato] GET parameter. The user-supplied value is read from $superselect['stato'] and concatenated directly into SQL WHERE clauses as a bare expression, without any sanitization, parameterization, or allowlist validation. An authenticated attacker can inject arbitrary SQL statements to extract sensitive data from the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		database. This issue has been patched in version 2.10.2.		
CVE-2026-34455	Hi.Events SQL Injection via sort_by Parameter in Repository Classes	Hi.Events is an open-source event management and ticket selling platform. From version 0.8.0-beta.1 to before version 1.7.1-beta, multiple repository classes pass the user-supplied sort_by query parameter directly to Eloquent's orderBy() without validation, enabling SQL injection. The application uses PostgreSQL which supports stacked queries. This issue has been patched in version 1.7.1-beta.	Patched by core rule	Y
CVE-2026-30520	SourceCodester Loan Management Blind SQL Injection via borrower_id	A Blind SQL Injection vulnerability exists in SourceCodester Loan Management System v1.0. The vulnerability is located in the ajax.php file (specifically the save_loan action). The application fails to properly sanitize user input supplied to the borrower_id parameter in a POST request, allowing an authenticated attacker to inject malicious SQL commands.	Patched by core rule	Y
CVE-2026-32714	SciTokens SQL Injection via issuer and key_id in KeyCache Class	SciTokens is a reference library for generating and using SciTokens. Prior to version 1.9.6, the KeyCache class in scitokens was vulnerable to SQL Injection because it used Python's str.format() to construct SQL queries with user-supplied data (such as issuer and key_id). This allowed an attacker to execute arbitrary SQL commands against the local SQLite database. This issue has been patched in version 1.9.6.	Patched by core rule	Y
CVE-2026-33643	SchemaHero SQL Injection via column in mysqlColumnAsInsert	SQL Injection vulnerability in SchemaHero 0.23.0 via the column parameter to the mysqlColumnAsInsert function in file plugins/mysql/lib/column.go.	Patched by core rule	Y
CVE-2026-29953	SchemaHero SQL Injection via column in columnAsInsert (PostgreSQL)	SQL Injection vulnerability in SchemaHero 0.23.0 via the column parameter to the columnAsInsert function in file plugins/postgres/lib/column.go.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-33991	WeGIA SQL Injection via id_tag in deletar_tag.php via extract($_REQUEST)	WeGIA is a web manager for charitable institutions. Prior to version 3.6.7, the file html/socio/sistema/deletar_tag.php uses extract($_REQUEST) on line 14 and directly concatenates the $id_tag variable into SQL queries on lines 16-17 without prepared statements or sanitization. Version 3.6.7 patches the vulnerability.	Patched by core rule	Y
CVE-2026-34374	WWBN AVideo SQL Injection via Stream Key in Live_schedule::keyExists()	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the Live_schedule::keyExists() method constructs a SQL query by interpolating a stream key directly into the query string without parameterization. This method is called as a fallback from LiveTransmition::keyExists() when the initial parameterized lookup returns no results. Although the calling function correctly uses parameterized queries for its own lookup, the fallback path undoes this protection entirely. As of time of publication, no patched versions are available.	Patched by core rule	Y
CVE-2026-33770	WWBN AVideo SQL Injection via clean_title in fixCleanTitle() in category.php	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the fixCleanTitle() static method in objects/category.php constructs a SQL SELECT query by directly interpolating both $clean_title and $id into the query string without using prepared statements or parameterized queries. An attacker who can trigger category creation or renaming with a crafted title value can inject arbitrary SQL. Commit 994cc2b3d802b819e07e6088338e8bf4e484aae4 contains a patch.	Patched by core rule	Y
CVE-2026-33767	WWBN AVideo SQL Injection via videos_id in getLike() in like.php	WWBN AVideo is an open source video platform. In versions up to and including 26.0, in objects/like.php, the getLike() method constructs a SQL query using a prepared statement placeholder for users_id but	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		directly concatenates $this->videos_id into the query string without parameterization. An attacker who can control the videos_id value can inject arbitrary SQL, bypassing the partial prepared-statement protection. Commit 0215d3c4f1ee748b8880254967b51784b8ac4080 contains a patch.		
CVE-2026-30534	SourceCodester Online Food Ordering SQL Injection via id in manage_category.php	A SQL Injection vulnerability exists in SourceCodester Online Food Ordering System v1.0 in admin/manage_category.php via the id parameter.	Patched by core rule	Y
CVE-2026-30533	SourceCodester Online Food Ordering SQL Injection via id in manage_product.php	A SQL Injection vulnerability exists in SourceCodester Online Food Ordering System v1.0 in the admin/manage_product.php file via the id parameter.	Patched by core rule	Y
CVE-2026-30532	SourceCodester Online Food Ordering SQL Injection via id in view_product.php	A SQL Injection vulnerability exists in SourceCodester Online Food Ordering System v1.0 in the admin/view_product.php file via the id parameter.	Patched by core rule	Y
CVE-2026-30531	SourceCodester Online Food Ordering SQL Injection via name in save_category	A SQL Injection vulnerability exists in SourceCodester Online Food Ordering System v1.0 in the Actions.php file (specifically the save_category action). The application fails to properly sanitize user input supplied to the name parameter. This allows an authenticated attacker to inject malicious SQL commands.	Patched by core rule	Y
CVE-2026-30530	SourceCodester Online Food Ordering SQL Injection via username in save_customer	A SQL Injection vulnerability exists in SourceCodester Online Food Ordering System v1.0 in the Actions.php file (specifically the save_customer action). The application fails to properly sanitize user input supplied to the username parameter. This allows an attacker to inject malicious SQL commands.	Patched by core rule	Y
CVE-2026-30529	SourceCodester Online Food Ordering SQL Injection via username in save_user	A SQL Injection vulnerability exists in SourceCodester Online Food Ordering System v1.0 in the Actions.php file (specifically the save_user action). The application	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		fails to properly sanitize user input supplied to the username parameter. This allows an authenticated attacker to inject malicious SQL commands.		
CVE-2026-33755	Group-Office SQL Injection via JMAP Contact/query Enabling Session Takeover	Group-Office is an enterprise customer relationship management and groupware tool. Prior to versions 6.8.158, 25.0.92, and 26.0.17, an authenticated SQL Injection vulnerability in the JMAP Contact/query endpoint allows any authenticated user with basic addressbook access to extract arbitrary data from the database including active session tokens of other users. This enables full account takeover of any user, including the System Administrator, without knowing their password. Versions 6.8.158, 25.0.92, and 26.0.17 fix the issue.	Patched by core rule	Y
CVE-2026-33545	MobSF SQL Injection via Malicious SQLite Table Name in read_sqlite()	MobSF is a mobile application security testing tool. Prior to version 4.4.6, MobSF's read_sqlite() function in mobsf/MobSF/utils.py uses Python string formatting to construct SQL queries with table names read from a SQLite database's sqlite_master table. When a security analyst uses MobSF to analyze a malicious mobile application containing a crafted SQLite database, attacker-controlled table names are interpolated directly into SQL queries without parameterization or escaping. This allows an attacker to cause denial of service and achieve SQL injection. Version 4.4.6 patches the issue.	Patched by core rule	Y
CVE-2026-33153	Tandoor Recipes SQL Schema Disclosure via Hidden debug=true Parameter	Tandoor Recipes is an application for managing recipes, planning meals, and building shopping lists. In versions prior to 2.6.0, the Recipe API endpoint exposes a hidden ?debug=true query parameter that returns the complete raw SQL query being executed, including all table names, column names, JOIN	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		relationships, WHERE conditions, and multi-tenant space IDs. This parameter works even when Django's DEBUG=False (production mode) and is accessible to any authenticated user regardless of their privilege level. This allows a low-privilege attacker to map the entire database schema. Version 2.6.0 patches the issue.		
CVE-2026-30463	FuelCMS SQL Injection via /controllers/Login.php	Daylight Studio FuelCMS v1.5.2 was discovered to contain a SQL injection vulnerability via the /controllers/Login.php component.	Patched by core rule	Y
CVE-2026-33468	Kysely SQL Injection via Backslash Escape Bypass in sanitizeStringLiteral (MySQL)	Kysely is a type-safe TypeScript SQL query builder. Prior to version 0.28.14, Kysely's DefaultQueryCompiler.sanitizeStringLiteral() only escapes single quotes by doubling them but does not escape backslashes. When used with the MySQL dialect (where NO_BACKSLASH_ESCAPES is OFF by default), an attacker can use a backslash to escape the trailing quote of a string literal, breaking out of the string context and injecting arbitrary SQL. This affects CreateIndexBuilder.where() and CreateViewBuilder.as(). Version 0.28.14 contains a fix.	Patched by core rule	Y
CVE-2026-33442	Kysely SQL Injection via Backslash in JSON Path String Literal (MySQL)	Kysely is a type-safe TypeScript SQL query builder. In versions 0.28.12 and 0.28.13, the sanitizeStringLiteral method in Kysely's query compiler escapes single quotes but does not escape backslashes. On MySQL with the default BACKSLASH_ESCAPES SQL mode, an attacker can inject a backslash before a single quote to neutralize the escaping, breaking out of the JSON path string literal and injecting arbitrary SQL. Version 0.28.14 fixes the issue.	Patched by core rule	Y
CVE-2018-25209	OpenBiz Cubi Lite SQL Injection via username in Login Form	OpenBiz Cubi Lite 3.0.8 contains a SQL injection vulnerability in the login form that allows	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		unauthenticated attackers to manipulate database queries through the username parameter. Attackers can submit POST requests to /bin/controller.php with malicious SQL code in the username field to extract sensitive database information or bypass authentication.		
CVE-2018-25208	qdPM SQL Injection via filter_by Parameters in timeReport Endpoint	qdPM 9.1 contains an SQL injection vulnerability that allows unauthenticated attackers to extract database information by injecting SQL code through filter_by parameters. Attackers can submit malicious POST requests to the timeReport endpoint with crafted filter_by[CommentCreatedFrom] and filter_by[CommentCreatedTo] parameters to execute arbitrary SQL queries and retrieve sensitive data.	Patched by core rule	Y
CVE-2018-25207	Online Quiz Maker SQL Injection via catid and usern Parameters	Online Quiz Maker 1.0 contains SQL injection vulnerabilities in the catid and usern parameters that allow authenticated attackers to execute arbitrary SQL commands. Attackers can submit malicious POST requests to quiz-system.php or add-category.php with crafted SQL payloads in POST parameters to extract sensitive database information or bypass authentication.	Patched by core rule	Y
CVE-2018-25206	KomSeo Cart SQL Injection via my_item_search Parameter in edit.php	KomSeo Cart 1.3 contains an SQL injection vulnerability that allows attackers to inject SQL commands through the my_item_search parameter in edit.php. Attackers can submit POST requests with malicious SQL payloads to extract sensitive database information using boolean-based blind or error-based injection techniques.	Patched by core rule	Y
CVE-2018-25205	ASP.NET jVideo Kit SQL Injection via query Parameter in Search	ASP.NET jVideo Kit 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to inject SQL commands through the query parameter in the search functionality. Attackers can submit malicious SQL payloads via GET or POST requests to the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/search endpoint to extract sensitive database information using boolean-based blind or error-based techniques.		
CVE-2018-25204	Library CMS SQL Injection via username Parameter Enabling Auth Bypass	Library CMS 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to bypass authentication by injecting SQL code through the username parameter. Attackers can send POST requests to the admin login endpoint with boolean-based blind SQL injection payloads in the username field to manipulate database queries and gain unauthorized access.	Patched by core rule	Y
CVE-2018-25203	Online Store System CMS SQL Injection via email Parameter	Online Store System CMS 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the email parameter. Attackers can send POST requests to index.php with the action=clientaccess parameter using boolean-based blind or time-based blind SQL injection payloads in the email field to extract sensitive database information.	Patched by core rule	Y
CVE-2018-25202	SAT CFDI SQL Injection via id Parameter in signIn Endpoint	SAT CFDI 3.3 contains an SQL injection vulnerability that allows attackers to manipulate database queries by injecting SQL code through the id parameter in the signIn endpoint. Attackers can submit POST requests with boolean-based blind, stacked queries, or time-based blind SQL injection payloads to extract sensitive data or compromise the application.	Patched by core rule	Y
CVE-2018-25201	School Management System CMS SQL Injection via username Enabling Auth Bypass	School Management System CMS 1.0 contains an SQL injection vulnerability in the admin login functionality that allows attackers to bypass authentication by injecting SQL code through the username parameter. Attackers can submit malicious payloads using boolean-based blind SQL injection techniques to the processlogin endpoint to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		authenticate as administrator without valid credentials.		
CVE-2018-25195	Wecodex Hotel CMS SQL Injection via username in processlogin	Wecodex Hotel CMS 1.0 contains an SQL injection vulnerability in the admin login functionality that allows unauthenticated attackers to bypass authentication by injecting SQL code. Attackers can submit malicious SQL payloads through the username parameter in POST requests to index.php with action=processlogin to extract sensitive database information or gain unauthorized administrative access.	Patched by core rule	Y
CVE-2018-25185	Wecodex Restaurant CMS SQL Injection via username in Login Endpoint	Wecodex Restaurant CMS 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the username parameter. Attackers can send POST requests to the login endpoint with malicious SQL payloads using boolean-based blind or time-based blind techniques to extract sensitive database information.	Patched by core rule	Y
CVE-2018-25183	Shipping System CMS SQL Injection via username Enabling Auth Bypass	Shipping System CMS 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to bypass authentication by injecting SQL code through the username parameter. Attackers can submit malicious SQL payloads using boolean-based blind techniques in POST requests to the admin login endpoint to authenticate without valid credentials.	Patched by core rule	Y
CVE-2026-33917	OpenEMR SQL Injection via ajax_save in CAMOS Form	OpenEMR is a free and open source electronic health records and medical practice management application. Versions prior to 8.0.0.3 contain a SQL injection vulnerability in the ajax_save CAMOS form that can be exploited by authenticated attackers. The vulnerability exists due to insufficient input validation in the ajax_save page in the CAMOS form. Version 8.0.0.3 patches the issue.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-33914	OpenEMR Blind SQL Injection via dels Parameter in PostCalendar categoriesUpdate	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0.3, the PostCalendar module contains a blind SQL injection vulnerability in the categoriesUpdate administrative function. The dels POST parameter is read via pnVarCleanFromInput(), which only strips HTML tags and performs no SQL escaping. The value is then interpolated directly into a raw SQL DELETE statement executed unsanitized via Doctrine DBAL's executeStatement(). Version 8.0.0.3 patches the issue.	Patched by core rule	Y
CVE-2026-33910	OpenEMR SQL Injection via Patient Selection Feature	OpenEMR is a free and open source electronic health records and medical practice management application. Versions up to and including 8.0.0.2 contain a SQL injection vulnerability in the patient selection feature that can be exploited by authenticated attackers. The vulnerability exists due to insufficient input validation in the patient selection feature. Version 8.0.0.3 contains a patch.	Patched by core rule	Y
CVE-2026-29187	OpenEMR Blind SQL Injection via HTTP Parameter Keys in Patient Search	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0.3, a Blind SQL Injection vulnerability exists in the Patient Search functionality (/interface/new/new_search_popup.php). The vulnerability allows an authenticated attacker to execute arbitrary SQL commands by manipulating the HTTP parameter keys rather than the values. Version 8.0.0.3 contains a patch.	Patched by core rule	Y

VULNERABILITY DETAILS

Server-Side Request Forgery (SSRF) Vulnerabilities

SSRF vulnerabilities allow attackers to induce the server to make HTTP requests to arbitrary internal or external targets, enabling internal network reconnaissance, cloud metadata exfiltration, and lateral movement. All 74 SSRF CVEs in April 2026 are patched by AppTrana core rules.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-42038	Axios SSRF via Incomplete no_proxy Hostname Normalization for Loopback Addresses	Axios is a promise based HTTP client for the browser and Node.js. Prior to 1.15.1 and 0.31.1, the fix for no_proxy hostname normalization bypass is incomplete. When no_proxy=localhost is set, requests to 127.0.0.1 and [::1] still route through the proxy instead of bypassing it. The shouldBypassProxy() function does pure string matching and does not resolve IP aliases or loopback equivalents. This vulnerability is fixed in 1.15.1 and 0.31.1.	Patched by core rule	Y
CVE-2026-41272	Flowise SSRF via DNS Rebinding and Default Configuration Bypass in secureAxiosRequest/ secureFetch	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, the core security wrappers (secureAxiosRequest and secureFetch) intended to prevent Server-Side Request Forgery contain multiple logic flaws. These flaws allow attackers to bypass the allow/deny lists via DNS Rebinding (TOCTOU) or by exploiting the default configuration which fails to enforce any deny list. This vulnerability is fixed in 3.1.0.	Patched by core rule	Y
CVE-2026-41271	Flowise SSRF via Malicious Prompt Templates in	Flowise is a drag & drop user interface to build a customized large language model flow.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	POST/GET API Chain Components	Prior to 3.1.0, a Server-Side Request Forgery vulnerability exists in FlowiseAI's POST/GET API Chain components that allows unauthenticated attackers to force the server to make arbitrary HTTP requests to internal and external systems. By injecting malicious prompt templates, attackers can bypass the intended API documentation constraints and redirect requests to sensitive internal services, potentially leading to internal network reconnaissance and data exfiltration. This vulnerability is fixed in 3.1.0.		
CVE-2026-41060	WWBN AVideo SSRF via Same-Domain Shortcircuit Bypassing isSSRFSafeURL() on Non-Standard Ports	WWBN AVideo is an open source video platform. In versions 29.0 and below, the isSSRFSafeURL() function in objects/functions.php contains a same-domain shortcircuit that allows any URL whose hostname matches webSiteRootURL to bypass all SSRF protections. Because the check compares only the hostname and ignores the port, an attacker can reach arbitrary ports on the AVideo server by using the site's public hostname with a non-standard port. The response body is saved to a web-accessible path, enabling full exfiltration. Commit a0156a6398362086390d949190f9d52a823000ba fixes the issue.	Patched by core rule	Y
CVE-2026-41055	WWBN AVideo SSRF via DNS TOCTOU in LiveLinks Proxy	WWBN AVideo is an open source video platform. In versions 29.0 and below,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Despite isSSRFSafeURL() Validation	an incomplete SSRF fix in AVideo's LiveLinks proxy adds isSSRFSafeURL() validation but leaves DNS TOCTOU vulnerabilities where DNS rebinding between validation and the actual HTTP request redirects traffic to internal endpoints. Commit 8d8fc0cadb425835b4861036d589abcea4d78ee8 contains an updated fix.		
CVE-2026-35587	Glances SSRF via public_api Config Parameter in IP Plugin with Credential Leakage	Glances is an open-source system cross-platform monitoring tool. Prior to version 4.5.4, a Server-Side Request Forgery vulnerability exists in the Glances IP plugin due to improper validation of the public_api configuration parameter. The value of public_api is used directly in outbound HTTP requests without any scheme restriction or hostname/IP validation. Additionally, when public_username and public_password are set, Glances automatically includes these credentials in the Authorization: Basic header, resulting in credential leakage to attacker-controlled servers. Version 4.5.4 contains a patch.	Patched by core rule	Y
CVE-2026-33626	LMDeploy SSRF via Unvalidated URLs in load_image() Vision-Language Module	LMDeploy is a toolkit for compressing, deploying, and serving large language models. Versions prior to 0.12.3 have a Server-Side Request Forgery vulnerability in LMDeploy's vision-language module. The load_image() function in lmdeploy/vl/utils.py fetches arbitrary URLs without validating internal/private IP addresses, allowing	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attackers to access cloud metadata services, internal networks, and sensitive resources. Version 0.12.3 patches the issue.		
CVE-2026-40348	Movary Authenticated SSRF via Unvalidated URL in Jellyfin Server Verify Endpoint	Movary is a self hosted web app to track and rate a user's watched movies. Prior to version 0.71.1, an ordinary authenticated user can trigger server-side requests to arbitrary internal targets through POST /settings/jellyfin/server-url-verify. The endpoint accepts a user-controlled URL, appends /system/info/public, and sends a server-side HTTP request with Guzzle. Because there is no restriction on internal hosts, loopback addresses, or private network ranges, this enables SSRF-based internal reconnaissance including host discovery, port-state probing, and service fingerprinting. Version 0.71.1 fixes the issue.	Patched by core rule	Y
CVE-2026-40516	OpenHarness SSRF via web_fetch and web_search Tool Parameters Without Address Validation	OpenHarness before commit bd4df81 contains a server-side request forgery vulnerability in the web_fetch and web_search tools that allows attackers to access private and localhost HTTP services by manipulating tool parameters without proper validation of target addresses. Attackers can influence an agent session to invoke these tools against loopback, RFC1918, link-local, or other non-public addresses to read response bodies from local development	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		services, cloud metadata endpoints, admin panels, or other private HTTP services reachable from the victim host.		
CVE-2026-35032	Jellyfin SSRF and Local File Read via Unvalidated LiveTV M3U Tuner URL	Jellyfin is an open source self hosted media server. Versions prior to 10.11.7 contain a vulnerability chain in the LiveTV M3U tuner endpoint (POST /LiveTv/TunerHosts), where the tuner URL is not validated, allowing local file read via non-HTTP paths and Server-Side Request Forgery via HTTP URLs. This is exploitable by any authenticated user because the EnableLiveTvManagement permission defaults to true for all new users. An attacker can chain these vulnerabilities to exfiltrate the database and extract admin session tokens. This issue has been fixed in version 10.11.7.	Patched by core rule	Y
CVE-2026-34225	Open WebUI Blind SSRF via Unvalidated URL in Image Edit Prompt Endpoint	Open WebUI is a self-hosted artificial intelligence platform. Versions 0.7.2 and below contain a Blind Server Side Request Forgery in the functionality that allows editing an image via a prompt. The affected function performs a GET request to a user-provided URL with no restriction on the domain, allowing the local address space to be accessed. Since the SSRF is blind, the primary impact is port scanning of the local network. This issue was unresolved at the time of publication.	Patched by core rule	Y
CVE-2026-33659	EspoCRM SSRF via DNS Rebinding TOCTOU in	EspoCRM is an open source customer relationship management application. In versions	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	fromImageUrl Attachment Endpoint	9.3.3 and below, the POST /api/v1/Attachment/fromImageUrl endpoint is vulnerable to Server-Side Request Forgery via a DNS rebinding (TOCTOU) condition. Host validation uses dns_get_record() but the actual HTTP request resolves hostnames through curl's internal resolver (gethostbyname()), allowing the two lookups to return different IP addresses. A secondary issue exists where an empty DNS result causes the validation to implicitly allow the host without further checks. This issue has been fixed in version 9.3.4.		
CVE-2026-33534	EspoCRM SSRF via Octal IP Notation Bypassing filter_var FILTER_VALIDATE_IP	EspoCRM is an open source customer relationship management application. Versions 9.3.3 and below have an authenticated Server-Side Request Forgery vulnerability that allows bypassing the internal-host validation logic by using alternative IPv4 representations such as octal notation (e.g., 0177.0.0.1 instead of 127.0.0.1). This is caused by HostCheck::isNotInternalHost() relying on PHP's filter_var(..., FILTER_VALIDATE_IP), which does not recognize alternative IP formats. Through the confirmed /api/v1/Attachment/fromImageUrl endpoint, an authenticated user can force the server to make requests to loopback-only services. This issue has been fixed in version 9.3.4.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-6111	MetaGPT SSRF via img_url_or_b64 in decode_image() in common.py	A security flaw has been discovered in FoundationAgents MetaGPT up to 0.8.1. This impacts the function decode_image of the file metagpt/utils/common.py. The manipulation of the argument img_url_or_b64 results in server-side request forgery. It is possible to launch the attack remotely. The exploit has been released to the public and may 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-2026-40242	Arcane Unauthenticated SSRF via url Parameter in /api/templates/fetch Endpoint	Arcane is an interface for managing Docker containers, images, networks, and volumes. Prior to 1.17.3, the /api/templates/fetch endpoint accepts a caller-supplied url parameter and performs a server-side HTTP GET request to that URL without authentication and without URL scheme or host validation. The server's response is returned directly to the caller. This constitutes an unauthenticated SSRF vulnerability affecting any publicly reachable Arcane instance. This vulnerability is fixed in 1.17.3.	Patched by core rule	Y
CVE-2026-40168	Postiz SSRF via HTTP Redirect Bypass in /api/public/stream Endpoint	Postiz is an AI social media scheduling tool. Prior to 2.21.5, the /api/public/stream endpoint is vulnerable to SSRF. Although the application validates the initially supplied URL and blocks direct private/internal hosts, it does not re-validate the final destination after	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		HTTP redirects. As a result, an attacker can supply a public HTTPS URL that passes validation and then redirects the server-side request to an internal resource.		
CVE-2026-40160	PraisonAI SSRF via web_crawl httpx Fallback Path Without Host Validation	PraisonAIAgents is a multi-agent teams system. Prior to 1.5.128, web_crawl's httpx fallback path passes user-supplied URLs directly to httpx.AsyncClient.get() with follow_redirects=True and no host validation. An LLM agent tricked into crawling an internal URL can reach cloud metadata endpoints (169.254.169.254), internal services, and localhost. The response content is returned to the agent and may appear in output visible to the attacker. This vulnerability is fixed in 1.5.128.	Patched by core rule	Y
CVE-2026-6011	OpenClaw SSRF via assertPublicHostname Handler in web-fetch.ts	A weakness has been identified in OpenClaw up to 2026.1.26. Affected by this issue is some unknown functionality of the file src/agents/tools/web-fetch.ts of the component assertPublicHostname Handler. Executing a manipulation can lead to server-side request forgery. The attack can be executed remotely. Upgrading to version 2026.1.29 can resolve this issue.	Patched by core rule	Y
CVE-2026-40150	PraisonAI SSRF via web_crawl() Accepting Arbitrary URLs Including file:// Without Validation	PraisonAIAgents is a multi-agent teams system. Prior to 1.5.128, the web_crawl() function in praisonaiagents/tools/web_crawl_tools.py accepts arbitrary URLs from AI	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		agents with zero validation. No scheme allowlisting, hostname/IP blocklisting, or private network checks are applied before fetching. This allows an attacker or prompt injection in crawled content to force the agent to fetch cloud metadata endpoints, internal services, or local files via file:// URLs. This vulnerability is fixed in 1.5.128.		
CVE-2026-40114	PraisonAI SSRF via Unvalidated webhook_url in /api/v1/runs Endpoint	PraisonAI is a multi-agent teams system. Prior to 4.5.128, the /api/v1/runs endpoint accepts an arbitrary webhook_url in the request body with no URL validation. When a submitted job completes, the server makes an HTTP POST request to this URL using httpx.AsyncClient. An unauthenticated attacker can use this to make the server send POST requests to arbitrary internal or external destinations, enabling SSRF against cloud metadata services, internal APIs, and other network-adjacent services. This vulnerability is fixed in 4.5.128.	Patched by core rule	Y
CVE-2026-40107	SiYuan SSRF via Mermaid img src UNC Path Triggering NTLMv2 Hash Exfiltration on Windows	SiYuan is a personal knowledge management system. Prior to 3.6.4, SiYuan configures Mermaid.js with securityLevel: loose and htmlLabels: true. In this mode, img tags with src attributes survive Mermaid's internal DOMPurify and land in SVG foreignObject blocks. The SVG is injected via innerHTML with no secondary sanitization. On Windows, a protocol-relative URL	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		(//attacker.com/image.png) resolves as a UNC path. Windows attempts SMB authentication automatically, sending the victim's NTLMv2 hash to the attacker. This vulnerability is fixed in 3.6.4.		
CVE-2026-39843	Plane SSRF via Unvalidated Favicon Fetch Redirect in Add Link Feature	Plane is an open-source project management tool. From 0.28.0 to before 1.3.0, the remediation of GHSA-jcc6-f9v6-f7jw is incomplete. Redirects for the main page URL are validated, but not the favicon fetch path. fetch_and_encode_favicon() still uses requests.get(favicon_url) with the default redirect-following. An authenticated attacker with low privileges can supply an HTML page with a link tag whose href redirects to a private IP address. This vulnerability is fixed in 1.3.0.	Patched by core rule	Y
CVE-2025-62718	Axios SSRF via NO_PROXY Bypass for localhost. Trailing Dot and IPv6 Loopback	Axios is a promise based HTTP client for the browser and Node.js. Prior to 1.15.0 and 0.31.0, Axios does not correctly handle hostname normalization when checking NO_PROXY rules. Requests to loopback addresses like localhost. (with a trailing dot) or [::1] (IPv6 literal) skip NO_PROXY matching and go through the configured proxy. This leads to the possibility of proxy bypass and SSRF vulnerabilities allowing attackers to reach sensitive loopback or internal services despite the configured protections. This vulnerability is fixed in 1.15.0 and 0.31.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-39885	FrontMCP SSRF via $ref Pointers in OpenAPI Spec Fetched Without URL Restrictions	FrontMCP is a TypeScript-first framework for the Model Context Protocol. Prior to 2.3.0, the mcp-from-openapi library uses @apidevtools/json-schema-ref-parser to dereference $ref pointers in OpenAPI specifications without configuring any URL restrictions or custom resolvers. A malicious OpenAPI specification containing $ref values pointing to internal network addresses, cloud metadata endpoints, or local files will cause the library to fetch those resources during the initialize() call. This vulnerability is fixed in 2.3.0.	Patched by core rule	Y
CVE-2026-39376	FastFeedParser SSRF via Unbounded meta-refresh Redirect Recursion in parse()	FastFeedParser is a high performance RSS, Atom and RDF parser. Prior to 0.5.10, when parse() fetches a URL that returns an HTML page containing a meta http-equiv=refresh tag, it recursively calls itself with the redirect URL with no depth limit, no visited-URL deduplication, and no redirect count cap. An attacker-controlled server that returns an infinite chain of HTML meta-refresh responses causes unbounded recursion, exhausting the Python call stack and crashing the process. This vulnerability can also be chained with the companion SSRF issue to reach internal network targets. This vulnerability is fixed in 0.5.10.	Patched by core rule	Y
CVE-2026-39361	OpenObserve SSRF via IPv6 Bracket Notation Bypassing validate_enrichment_url	OpenObserve is a cloud-native observability platform. In 0.70.3 and earlier, the validate_enrichment_url function fails to block	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		IPv6 addresses because Rust's url crate returns them with surrounding brackets (e.g. [::1] not ::1). An authenticated attacker can reach internal services blocked from external access. On cloud deployments this enables retrieval of IAM credentials via AWS IMDSv1 (169.254.169.254), GCP metadata, or Azure IMDS.		
CVE-2026-35572	ChurchCRM SSRF via Crafted Referer Header Triggering Outbound HTTP Request	ChurchCRM is an open-source church management system. Prior to 6.5.3, it is possible to trigger server-side HTTP/HTTPS requests to arbitrary hosts by supplying a crafted URL in the Referer request header. The server subsequently makes an outbound request to the attacker-controlled domain. This vulnerability is fixed in 6.5.3.	Patched by core rule	Y
CVE-2026-35516	LinkAce SSRF via Internal Hostname Bypass in Link Update and checkLink Without IP Filtering	LinkAce is a self-hosted archive to collect website links. Prior to 2.5.4, LinkRepository::update and CheckLinksCommand::checkLink do not check for private IPs. An authenticated user can read responses from internal services (AWS IMDSv1, cloud metadata, internal APIs) by creating a link with a public URL and then updating it to a private IP. The links:check cron job makes the request server-side without IP filtering. This vulnerability is fixed in 2.5.4.	Patched by core rule	Y
CVE-2026-35486	text-generation-webui SSRF via Unvalidated URLs in superbooga/superbo	text-generation-webui is an open-source web interface for running Large Language Models. Prior to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	ogav2 RAG Extensions	4.3, the superbooga and superboogav2 RAG extensions fetch user-supplied URLs via requests.get() with zero validation - no scheme check, no IP filtering, no hostname allowlist. An attacker can access cloud metadata endpoints, steal IAM credentials, and probe internal services. The fetched content is exfiltrated through the RAG pipeline. This vulnerability is fixed in 4.3.		
CVE-2026-35461	Papra SSRF via Unvalidated Webhook URLs Including localhost and Cloud Metadata Endpoints	Papra is a minimalistic document management and archiving platform. Prior to 26.4.0, the Papra webhook system allows authenticated users to register arbitrary URLs as webhook endpoints with no validation of the destination address. The server makes outbound HTTP POST requests to registered URLs, including localhost, internal network ranges, and cloud provider metadata endpoints, on every document event. This vulnerability is fixed in 26.4.0.	Patched by core rule	Y
CVE-2025-15611	Popup Box WordPress Plugin CSRF via Missing Nonce Validation in add_or_edit_popupbox()	The Popup Box WordPress plugin before 5.5.0 does not properly validate nonces in the add_or_edit_popupbox() function before saving popup data, allowing unauthenticated attackers to perform Cross-Site Request Forgery attacks. When an authenticated admin visits a malicious page, the attacker can create or modify popups with arbitrary JavaScript that executes in the admin panel and frontend.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-35459	pyLoad SSRF via HTTP Redirect Bypass Circumventing CVE-2026-33992 IP Validation Fix	pyLoad is a free and open-source download manager written in Python. In 0.5.0b3.dev96 and earlier, pyLoad has a server-side request forgery vulnerability. The fix for CVE-2026-33992 added IP validation to BaseDownloader.download() that checks the hostname of the initial download URL. However, pycurl is configured with FOLLOWLOCATION=1 and MAXREDIRS=10, causing it to automatically follow HTTP redirects. Redirect targets are never validated against the SSRF filter. An authenticated user with ADD permission can bypass the SSRF fix by submitting a URL that redirects to an internal address.	Patched by core rule	Y
CVE-2026-35187	pyLoad SSRF via parse_urls API Fetching Arbitrary URLs Including file:// and gopher://	pyLoad is a free and open-source download manager written in Python. In 0.5.0b3.dev96 and earlier, the parse_urls API function fetches arbitrary URLs server-side via get_url(url) (pycurl) without any URL validation, protocol restriction, or IP blacklist. An authenticated user with ADD permission can make HTTP/HTTPS requests to internal network resources and cloud metadata endpoints, read local files via file:// protocol, interact with internal services via gopher:// and dict:// protocols, and enumerate file existence via error-based oracle.	Patched by core rule	Y
CVE-2026-35037	Ech0 Unauthenticated SSRF via website_url Parameter in	Ech0 is an open-source, self-hosted publishing platform. Prior to 4.2.8, the GET /api/website/title	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	/api/website/title Endpoint	endpoint accepts an arbitrary URL via the website_url query parameter and makes a server-side HTTP request to it without any validation of the target host or IP address. The endpoint requires no authentication. An attacker can use this to reach internal network services, cloud metadata endpoints (169.254.169.254), and localhost-bound services. This vulnerability is fixed in 4.2.8.		
CVE-2026-35036	Ech0 SSRF via Unauthenticated /api/website/title with InsecureSkipVerify and Full Response Body Read	Ech0 is an open-source, self-hosted publishing platform. Prior to 4.2.8, the link preview route GET /api/website/title is unauthenticated, accepts a fully attacker-controlled URL, performs a server-side GET, reads the entire response body into memory via io.ReadAll. There is no host allowlist, no SSRF filter, and InsecureSkipVerify: true on the outbound client. Anyone who can reach the instance can force the Ech0 server to open HTTP/HTTPS URLs of their choice. This vulnerability is fixed in 4.2.8.	Patched by core rule	Y
CVE-2026-34981	whisperX API SSRF via download_from_url() With Zero URL Validation and Extension Bypass	The whisperX API is a tool for enhancing and analyzing audio content. From 0.3.1 to 0.5.0, FileService.download_from_url() in app/services/file_service.py calls requests.get(url) with zero URL validation. The file extension check occurs AFTER the HTTP request is already made, and can be bypassed by appending .mp3 to any internal URL. The /speech-to-text-url	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		endpoint is unauthenticated. This vulnerability is fixed in 0.6.0.		
CVE-2026-33752	curl_cffi SSRF via Unrestricted Internal IP Access with Automatic Redirect Following	curl_cffi is a Python binding for curl. Prior to 0.15.0, curl_cffi does not restrict requests to internal IP ranges, and follows redirects automatically via the underlying libcurl. An attacker-controlled URL can redirect requests to internal services such as cloud metadata endpoints. In addition, curl_cffi's TLS impersonation feature can make these requests appear as legitimate browser traffic, which may bypass certain network controls. This vulnerability is fixed in 0.15.0.	Patched by core rule	Y
CVE-2026-33540	Distribution SSRF via Unvalidated WWW-Authenticate realm URL Sending Upstream Credentials	Distribution is a toolkit to pack, ship, store, and deliver container content. Prior to 3.1.0, in pull-through cache mode, distribution discovers token auth endpoints by parsing WWW-Authenticate challenges returned by the configured upstream registry. The realm URL from a bearer challenge is used without validating that it matches the upstream registry host. As a result, an attacker-controlled upstream can cause distribution to send the configured upstream credentials via basic auth to an attacker-controlled realm URL. This vulnerability is fixed in 3.1.0.	Patched by core rule	Y
CVE-2026-34954	PraisonAI SSRF via Unvalidated url in FileTools.download_file() with	PraisonAI is a multi-agent teams system. Prior to version 1.5.95, FileTools.download_file()	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	follow_redirects=True	in praisonaiagents validates the destination path but performs no validation on the url parameter, passing it directly to httpx.stream() with follow_redirects=True. An attacker who controls the URL can reach any host accessible from the server including cloud metadata services and internal network services. This issue has been patched in version 1.5.95.		
CVE-2026-34936	PraisonAI SSRF via Unvalidated api_base Parameter in passthrough()/apassthrough()	PraisonAI is a multi-agent teams system. Prior to version 4.5.90, passthrough() and apassthrough() in praisonai accept a caller-controlled api_base parameter that is concatenated with endpoint and passed directly to httpx.Client.request() when the litellm primary path raises AttributeError. No URL scheme validation, private IP filtering, or domain allowlist is applied. This issue has been patched in version 4.5.90.	Patched by core rule	Y
CVE-2026-22664	prompts.chat SSRF via Unvalidated token Parameter in Fal.ai Media Status Polling	prompts.chat prior to commit 30a8f04 contains a server-side request forgery vulnerability in Fal.ai media status polling that allows authenticated users to perform arbitrary outbound requests by supplying attacker-controlled URLs in the token parameter. Attackers can exploit the lack of URL validation to disclose the FAL_API_KEY in the Authorization header, enabling credential theft, internal network probing,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and abuse of the victim's Fal.ai account.		
CVE-2026-28798	ZimaOS Unauthenticated SSRF via /v1/sys/proxy Endpoint Accessible via Cloudflare Tunnel	ZimaOS is a fork of CasaOS. Prior to version 1.5.3, a proxy endpoint (/v1/sys/proxy) exposed by ZimaOS's web interface can be abused to make requests to internal localhost services. This results in unauthenticated access to internal-only endpoints and sensitive local services when the product is reachable from the Internet through a Cloudflare Tunnel. This issue has been patched in version 1.5.3.	Patched by core rule	Y
CVE-2026-31818	Budibase SSRF via Empty BLACKLIST_IPS Causing REST Datasource Connector to Allow All Requests	Budibase is an open-source low-code platform. Prior to version 3.33.4, a server-side request forgery vulnerability exists in Budibase's REST datasource connector. The platform's SSRF protection mechanism (IP blacklist) is rendered completely ineffective because the BLACKLIST_IPS environment variable is not set by default in any of the official deployment configurations. When this variable is empty, the blacklist function unconditionally returns false, allowing all requests through without restriction. This issue has been patched in version 3.33.4.	Patched by core rule	Y
CVE-2026-5417	Dataease SQLbot SSRF via address Argument in get_es_data_by_http() Elasticsearch Handler	A vulnerability was determined in Dataease SQLbot up to 1.6.0. This issue affects the function get_es_data_by_http of the file backend/apps/db/es_engine.py of the component Elasticsearch Handler. This manipulation of the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		argument address causes server-side request forgery. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized. Upgrading to version 1.7.0 is capable of addressing this issue.		
CVE-2026-34590	Postiz Blind SSRF via Missing IsSafeWebhookUrl Validator in POST /webhooks/ Creation	Postiz is an AI social media scheduling tool. Prior to version 2.21.4, the POST /webhooks/ endpoint for creating webhooks uses WebhooksDto which validates the url field with only @IsUrl() (format check), missing the @IsSafeWebhookUrl validator that blocks internal/private network addresses. The update and test endpoints correctly apply @IsSafeWebhookUrl. When a post is published, the orchestrator fetches the stored webhook URL without runtime validation, enabling blind SSRF against internal services. This issue has been patched in version 2.21.4.	Patched by core rule	Y
CVE-2026-34577	Postiz Unauthenticated SSRF via .mp4 Extension Check Bypass in /public/stream Endpoint	Postiz is an AI social media scheduling tool. Prior to version 2.21.3, the GET /public/stream endpoint accepts a user-supplied url query parameter and proxies the full HTTP response back to the caller. The only validation is url.endsWith('mp4'), which is trivially bypassable by appending .mp4 as a query parameter value or URL fragment. The endpoint requires no authentication and has no SSRF protections. This issue	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		has been patched in version 2.21.3.		
CVE-2026-34576	Postiz SSRF via File Extension Bypass in POST /public/v1/upload-from-url	Postiz is an AI social media scheduling tool. Prior to version 2.21.3, the POST /public/v1/upload-from-url endpoint accepts a user-supplied URL and fetches it server-side using axios.get() with no SSRF protections. The only validation is a file extension check which is trivially bypassed by appending an image extension to any URL path. An authenticated API user can fetch internal network resources and cloud instance metadata. This issue has been patched in version 2.21.3.	Patched by core rule	Y
CVE-2026-34526	SillyTavern SSRF via Incomplete IP Regex Missing localhost, IPv6, and Internal DNS Names	SillyTavern is a locally installed user interface for interacting with text generation LLMs. Prior to version 1.17.0, in src/endpoints/search.js, the hostname is checked against a regex that only matches literal dotted-quad IPv4. It does not catch localhost (hostname), [::1] (IPv6 loopback), and DNS names resolving to internal addresses (e.g. localtest.me). This issue has been patched in version 1.17.0.	Patched by core rule	Y
CVE-2026-32871	FastMCP SSRF via Path Traversal in _build_url() Due to urljoin ../ Resolution of Path Parameters	FastMCP is a Pythonic way to build MCP servers and clients. Prior to version 3.2.0, the OpenAPIProvider in FastMCP exposes internal APIs to MCP clients. When an OpenAPI operation defines path parameters, the system directly substitutes parameter values into the URL	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		template string without URL-encoding. Subsequently, urllib.parse.urljoin() resolves the final URL. Since urljoin() interprets ../ sequences as directory traversal, an attacker controlling a path parameter can perform path traversal attacks to escape the intended API prefix and access arbitrary backend endpoints. This results in authenticated SSRF as requests are sent with the authorization headers configured in the MCP provider. This issue has been patched in version 3.2.0.		
CVE-2026-34443	FreeScout SSRF via CIDR Check Bypass in checkIpByMask() Always Returning false for Plain IPs	FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. Prior to version 1.8.211, checkIpByMask() in app/Misc/Helper.php checks whether the input IP contains a / character. Plain IP addresses never contain /, so the function always returns false without checking any CIDR ranges. The entire 10.0.0.0/8 and 172.16.0.0/12 private ranges are unprotected. This issue has been patched in version 1.8.211.	Patched by core rule	Y
CVE-2026-34740	WWBN AVideo Stored SSRF via EPG Link URL Fetched Without isSSRFSafeURL() Validation	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the EPG link feature allows authenticated users with upload permissions to store arbitrary URLs that the server fetches on every EPG page visit. The URL is validated only with PHP's FILTER_VALIDATE_URL, which accepts internal network addresses.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Although AVideo has a dedicated isSSRFSafeURL() function for preventing SSRF, it is not called in this code path. This results in a stored server-side request forgery vulnerability. At time of publication, there are no publicly available patches.		
CVE-2026-34367	InvoiceShelf SSRF via Unsanitized HTML in Invoice Notes Field Passed to Dompdf	InvoiceShelf is an open-source web and mobile app for tracking expenses and payments. Prior to version 2.2.0, a Server-Side Request Forgery vulnerability exists in the Invoice PDF generation module. User-supplied HTML in the invoice Notes field is passed unsanitised to the Dompdf rendering library, which will fetch any remote resources referenced in the markup. This can be triggered via the PDF preview and email delivery endpoints. This issue has been patched in version 2.2.0.	Patched by core rule	Y
CVE-2026-34366	InvoiceShelf SSRF via Unsanitized HTML in Payment Notes Field Passed to Dompdf	InvoiceShelf is an open-source web and mobile app for tracking expenses and payments. Prior to version 2.2.0, a Server-Side Request Forgery vulnerability exists in the Payment receipt PDF generation module. User-supplied HTML in the payment Notes field is passed unsanitised to the Dompdf rendering library, which will fetch any remote resources referenced in the markup. This issue has been patched in version 2.2.0.	Patched by core rule	Y
CVE-2026-34365	InvoiceShelf SSRF via Unsanitized HTML in Estimate Notes Field Passed to Dompdf	InvoiceShelf is an open-source web and mobile app for tracking expenses and payments. Prior to version 2.2.0, a Server-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Side Request Forgery vulnerability exists in the Estimate PDF generation module. User-supplied HTML in the estimate Notes field is passed unsanitised to the Dompdf rendering library, which will fetch any remote resources referenced in the markup. This issue has been patched in version 2.2.0.		
CVE-2026-34360	HAPI FHIR Unauthenticated SSRF via User-Supplied URL in /loadIG Validator Endpoint	HAPI FHIR is a complete implementation of the HL7 FHIR standard for healthcare interoperability in Java. Prior to version 6.9.4, the /loadIG HTTP endpoint in the FHIR Validator HTTP service accepts a user-supplied URL via JSON body and makes server-side HTTP requests to it without any hostname, scheme, or domain validation. An unauthenticated attacker with network access to the validator can probe internal network services, cloud metadata endpoints, and map network topology through error-based information leakage. This issue has been patched in version 6.9.4.	Patched by core rule	Y
CVE-2026-34163	FastGPT SSRF via MCP Tools Endpoints Bypassing isInternalAddress() Validation	FastGPT is an AI Agent building platform. Prior to version 4.14.9.5, FastGPT's MCP tools endpoints (/api/core/app/mcpTools/getTools and /api/core/app/mcpTools/runTool) accept a user-supplied URL parameter and make server-side HTTP requests to it without validating whether the URL points to an internal/private network address.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Although the application has a dedicated isInternalAddress() function for SSRF protection used in other endpoints, the MCP tools endpoints do not call this function. An authenticated attacker can use these endpoints to scan internal networks and access cloud metadata services. This issue has been patched in version 4.14.9.5.		
CVE-2026-3881	Performance Monitor WordPress Plugin Unauthenticated SSRF via Unvalidated Parameter	The Performance Monitor WordPress plugin through 1.0.6 does not validate a parameter before making a request to it, which could allow unauthenticated users to perform SSRF attacks.	Patched by core rule	Y
CVE-2026-34881	OpenStack Glance SSRF via HTTP Redirect Bypass in web-download and glance-download Import	OpenStack Glance before 29.1.1, 30.x before 30.1.1, and 31.0.0 is affected by Server-Side Request Forgery. By use of HTTP redirects, an authenticated user can bypass URL validation checks and redirect to internal services. Only glance image import functionality is affected. In particular, the web-download and glance-download import methods are subject to this vulnerability, as is the optional ovf_process image import plugin.	Patched by core rule	Y
CVE-2026-31804	Tautulli SSRF via Unvalidated img Parameter in Unauthenticated /pms_image_proxy Endpoint	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. Prior to version 2.17.0, the /pms_image_proxy endpoint accepts a user-supplied img parameter and forwards it to Plex Media Server's photo transcoder without authentication and without restricting the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		scheme or host. The endpoint is intentionally excluded from all authentication checks. Any value of img beginning with http is passed directly to Plex, causing the Plex Media Server process to issue an outbound HTTP request to any attacker-specified URL. This issue has been patched in version 2.17.0.		
CVE-2026-29925	Invoice Ninja SSRF in CheckDatabaseRequest.php	Invoice Ninja v5.12.46 and v5.12.48 is vulnerable to Server-Side Request Forgery (SSRF) in CheckDatabaseRequest.php.	Patched by core rule	Y
CVE-2026-29954	KubePlus SSRF via chartURL in ResourceComposition with wget Header Injection	In KubePlus 4.1.4, the mutating webhook and kubeconfiggenerator components have an SSRF vulnerability when processing the chartURL field of ResourceComposition resources. The field is only URL-encoded without validating the target address. When kubeconfiggenerator uses wget to download charts, the chartURL is directly concatenated into the command, allowing attackers to inject wget's --header option to achieve arbitrary HTTP header injection.	Patched by core rule	Y
CVE-2026-0560	lollms SSRF via Unvalidated URL in _download_image_to_temp() in /api/files/export-content	A Server-Side Request Forgery vulnerability exists in parisneo/lollms versions prior to 2.2.0, specifically in the /api/files/export-content endpoint. The _download_image_to_temp() function in backend/routers/files.py fails to validate user-controlled URLs, allowing attackers to make arbitrary HTTP requests to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		internal services and cloud metadata endpoints. This vulnerability can lead to internal network access, cloud metadata access, information disclosure, port scanning, and potentially remote code execution.		
CVE-2026-33992	pyLoad SSRF via Unvalidated Download URL Enabling Internal Service Access and Metadata Exfiltration	pyLoad is a free and open-source download manager written in Python. Prior to version 0.5.0b3.dev97, PyLoad's download engine accepts arbitrary URLs without validation, enabling Server-Side Request Forgery attacks. An authenticated attacker can exploit this to access internal network services and exfiltrate cloud provider metadata. On DigitalOcean droplets, this exposes sensitive infrastructure data including droplet ID, network configuration, region, authentication keys, and SSH keys configured in user-data/cloud-init. Version 0.5.0b3.dev97 contains a patch.	Patched by core rule	Y
CVE-2026-33953	LinkAce SSRF via Internal Hostname Bypass Despite Private IP Literal Blocking	LinkAce is a self-hosted archive to collect website links. Versions prior to 2.5.3 block direct requests to private IP literals, but still perform server-side requests to internal-only resources when those resources are referenced through an internal hostname. This allows an authenticated user to trigger server-side requests to internal services reachable by the LinkAce server but not directly reachable by an external user. Version 2.5.3 patches the issue.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-31945	LibreChat SSRF via DNS Resolution Bypass of Hostname-Only Validation in Agent Actions/MCP	LibreChat is a ChatGPT clone with additional features. Versions 0.8.2-rc2 through 0.8.2 are vulnerable to a server-side request forgery attack when using agent actions or MCP. Although a previous SSRF vulnerability was patched, the fix only introduced hostname validation. It does not verify whether DNS resolution results in a private IP address. As a result, an attacker can still bypass the protection and gain access to internal resources such as cloud instance metadata endpoints. Version 0.8.3-rc1 contains a patch.	Patched by core rule	Y
CVE-2026-31943	LibreChat SSRF via IPv4-Mapped IPv6 Hex Notation Bypassing isPrivateIP() Check	LibreChat is a ChatGPT clone with additional features. Prior to version 0.8.3, isPrivateIP() in packages/api/src/auth/domain.ts fails to detect IPv4-mapped IPv6 addresses in their hex-normalized form, allowing any authenticated user to bypass SSRF protection and make the server issue HTTP requests to internal network resources including cloud metadata services (e.g., AWS 169.254.169.254), loopback, and RFC1918 ranges. Version 0.8.3 fixes the issue.	Patched by core rule	Y
CVE-2026-4964	letta SSRF via ImageContent in _convert_message_create_to_message() File URL Handler	A security vulnerability has been detected in letta-ai letta 0.16.4. This vulnerability affects the function _convert_message_create_to_message of the file letta/helpers/message_helper.py of the component File URL Handler. Such manipulation of the argument ImageContent leads to server-side	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		request forgery. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.		
CVE-2026-33766	WWBN AVideo SSRF via Redirect Following in url_get_contents() Bypassing isSSRFSafeURL()	WWBN AVideo is an open source video platform. In versions up to and including 26.0, isSSRFSafeURL() validates URLs against private/reserved IP ranges before fetching, but url_get_contents() follows HTTP redirects without re-validating the redirect target. An attacker can bypass SSRF protection by redirecting from a public URL to an internal target. Commit 8b7e9dad359d5fac69e0cbbb370250e0b284bc12 contains a patch.	Patched by core rule	Y
CVE-2026-33205	calibre SSRF via Unvalidated background-image URL in Web View Endpoint	calibre is a cross-platform e-book manager. Prior to version 9.6.0, a Server-Side Request Forgery vulnerability in the background-image endpoint of calibre e-book reader's web view allows an attacker to perform blind GET requests to arbitrary URLs and exfiltrate information out from the ebook sandbox. Version 9.6.0 patches the issue.	Patched by core rule	Y
CVE-2026-30637	OTCMS SSRF via AnnounContent in /admin/read.php Without Authentication	Server-Side Request Forgery (SSRF) vulnerability exists in the AnnounContent of the /admin/read.php in OTCMS V7.66 and before. The vulnerability allows remote attackers to craft HTTP requests, without authentication, containing a URL pointing to internal services or any remote server.	Patched by core rule	Y
CVE-2026-33644	Lychee SSRF via DNS Rebinding Bypass in	Lychee is a free, open-source photo-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	PhotoUrlRule.php Skipping IP Validation for Hostnames	management tool. Prior to version 7.5.2, the SSRF protection in PhotoUrlRule.php can be bypassed using DNS rebinding. The IP validation check only activates when the hostname is an IP address. When a domain name is used, filter_var($host, FILTER_VALIDATE_IP) returns false, skipping the entire check. Version 7.5.2 patches the issue.		
CVE-2026-33619	PinchTab SSRF via Unvalidated callbackUrl in Optional Scheduler Webhook Delivery	PinchTab is a standalone HTTP server that gives AI agents direct control over a Chrome browser. PinchTab v0.8.3 contains a server-side request forgery issue in the optional scheduler's webhook delivery path. When a task is submitted to POST /tasks with a user-controlled callbackUrl, the v0.8.3 scheduler sends an outbound HTTP POST to that URL when the task reaches a terminal state. In that release, the webhook path validated only the URL scheme and did not reject loopback, private, link-local, or other non-public destinations. This was addressed in v0.8.4 by validating callback targets before dispatch, rejecting non-public IP ranges, and disabling redirect following.	Patched by core rule	Y
CVE-2026-33537	Lychee SSRF via Incomplete IP Validation Missing Loopback and Link-Local in Photo::fromUrl Patch	Lychee is a free, open-source photo-management tool. The patch introduced for GHSA-cpgw-wgf3-xc6v (SSRF via Photo::fromUrl) contains an incomplete IP validation check that fails to block loopback	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		addresses and link-local addresses. Prior to version 7.5.1, an authenticated user can still reach internal services using direct IP addresses, bypassing all four protection configuration settings even when they are set to their secure defaults. Version 7.5.1 contains a fix.		
CVE-2026-33486	Roadiz SSRF Enabling Local File Read via file:// Protocol in documents Module	Roadiz is a polymorphic content management system. A vulnerability in roadiz/documents prior to versions 2.7.9, 2.6.28, 2.5.44, and 2.3.42 allows an authenticated attacker to read any file on the server's local file system that the web server process has access to, including highly sensitive environment variables, database credentials, and internal configuration files. Versions 2.7.9, 2.6.28, 2.5.44, and 2.3.42 contain a patch.	Patched by core rule	Y

VULNERABILITY DETAILS

Cross-Site Scripting (XSS) Vulnerabilities

Cross-site scripting vulnerabilities allow attackers to inject malicious scripts into web pages, enabling session hijacking, credential theft, and full remote code execution. With 160 CVEs, XSS was the largest attack category in April 2026. All are patched by AppTrana core rules.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-41472	CyberPanel Stored XSS via Unauthenticated AI Scanner Callback	CyberPanel versions prior to 2.4.4 contain a stored cross-site scripting vulnerability in the AI Scanner dashboard where the POST /api/ai-scanner/callback endpoint lacks authentication and allows unauthenticated attackers to inject malicious JavaScript by overwriting the findings_json field of ScanHistory records. Attackers can inject JavaScript that executes in an administrator's authenticated session when they visit the AI Scanner dashboard, allowing them to issue same-origin requests to plant cron jobs and achieve remote code execution on the server.	Patched by core rule	Y
CVE-2026-41067	Astro Server-Side XSS via Case-Insensitive Script Tag Bypass in defineScriptVars	Astro is a web framework. Prior to 6.1.6, the defineScriptVars function in Astro's server-side rendering pipeline uses a case-sensitive regex to sanitize values injected into inline script tags via the define:vars directive. HTML parsers close script elements case-insensitively, allowing an attacker to bypass the sanitization with payloads like </Script>, </script >, or </script/> and inject arbitrary HTML/JavaScript. This vulnerability is fixed in 6.1.6.	Patched by core rule	Y
CVE-2026-41318	AnythingLLM Stored DOM XSS via Chartable Component Chart Caption	AnythingLLM is an application that turns pieces of content into context that any LLM can use as references during	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		chatting. Prior to version 1.12.1, AnythingLLM's in-chat markdown renderer has an unsafe custom rule for images that interpolates the markdown image's alt text into an HTML alt attribute without any HTML encoding. The Chartable component renders chart captions with no sanitization, allowing an attacker who can influence the LLM's output via indirect prompt injection to trigger stored DOM-level XSS in every other user's browser when they open that conversation. Version 1.12.1 contains a patch.		
CVE-2026-41240	DOMPurify XSS Bypass via FORBID_TAGS Skip in EXTRA_ELEMENT_HANDLING	DOMPurify is a DOM-only cross-site scripting sanitizer for HTML, MathML, and SVG. Versions prior to 3.4.0 have an inconsistency between FORBID_TAGS and FORBID_ATTR handling when function-based ADD_TAGS is used. When EXTRA_ELEMENT_HANDLING.tagCheck returns true, the short-circuit evaluation skips the FORBID_TAGS check entirely, allowing forbidden elements to survive sanitization with their attributes intact. Version 3.4.0 patches the issue.	Patched by core rule	Y
CVE-2026-4512	reCaptcha by WebDesignBy WordPress Plugin XSS via Site Key in grecaptcha_js()	The reCaptcha by WebDesignBy WordPress plugin before 2.0 does not sanitize or escape the Site Key setting before outputting it in a JavaScript string context via the grecaptcha_js() function. This allows administrators on multisite installations to inject arbitrary JavaScript that executes for all visitors to the WordPress login page.	Patched by core rule	Y
CVE-2024-58344	Carbon Forum Persistent XSS via Forum Name in Dashboard Settings	Carbon Forum 5.9.0 contains a persistent cross-site scripting vulnerability that allows authenticated	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		administrators to inject malicious JavaScript code through the Forum Name field in dashboard settings. Attackers with admin privileges can store JavaScript payloads in the Forum Name field that execute in the browsers of all users visiting the forum, enabling session hijacking and data theft.		
CVE-2018-25269	ICEWARP XSS via Base64-Encoded Payloads in Object and Embed Email Tags	ICEWARP 11.0.0.0 contains a cross-site scripting vulnerability that allows attackers to inject malicious HTML elements into emails by embedding base64-encoded payloads in object and embed tags. Attackers can craft emails containing data URIs with embedded scripts that execute in the client when the email is viewed, compromising user sessions and stealing sensitive information.	Patched by core rule	Y
CVE-2026-41063	WWBN AVideo XSS via javascript: URLs in Markdown Links Bypassing ParsedownSafeWithLinks	WWBN AVideo is an open source video platform. In versions 29.0 and below, an incomplete XSS fix in AVideo's ParsedownSafeWithLinks class overrides inlineMarkup for raw HTML but does not override inlineLink() or inlineUrlTag(), allowing javascript: URLs in markdown link syntax to bypass sanitization. Commit cae8f0dadbdd962c89b91d0095c76edb8aadcacf contains an updated fix.	Patched by core rule	Y
CVE-2026-41061	WWBN AVideo Stored XSS via Unanchored Duration Regex in isValidDuration()	WWBN AVideo is an open source video platform. In versions 29.0 and below, the isValidDuration() regex uses a pattern without a $ end anchor, allowing arbitrary HTML/JavaScript to be appended after a valid duration prefix. The crafted duration is stored in the database and rendered	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		without HTML escaping on trending pages, playlist pages, and video gallery thumbnails, resulting in stored cross-site scripting. Commit bcba324644df8b4ed1f891462455f1cd26822a45 contains a fix.		
CVE-2026-6624	BichitroGan ISP Billing Software XSS via Pool List Interface	A weakness has been identified in BichitroGan ISP Billing Software 2025.3.20. Affected is an unknown function of the file /?_route=pool/add of the component Pool List Interface. Executing a manipulation 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-2026-6623	BichitroGan ISP Billing Software XSS via Profile Page Handler	A security flaw has been discovered in BichitroGan ISP Billing Software 2025.3.20. This impacts an unknown function of the file /?_route=settings/users-view/ of the component Profile Page Handler. Performing a manipulation results in cross site scripting. The attack is possible to be carried out remotely.	Patched by core rule	Y
CVE-2026-6622	BichitroGan ISP Billing Software XSS via Customer Handler	A vulnerability was identified in BichitroGan ISP Billing Software 2025.3.20. This affects an unknown function of the file /?_route=customers/edit/ of the component Customer Handler. Such manipulation leads to cross site scripting. The attack can be executed remotely.	Patched by core rule	Y
CVE-2024-7083	Email Encoder WordPress Plugin Stored XSS via Admin Settings	The Email Encoder WordPress plugin before 2.3.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).		
CVE-2026-40487	Postiz Stored XSS via SVG/HTML File Upload Content-Type Bypass	Postiz is an AI social media scheduling tool. Prior to version 2.21.6, a file upload validation bypass allows any authenticated user to upload arbitrary HTML, SVG, or other executable file types to the server by spoofing the Content-Type header. The uploaded files are then served by nginx with a Content-Type derived from their original extension, enabling Stored Cross-Site Scripting (XSS) in the context of the application's origin. This can lead to session riding, account takeover, and full compromise of other users' accounts. Version 2.21.6 contains a fix.	Patched by core rule	Y
CVE-2026-40479	Kimai Stored XSS via Profile Alias in HTML Attribute Context	Kimai is an open-source time tracking application. In versions 1.16.3 through 2.52.0, the escapeForHtml() function in KimaiEscape.js does not escape double quote or single quote characters. When a user's profile alias is inserted into an HTML attribute context via the team member form prototype and rendered through innerHTML, this incomplete escaping allows HTML attribute injection. An authenticated user with ROLE_USER privileges can store a malicious alias that executes JavaScript in the browser of any administrator viewing the team form. This issue has been fixed in version 2.53.0.	Patched by core rule	Y
CVE-2026-40353	wger Stored XSS via license_author Field Rendered with Django safe Filter	wger is a free, open-source workout and fitness manager. In versions 2.5 and below, the attribution_link property in AbstractLicenseModel constructs HTML by directly	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		interpolating user-controlled license fields (such as license_author) without escaping, and templates render the result using Django's |safe filter. An authenticated user can create an ingredient with a malicious license_author value containing JavaScript, which executes in the browser of any visitor viewing the ingredient page. This issue has been fixed in version 2.5.		
CVE-2026-40283	WeGIA Stored XSS via Nome Field in Informacoes Pacientes Page	WeGIA is a web manager for charitable institutions. In versions prior to 3.6.10, a Stored Cross-Site Scripting (XSS) vulnerability allows an authenticated user to inject malicious JavaScript via the Nome field in the Informacoes Pacientes page. The payload is stored and executed when the patient information is viewed. Version 3.6.10 fixes the issue.	Patched by core rule	Y
CVE-2026-6486	classroombookings Stored XSS via displayname Argument in layout.php	A vulnerability was detected in classroombookings up to 2.17.0. This impacts the function read of the file crbs-core/application/views/layout.php of the component User Display Name Handler. The manipulation of the argument displayname results in cross site scripting. The attack can be executed remotely. Upgrading to version 2.17.1 will fix this issue.	Patched by core rule	Y
CVE-2026-40922	SiYuan XSS via iframe srcdoc in Bazaar README Bypassing Lute Sanitizer	SiYuan is an open-source personal knowledge management system. In versions 3.6.1 through 3.6.3, a prior fix for XSS in bazaar README rendering enabled the Lute HTML sanitizer, but the sanitizer does not block iframe tags, and its URL-prefix blocklist does not effectively filter srcdoc attributes which contain raw	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		HTML rather than URLs. A malicious bazaar package author can include an iframe with a srcdoc attribute containing embedded scripts in their README. When other users view the package in SiYuan's marketplace UI, the payload executes in the Electron context with full application privileges. This issue has been fixed in version 3.6.4.		
CVE-2026-40186	ApostropheCMS Stored XSS via Entity Encoding Bypass in sanitize-html textarea/option	ApostropheCMS is an open-source Node.js content management system. A regression in versions 2.17.1 of the sanitize-html package bypasses allowedTags enforcement for text inside nonTextTagsArray elements (textarea and option). The code incorrectly assumes that htmlparser2 does not decode entities inside these elements and skips escaping, but htmlparser2 10.x does decode entities before passing text to the ontext callback. An attacker can inject arbitrary tags including XSS payloads through any allowed option or textarea element using entity encoding. This issue has been fixed in version 2.17.2 of sanitize-html and 4.29.0 of ApostropheCMS.	Patched by core rule	Y
CVE-2026-35569	ApostropheCMS Stored XSS via SEO Title/Meta Fields Breaking HTML Context	ApostropheCMS is an open-source Node.js content management system. Versions 4.28.0 and prior contain a stored cross-site scripting vulnerability in SEO-related fields (SEO Title and Meta Description), where user-controlled input is rendered without proper output encoding into HTML contexts including title tags, meta attributes, and JSON-LD structured data. An attacker can inject a payload to break out of the intended HTML context and execute	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		arbitrary JavaScript in the browser of any authenticated user who views the affected page. This issue has been fixed in version 4.29.0.		
CVE-2026-33889	ApostropheCMS Stored XSS via CSS Custom Property Bypass in color-field Module	ApostropheCMS is an open-source Node.js content management system. Versions 4.28.0 and prior contain a stored cross-site scripting vulnerability in the @apostrophecms/color-field module, where color values prefixed with -- bypass TinyColor validation, and the launder.string() call performs only type coercion without stripping HTML metacharacters. These unsanitized values are concatenated directly into style tags. An editor can inject a value which closes the style tag and executes arbitrary JavaScript in the browser of every visitor to any page containing the affected widget. This issue has been fixed in version 4.29.0.	Patched by core rule	Y
CVE-2026-40096	immich Open Redirect XSS via Album Name in og:title Meta Tag	immich is a high performance self-hosted photo and video management solution. Versions prior to 2.7.3 contain an open redirect vulnerability in the shared album functionality, where the album name is inserted unsanitized into a meta tag in api.service.ts. A registered attacker can create a shared album with a crafted name causing the victim's browser to redirect to an attacker-controlled site upon opening the share link. This facilitates phishing attacks. This issue has been fixed in version 2.7.3.	Patched by core rule	Y
CVE-2026-34212	Docmost Stored XSS via javascript: URL in Attachment Node	Docmost is open-source collaborative wiki and documentation software. In versions prior to 0.71.0, improper neutralization of	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attachment URLs in Docmost allows a low-privileged authenticated user to store a malicious javascript: URL inside an attachment node in page content. When another user views the page and activates the attachment link/icon, attacker-controlled JavaScript executes in the context of the Docmost origin. Version 0.71.0 patches the issue.		
CVE-2025-69993	Leaflet XSS via Unsanitized HTML in bindPopup() Method	Leaflet versions up to and including 1.9.4 are vulnerable to Cross-Site Scripting (XSS) via the bindPopup() method. This method renders user-supplied input as raw HTML without sanitization, allowing attackers to inject arbitrary JavaScript code through event handler attributes. When a victim views an affected map popup, the malicious script executes in the context of the victim's browser session.	Patched by core rule	Y
CVE-2026-39422	MaxKB Stored XSS via Application Name/Icon in Public Chat Interface	MaxKB is an open-source AI assistant for enterprise. Versions 2.7.1 and below contain a Stored Cross-Site Scripting (XSS) vulnerability through the application name or icon fields when creating an application. When a victim visits the public chat interface, the ChatHeadersMiddleware retrieves the application data and directly inserts the unescaped application name and icon into the HTML response via string replacement. This allows an attacker to execute arbitrary JavaScript in the victim's browser context. This issue has been fixed in version 2.8.0.	Patched by core rule	Y
CVE-2026-6218	ytDownloader XSS via createTextNode in Error Details Panel	A vulnerability was found in aandrew-me ytDownloader up to 3.20.2. Affected by this issue is the function	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		createTextNode of the component Error Details Panel. The manipulation results in cross site scripting. The attack may be performed from remote.		
CVE-2026-33657	EspoCRM Stored HTML Injection via post Field in Stream Activity Emails	EspoCRM is an open source customer relationship management application. Versions 9.3.3 and below have a stored HTML injection vulnerability that allows any authenticated user with standard privileges to inject arbitrary HTML into system-generated email notifications by crafting malicious content in the post field of stream activity notes. The server-side Handlebars templates render the post field using unescaped triple-brace syntax, creating a path where attacker-controlled HTML is accepted, stored, and rendered directly into emails without any escaping. This issue has been fixed in version 9.3.4.	Patched by core rule	Y
CVE-2026-2728	LibreNMS Authenticated XSS on showconfig Page	LibreNMS versions before 26.3.0 are affected by an authenticated Cross-site Scripting vulnerability on the showconfig page. Successful exploitation requires administrative privileges. Exploitation could result in XSS attacks being performed against other users with access to the page.	Patched by core rule	Y
CVE-2017-20239	MDwiki XSS via Unsanitized Location Hash Parameter	MDwiki contains a cross-site scripting vulnerability that allows remote attackers to execute arbitrary JavaScript by injecting malicious code through the location hash parameter. Attackers can craft URLs with JavaScript payloads in the hash fragment that are parsed and rendered without sanitization, causing the injected scripts to execute in the victim's browser context.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-1116	lollms XSS via Unsanitized content Field in AppLollmsMessage.from_dict()	A Cross-site Scripting (XSS) vulnerability was identified in the from_dict method of the AppLollmsMessage class in parisneo/lollms prior to version 2.2.0. The vulnerability arises from the lack of sanitization or HTML encoding of the content field when deserializing user-provided data. This allows an attacker to inject malicious HTML or JavaScript payloads, which can be executed in the context of another user's browser. Exploitation of this vulnerability can lead to account takeover, session hijacking, or wormable attacks.	Patched by core rule	Y
CVE-2026-35600	Vikunja Markdown Injection via Unescaped Task Title in Overdue Email Notifications	Vikunja is an open-source self-hosted task management platform. Prior to 2.3.0, task titles are embedded directly into Markdown link syntax in overdue email notifications without escaping Markdown special characters. When rendered by goldmark and sanitized by bluemonday, injected Markdown constructs produce phishing links and tracking pixels in legitimate notification emails. This vulnerability is fixed in 2.3.0.	Patched by core rule	Y
CVE-2026-1115	lollms Stored XSS via create_post Function in Social Feature	A Stored Cross-Site Scripting (XSS) vulnerability was identified in the social feature of parisneo/lollms, affecting the latest version prior to 2.2.0. The vulnerability exists in the create_post function within backend/routers/social/__init__.py, where user-provided content is directly assigned to the DBPost model without sanitization. This allows attackers to inject and store malicious JavaScript, which is executed in the browsers of users viewing the Home Feed, including	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		administrators. This can lead to account takeover, session hijacking, and wormable attacks. The issue is resolved in version 2.2.0.		
CVE-2026-40112	PraisonAI XSS via Agent Output Rendered as HTML Without nh3 Dependency	PraisonAI is a multi-agent teams system. Prior to 4.5.128, the Flask API endpoint in src/praisonai/api.py renders agent output as HTML without effective sanitization. The _sanitize_html function relies on the nh3 library, which is not listed as a required dependency. When nh3 is absent (the default installation), the sanitizer is a no-op that returns HTML unchanged. An attacker who can influence agent input via RAG data poisoning, web scraping results, or prompt injection can inject arbitrary JavaScript that executes in the browser of anyone viewing the API output. This vulnerability is fixed in 4.5.128.	Patched by core rule	Y
CVE-2023-54364	Joomla HikaShop Reflected XSS via GET Parameters in Product Filter	Joomla HikaShop 4.7.4 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating GET parameters in the product filter endpoint. Attackers can craft malicious URLs containing XSS payloads in the from_option, from_ctrl, from_task, or from_itemid parameters to steal session tokens or login credentials when victims visit the link.	Patched by core rule	Y
CVE-2023-54363	Joomla Solidres Reflected XSS via Multiple GET Parameters	Joomla Solidres 2.13.3 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating multiple GET parameters including show, reviews, type_id, distance, facilities, categories, prices, location,	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		and Itemid. Attackers can craft malicious URLs containing JavaScript payloads in these parameters to steal session tokens, login credentials, or manipulate site content when victims visit the crafted links.		
CVE-2023-54362	Joomla VirtueMart Reflected XSS via keyword Parameter in Product Variants	Joomla VirtueMart Shopping-Cart 4.0.12 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the keyword parameter. Attackers can craft malicious URLs containing script payloads in the keyword parameter of the product-variants endpoint to execute arbitrary JavaScript in victim browsers and steal session tokens or credentials.	Patched by core rule	Y
CVE-2023-54361	Joomla iProperty Real Estate Reflected XSS via filter_keyword Parameter	Joomla iProperty Real Estate 4.1.1 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the filter_keyword parameter. Attackers can craft URLs containing JavaScript payloads in the filter_keyword GET parameter of the all-properties-with-map endpoint to execute arbitrary code in victim browsers and steal session tokens or credentials.	Patched by core rule	Y
CVE-2023-54360	Joomla JLex Review Reflected XSS via review_id URL Parameter	Joomla JLex Review 6.0.1 contains a reflected cross-site scripting vulnerability that allows attackers to inject malicious scripts by manipulating the review_id URL parameter. Attackers can craft malicious links containing JavaScript payloads that execute in victims' browsers when clicked, enabling session hijacking or credential theft.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-54358	WordPress adivaha Travel Plugin Reflected XSS via isMobile Parameter	WordPress adivaha Travel Plugin 2.3 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts by manipulating the isMobile parameter. Attackers can craft malicious URLs containing JavaScript payloads in the isMobile GET parameter at the /mobile-app/v3/ endpoint to execute arbitrary code in victims' browsers and steal session tokens or credentials.	Patched by core rule	Y
CVE-2025-70797	Limesurvey XSS via Box[title] and box[url] Parameters	Cross Site Scripting vulnerability in Limesurvey v.6.15.20+251021 allows a remote attacker to execute arbitrary code via the Box[title] and box[url] parameters.	Patched by core rule	Y
CVE-2025-63238	LimeSurvey Reflected XSS via gid Parameter in getInstance() Function	A Reflected Cross-Site Scripting (XSS) affects LimeSurvey versions prior to 6.15.11+250909, due to the lack of validation of gid parameter in getInstance() function in application/models/QuestionCreate.php. This allows an attacker to craft a malicious URL and compromise the logged in user.	Patched by core rule	Y
CVE-2026-39941	ChurchCRM XSS via EName and EDesc Parameters in EditEventAttendees.php	ChurchCRM is an open-source church management system. Prior to 7.1.0, an XSS vulnerability allows attacker-supplied input sent via the EName and EDesc parameters in EditEventAttendees.php to be rendered in a page without proper output encoding, enabling arbitrary JavaScript execution in victims' browsers. This vulnerability is fixed in 7.1.0.	Patched by core rule	Y
CVE-2026-5810	SourceCodester Sales and Inventory System XSS via ID Parameter in delete.php	A flaw has been found in SourceCodester Sales and Inventory System 1.0. Affected is an unknown function of the file	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		/delete.php of the component GET Parameter Handler. This manipulation of the argument ID causes cross site scripting. Remote exploitation of the attack is possible. The exploit has been published and may be used.		
CVE-2026-35455	immich Stored XSS via OCR Text Rendered via innerHTML in 360 Panorama Viewer	immich is a high performance self-hosted photo and video management solution. Prior to 2.7.0, Stored Cross-Site Scripting in the 360-degree panorama viewer allows any authenticated user to execute arbitrary JavaScript in the browser of any other user who views the malicious panorama with the OCR overlay enabled. The attacker uploads an equirectangular image containing crafted text; OCR extracts it, and the panorama viewer renders it via innerHTML without sanitization. This enables session hijacking, private photo exfiltration, and access to GPS location history and face biometric data. This vulnerability is fixed in 2.7.0.	Patched by core rule	Y
CVE-2026-39392	CI4MS Stored XSS via Unsanitized Page Content Rendered via echo on Public Frontend	CI4MS is a CodeIgniter 4-based CMS skeleton. Prior to 0.31.4.0, the Pages module does not apply the html_purify validation rule to content fields during create and update operations. Page content is stored unsanitized in the database and rendered as raw HTML on the public frontend via echo $pageInfo->content. An authenticated admin with page-editing privileges can inject arbitrary JavaScript that executes in the browser of every public visitor viewing the page. This vulnerability is fixed in 0.31.4.0.	Patched by core rule	Y
CVE-2026-39391	CI4MS Stored XSS via Blacklist Note in data-note HTML Attribute	CI4MS is a CodeIgniter 4-based CMS skeleton. Prior to 0.31.4.0, the blacklist (ban)	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		note parameter in UserController::ajax_blackList_post() is stored in the database without sanitization and rendered into an HTML data-note attribute without escaping. An admin with blacklist privileges can inject arbitrary JavaScript that executes in the browser of any other admin who views the user management page. This vulnerability is fixed in 0.31.4.0.		
CVE-2026-39846	SiYuan Stored XSS to RCE via Table Caption in Electron Desktop Client	SiYuan is a personal knowledge management system. Prior to 3.6.4, a malicious note synced to another user can trigger remote code execution in the SiYuan Electron desktop client. Table caption content is stored without safe escaping and later unescaped into rendered HTML, creating a stored XSS sink. Because the desktop renderer runs with nodeIntegration enabled and contextIsolation disabled, attacker-controlled JavaScript executes with access to Node.js APIs. This vulnerability is fixed in 3.6.4.	Patched by core rule	Y
CVE-2026-39400	Cronicle Stored XSS via Job Output Fields Rendered via innerHTML on Job Details Page	Cronicle is a multi-server task scheduler and runner. Prior to 0.9.111, a non-admin user with create_events and run_events privileges can inject arbitrary JavaScript through job output fields (html.content, html.title, table.header, table.rows, table.caption). The server stores this data without sanitization, and the client renders it via innerHTML on the Job Details page. This vulnerability is fixed in 0.9.111.	Patched by core rule	Y
CVE-2026-32712	Open Source POS Stored XSS via customer_name in Daily Sales Table	Open Source Point of Sale is a web based point-of-sale application. Prior to 3.4.3, a Stored Cross-Site Scripting (XSS) vulnerability exists in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		the Daily Sales management table. The customer_name column is configured with escape: false in the bootstrap-table column configuration, causing customer names to be rendered as raw HTML. An attacker with customer management permissions can inject arbitrary JavaScript into a customer's first_name or last_name field, which executes in the browser of any user viewing the Daily Sales page. This vulnerability is fixed in 3.4.3.		
CVE-2026-39841	Wikimedia Mediawiki Cargo Extension Stored XSS	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in Wikimedia Foundation Mediawiki - Cargo Extension allows Stored XSS. This issue affects Mediawiki - Cargo Extension: before 3.8.7.	Patched by core rule	Y
CVE-2026-39840	Wikimedia Mediawiki Cargo Extension XSS Targeting Non-Script Elements	Improper neutralization of input during web page generation vulnerability in Wikimedia Foundation Mediawiki - Cargo Extension allows XSS Targeting Non-Script Elements. This issue affects Mediawiki - Cargo Extension: before 3.8.7.	Patched by core rule	Y
CVE-2026-39839	Wikimedia Mediawiki Cargo Extension Stored XSS via Script-Related HTML Tags	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in Wikimedia Foundation Mediawiki - Cargo Extension allows Stored XSS. This issue affects Mediawiki - Cargo Extension: before 3.8.7.	Patched by core rule	Y
CVE-2026-39837	WikiWorks Mediawiki Cargo Extension Stored XSS via Script-Related HTML Tags	Improper neutralization of Script-Related HTML tags in a web page (basic XSS) vulnerability in WikiWorks Mediawiki - Cargo Extension allows Stored XSS. This issue affects Mediawiki - Cargo Extension: before 3.8.7.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-39380	Open Source POS Stored XSS via stock_location Parameter in Stock Locations	Open Source Point of Sale is a web based point-of-sale application. Prior to 3.4.3, a Stored Cross-Site Scripting (XSS) vulnerability exists in the Stock Locations configuration feature. The application fails to properly sanitize user input supplied through the stock_location parameter, allowing attackers to inject malicious JavaScript code that is stored in the database and executed when rendered in the Employees interface. This vulnerability is fixed in 3.4.3.	Patched by core rule	Y
CVE-2026-39338	ChurchCRM Blind Reflected XSS via search Parameter in Dashboard	ChurchCRM is an open-source church management system. Prior to 7.1.0, a Blind Reflected Cross-Site Scripting vulnerability exists in the search parameter accepted by the ChurchCRM dashboard. The application fails to sanitize or encode user-supplied input prior to rendering it within the browser's DOM. Although the application ultimately returns an HTTP 500 error, the browser's JavaScript engine parses and executes the injected script tags before the error response is returned. This vulnerability is fixed in 7.1.0.	Patched by core rule	Y
CVE-2026-39335	ChurchCRM Stored XSS in Group Remove Control and Family Editor State/Country	ChurchCRM is an open-source church management system. Prior to 7.1.1, there is Stored XSS in group remove control and family editor state/country. This is primarily an admin-to-admin stored XSS path when writable entity fields are abused. This vulnerability is fixed in 7.1.1.	Patched by core rule	Y
CVE-2026-35608	QuickDrop Stored XSS via SVG File Upload in File Preview Endpoint	QuickDrop is an easy-to-use file sharing application. Prior to 1.5.3, a stored XSS vulnerability exists in the file preview endpoint. The application allows SVG files	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		to be uploaded via the /api/file/upload-chunk endpoint. An attacker can upload a specially crafted SVG file containing a JavaScript payload. When any user views the file preview, the script executes in the context of the application's domain. This vulnerability is fixed in 1.5.3.		
CVE-2026-35574	ChurchCRM Stored XSS via Note Editor Allowing JavaScript Execution for Admins	ChurchCRM is an open-source church management system. Prior to 6.5.3, a stored Cross-Site Scripting (XSS) vulnerability in ChurchCRM's Note Editor allows authenticated users with note-adding permissions to execute arbitrary JavaScript code in the context of other users' browsers, including administrators. This can lead to session hijacking, privilege escalation, and unauthorized access to sensitive church member data. This vulnerability is fixed in 6.5.3.	Patched by core rule	Y
CVE-2026-35571	Emissary Stored XSS via javascript: URI in Mustache Navigation Template href Attribute	Emissary is a P2P based data-driven workflow engine. Prior to 8.39.0, Mustache navigation templates interpolated configuration-controlled link values directly into href attributes without URL scheme validation. An administrator who could modify the navItems configuration could inject javascript: URIs, enabling stored cross-site scripting against other authenticated users viewing the Emissary web interface. This vulnerability is fixed in 8.39.0.	Patched by core rule	Y
CVE-2026-35460	Papra HTML Injection via user.name in Transactional Email Templates	Papra is a minimalistic document management and archiving platform. Prior to 26.4.0, transactional email templates in Papra interpolate user.name directly into HTML without	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		escaping or sanitization. An attacker who registers with a display name containing HTML tags will have those tags injected into the verification and password reset email bodies, enabling convincing phishing attacks that appear to originate from official Papra notifications. This vulnerability is fixed in 26.4.0.		
CVE-2026-33865	MLflow Stored XSS via Malicious MLmodel YAML Artifact in Web Interface	MLflow is vulnerable to Stored Cross-Site Scripting (XSS) caused by unsafe parsing of YAML-based MLmodel artifacts in its web interface. An authenticated attacker can upload a malicious MLmodel file containing a payload that executes when another user views the artifact in the UI. This allows actions such as session hijacking or performing operations on behalf of the victim. This issue affects MLflow version through 3.10.1.	Patched by core rule	Y
CVE-2026-35399	WeGIA Stored XSS via Malicious Backup Filename	WeGIA is a Web manager for charitable institutions. Prior to 3.6.9, a stored XSS vulnerability allows an attacker to inject malicious scripts through a backup filename. This could lead to unauthorized execution of malicious code in the victim's browser, compromising session data or executing actions on behalf of the user. This vulnerability is fixed in 3.6.9.	Patched by core rule	Y
CVE-2026-35208	Lichess HTML Injection via Stream Title in Streamer Widget	lichess.org is the forever free, adless and open source chess server. Any approved streamer can inject arbitrary HTML into /streamer and the homepage Live streams widget by placing markup in their Twitch/YouTube stream title. CSP is present and blocks inline script execution, but the issue is still a server-	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		side HTML injection sink. This vulnerability is fixed with commit 0d5002696ae705e1888bf77de107c73de57bb1b3.		
CVE-2026-35046	Tandoor Recipes Stored CSS Injection via style Tag Whitelisted in bleach.clean()	Tandoor Recipes is an application for managing recipes, planning meals, and building shopping lists. Prior to 2.6.4, Tandoor Recipes allows authenticated users to inject arbitrary style tags into recipe step instructions. The bleach.clean() sanitizer explicitly whitelists the style tag, causing the backend to persist and serve unsanitized CSS payloads via the API. Any client consuming instructions_markdown from the API and rendering it as HTML without additional sanitization will execute attacker-controlled CSS, enabling UI redressing, phishing overlays, visual defacement, and CSS-based data exfiltration. This vulnerability is fixed in 2.6.4.	Patched by core rule	Y
CVE-2026-35035	CI4MS Stored XSS via System Settings Company Information Fields on Public Frontend	CI4MS is a CodeIgniter 4-based CMS skeleton. Prior to 0.31.2.0, the application fails to properly sanitize user-controlled input within System Settings Company Information. Several administrative configuration fields accept attacker-controlled input that is stored server-side and later rendered without proper output encoding. These values are persisted in the database and rendered unsafely on public-facing pages only, such as the main landing page. This vulnerability is fixed in 0.31.2.0.	Patched by core rule	Y
CVE-2026-34989	CI4MS Stored XSS via Profile Name Rendered Unsafely in Multiple Application Views	CI4MS is a CodeIgniter 4-based CMS skeleton. Prior to 31.0.0.0, the application fails to properly sanitize user-controlled input when users	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		update their profile name. An attacker can inject a malicious JavaScript payload into their profile name, which is then stored server-side. This stored payload is later rendered unsafely in multiple application views without proper output encoding, leading to stored cross-site scripting. This vulnerability is fixed in 31.0.0.0.		
CVE-2026-31313	Feehi CMS Stored XSS via Content Field in Creation/Editing Module	An authenticated stored cross-site scripting (XSS) vulnerability in the creation/editing module of Feehi CMS v2.1.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Content field.	Patched by core rule	Y
CVE-2026-31354	Feehi CMS Stored XSS via Group, Category or Description in Permissions Module	Multiple authenticated stored cross-site scripting (XSS) vulnerabilities in the Permissions module of Feehi CMS v2.1.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Group, Category or Description parameters.	Patched by core rule	Y
CVE-2026-31353	Feehi CMS Stored XSS via Name Parameter in Category Module	An authenticated stored cross-site scripting (XSS) vulnerability in the Category module of Feehi CMS v2.1.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Name parameter.	Patched by core rule	Y
CVE-2026-31352	Feehi CMS Stored XSS via Role Name in Role Management Module	An authenticated stored cross-site scripting (XSS) vulnerability in the Role Management module of Feehi CMS v2.1.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Role Name parameter.	Patched by core rule	Y
CVE-2026-31351	Feehi CMS Stored XSS via Title Parameter in Creation/Editing Module	An authenticated stored cross-site scripting (XSS) vulnerability in the creation/editing module of Feehi CMS v2.1.1 allows	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Title parameter.		
CVE-2026-31350	Feehi CMS Stored XSS via Page Sign Parameter	An authenticated stored cross-site scripting (XSS) vulnerability in Feehi CMS v2.1.1 allows attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the Page Sign parameter.	Patched by core rule	Y
CVE-2026-33510	Homarr DOM-Based XSS via callbackUrl Parameter on Login Page	Homarr is an open-source dashboard. Prior to 1.57.0, a DOM-based Cross-Site Scripting (XSS) vulnerability has been discovered in Homarr's /auth/login page. The application improperly trusts a URL parameter (callbackUrl), which is passed to redirect and router.push. An attacker can craft a malicious link that, when opened by an authenticated user, performs a client-side redirect and executes arbitrary JavaScript in the context of their browser. This vulnerability is fixed in 1.57.0.	Patched by core rule	Y
CVE-2026-33406	Pi-hole Admin HTML Attribute Injection via Config Values in settings-advanced.js	Pi-hole Admin Interface is a web interface for managing Pi-hole. From 6.0 to before 6.5, configuration values from the /api/config endpoint are placed directly into HTML value attributes without escaping in settings-advanced.js, enabling HTML attribute injection. A double quote in any config value breaks out of the attribute context. The primary attack vector is importing a malicious teleporter backup, which bypasses per-field server-side validation. This vulnerability is fixed in 6.5.	Patched by core rule	Y
CVE-2019-25676	Ask Expert Script XSS via cateid Parameter in categorysearch.php	Ask Expert Script 3.0.5 contains cross-site scripting and SQL injection vulnerabilities that allow unauthenticated attackers to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		inject malicious code by manipulating URL parameters. Attackers can inject script tags through the cateid parameter in categorysearch.php to execute arbitrary code or extract database information.		
CVE-2016-20054	Nodcms CSRF Allowing Unauthorized Admin Actions via Crafted Forms	Nodcms contains a cross-site request forgery vulnerability that allows attackers to perform unauthorized administrative actions by crafting malicious forms. Attackers can trick authenticated administrators into submitting requests to admin/user_manipulate and admin/settings/generall endpoints to create users or modify application settings without explicit consent.	Patched by core rule	Y
CVE-2018-25250	MyBB Last User Threads Plugin Persistent XSS via Thread Subject	MyBB Last User's Threads in Profile Plugin 1.2 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts by crafting thread subjects with script tags. Attackers can create threads with script payloads in the subject field that execute when users visit the attacker's profile page.	Patched by core rule	Y
CVE-2018-25249	MyBB My Arcade Plugin Persistent XSS via Arcade Game Score Comments	MyBB My Arcade Plugin 1.3 contains a persistent cross-site scripting vulnerability that allows authenticated users to inject malicious scripts through arcade game score comments. Attackers can add crafted HTML and JavaScript payloads in the comment field that execute when other users view or edit the comment.	Patched by core rule	Y
CVE-2018-25248	MyBB Downloads Plugin Persistent XSS via Download Title Field	MyBB Downloads Plugin 2.0.3 contains a persistent cross-site scripting vulnerability that allows regular members to inject malicious scripts through the download title field. Attackers can submit a new	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		download with HTML/JavaScript code in the title parameter, which executes when administrators validate the download in downloads.php.		
CVE-2018-25247	MyBB Like Plugin XSS via Post Subject Displayed Without Sanitization on Profile	MyBB Like Plugin 3.0.0 contains a cross-site scripting vulnerability that allows attackers to inject malicious scripts by creating posts or threads with unvalidated subject content. Attackers can craft post subjects containing script tags that execute when other users view the attacker's profile, where liked posts are displayed without sanitization.	Patched by core rule	Y
CVE-2026-34229	Emlog Stored XSS via URI Scheme Validation Bypass in Comment Module	Emlog is an open source website building system. Prior to version 2.6.8, there is a stored cross-site scripting (XSS) vulnerability in emlog comment module via URI scheme validation bypass. This issue has been patched in version 2.6.8.	Patched by core rule	Y
CVE-2026-35218	Budibase Stored XSS via Entity Name Rendered via Svelte {@html} in Command Palette	Budibase is an open-source low-code platform. Prior to version 3.32.5, Budibase's Builder Command Palette renders entity names (tables, views, queries, automations) using Svelte's {@html} directive without any sanitization. An authenticated user with Builder access can create a table, automation, view, or query whose name contains an HTML payload. When any Builder-role user in the same workspace opens the Command Palette, the payload executes in their browser, stealing their session cookie and enabling full account takeover. This issue has been patched in version 3.32.5.	Patched by core rule	Y
CVE-2026-34598	YesWiki Stored Blind XSS via Form Title	YesWiki is a wiki system written in PHP. Prior to version 4.6.0, a stored and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Field Without Authentication	blind XSS vulnerability exists in the form title field. A malicious attacker can inject JavaScript without any authentication via a form title that is saved in the backend database. When any user visits that injected page, the JavaScript payload gets executed. This issue has been patched in version 4.6.0.		
CVE-2026-34974	phpMyFAQ XSS via HTML Entity Encoding Bypass in SVG Sanitizer for javascript: URLs	phpMyFAQ is an open source FAQ web application. Prior to version 4.1.1, the regex-based SVG sanitizer in phpMyFAQ (SvgSanitizer.php) can be bypassed using HTML entity encoding in javascript: URLs within SVG a href attributes. Any user with edit_faq permission can upload a malicious SVG that executes arbitrary JavaScript when viewed, enabling privilege escalation from editor to full admin takeover. This issue has been patched in version 4.1.1.	Patched by core rule	Y
CVE-2026-34729	phpMyFAQ Stored XSS via Regex Bypass in Filter::removeAttributes()	phpMyFAQ is an open source FAQ web application. Prior to version 4.1.1, there is a stored XSS vulnerability via Regex Bypass in Filter::removeAttributes(). This issue has been patched in version 4.1.1.	Patched by core rule	Y
CVE-2026-32629	phpMyFAQ XSS via RFC 5321 Quoted Email Address Rendered with Twig |raw Filter	phpMyFAQ is an open source FAQ web application. Prior to version 4.1.1, an unauthenticated attacker can submit a guest FAQ with an email address that is syntactically valid per RFC 5321 yet contains raw HTML. PHP's FILTER_VALIDATE_EMAIL accepts this email as valid. The email is stored in the database without HTML sanitization and later rendered in the admin FAQ editor template using Twig's |raw filter, which bypasses	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		auto-escaping entirely. This issue has been patched in version 4.1.1.		
CVE-2026-34571	CI4MS Stored XSS via User Management Input in Backend Administrative Interface	CI4MS is a CodeIgniter 4-based CMS skeleton. Prior to version 0.31.0.0, a Stored Cross-Site Scripting vulnerability exists in the backend user management functionality. The application fails to properly sanitize user-controlled input before rendering it in the administrative interface, allowing attackers to inject persistent JavaScript code. This results in automatic execution whenever backend users access the affected page. This issue has been patched in version 0.31.0.0.	Patched by core rule	Y
CVE-2026-34569	CI4MS Stored XSS via Blog Category Title Rendered Across Public and Admin Views	CI4MS is a CodeIgniter 4-based CMS skeleton. Prior to version 0.31.0.0, the application fails to properly sanitize user-controlled input when creating or editing blog categories. An attacker can inject a malicious JavaScript payload into the category title field, which is stored server-side and later rendered unsafely across public-facing blog category pages, administrative interfaces, and blog post views. This issue has been patched in version 0.31.0.0.	Patched by core rule	Y
CVE-2026-34568	CI4MS Stored XSS via Blog Post Content Rendered Without Output Encoding	CI4MS is a CodeIgniter 4-based CMS skeleton. Prior to version 0.31.0.0, the application fails to properly sanitize user-controlled input when creating or editing blog posts. An attacker can inject a malicious JavaScript payload into blog post content, which is stored server-side and later rendered unsafely in multiple application views without proper output encoding. This issue has been patched in version 0.31.0.0.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-34567	CI4MS Stored XSS via Blog Post Categories Section Without Output Encoding	CI4MS is a CodeIgniter 4-based CMS skeleton. Prior to version 0.31.0.0, the application fails to properly sanitize user-controlled input when creating or editing blog posts within the Categories section. An attacker can inject a malicious JavaScript payload into the Categories content, which is then stored server-side. This stored payload is later rendered unsafely when the Categories are viewed via blog posts, without proper output encoding. This issue has been patched in version 0.31.0.0.	Patched by core rule	Y
CVE-2026-34566	CI4MS Stored DOM XSS via Page Management Input Fields	CI4MS is a CodeIgniter 4-based CMS skeleton. Prior to version 0.31.0.0, the application fails to properly sanitize user-controlled input within the Page Management functionality when creating or editing pages. Multiple input fields accept attacker-controlled JavaScript payloads that are stored server-side. These stored values are later rendered without proper output encoding across administrative page lists and public-facing page views, leading to stored DOM-based cross-site scripting. This issue has been patched in version 0.31.0.0.	Patched by core rule	Y
CVE-2026-34565	CI4MS Stored DOM XSS via Posts in Menu Management Navigation	CI4MS is a CodeIgniter 4-based CMS skeleton. Prior to version 0.31.0.0, the application fails to properly sanitize user-controlled input when adding Posts to navigation menus through the Menu Management functionality. Post-related data selected via the Posts section is stored server-side and rendered without proper output encoding within administrative dashboards and public-facing navigation	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		menus. This issue has been patched in version 0.31.0.0.		
CVE-2026-34564	CI4MS Stored DOM XSS via Pages in Menu Management Navigation	CI4MS is a CodeIgniter 4-based CMS skeleton. Prior to version 0.31.0.0, the application fails to properly sanitize user-controlled input when adding Pages to navigation menus through the Menu Management functionality. Page-related data selected via the Pages section is stored server-side and rendered without proper output encoding within administrative interfaces and public-facing navigation menus. This issue has been patched in version 0.31.0.0.	Patched by core rule	Y
CVE-2026-34563	CI4MS Stored Blind XSS via Backup Filename Injected via SQL into Backup Management Views	CI4MS is a CodeIgniter 4-based CMS skeleton. Prior to version 0.31.0.0, the application fails to properly sanitize user-controlled input when handling backup uploads and processing backup metadata. An attacker can inject a malicious JavaScript payload into the backup filename via the uploaded xss.sql, which uses SQL functionality to insert the XSS payload server-side. This stored payload is later rendered unsafely in multiple backup management views without proper output encoding. This issue has been patched in version 0.31.0.0.	Patched by core rule	Y
CVE-2026-34562	CI4MS Stored XSS via System Settings Company Information Fields	CI4MS is a CodeIgniter 4-based CMS skeleton. Prior to version 0.31.0.0, the application fails to properly sanitize user-controlled input within System Settings Company Information. Several administrative configuration fields accept attacker-controlled input that is stored server-side and later rendered without proper output encoding. This issue	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		has been patched in version 0.31.0.0.		
CVE-2026-34561	CI4MS Stored XSS via Social Media Configuration Fields in System Settings	CI4MS is a CodeIgniter 4-based CMS skeleton. Prior to version 0.31.0.0, the application fails to properly sanitize user-controlled input within System Settings Social Media Management. Multiple configuration fields including Social Media and Social Media Link accept attacker-controlled input that is stored server-side and later rendered without proper output encoding. This issue has been patched in version 0.31.0.0.	Patched by core rule	Y
CVE-2026-34560	CI4MS Stored Blind XSS via Logged Data Rendered in Logs Interface for Admins	CI4MS is a CodeIgniter 4-based CMS skeleton. Prior to version 0.31.0.0, the application renders user-controlled input unsafely within the logs interface. If any stored XSS payload exists within logged data, it is rendered without proper output encoding. The payload is stored within application logs and only executes later when an administrator views the logs page, resulting in a Blind XSS scenario. This issue has been patched in version 0.31.0.0.	Patched by core rule	Y
CVE-2026-34559	CI4MS Stored XSS via Blog Tag Name Rendered Across Public and Admin Interfaces	CI4MS is a CodeIgniter 4-based CMS skeleton. Prior to version 0.31.0.0, the application fails to properly sanitize user-controlled input when creating or editing blog tags. An attacker can inject a malicious JavaScript payload into the tag name field, which is stored server-side. This stored payload is later rendered unsafely across public tag pages and administrative interfaces without proper output encoding. This issue has been patched in version 0.31.0.0.	Patched by core rule	Y
CVE-2026-34530	File Browser Stored XSS via Admin	File Browser is a file managing interface. Prior to	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	branding.name Field Affecting All Visitors	version 2.62.2, the SPA index page in File Browser is vulnerable to Stored Cross-Site Scripting via admin-controlled branding fields. An admin who sets branding.name to a malicious payload injects persistent JavaScript that executes for ALL visitors, including unauthenticated users. This issue has been patched in version 2.62.2.		
CVE-2026-34529	File Browser Stored XSS via JavaScript Embedded in Crafted EPUB File Preview	File Browser is a file managing interface. Prior to version 2.62.2, the EPUB preview function in File Browser is vulnerable to Stored Cross-Site Scripting. JavaScript embedded in a crafted EPUB file executes in the victim's browser when they preview the file. This issue has been patched in version 2.62.2.	Patched by core rule	Y
CVE-2026-33978	Notesnook Stored XSS via Clip Metadata Title Injected into innerHTML in Share WebView	Notesnook is a note-taking app focused on user privacy. Prior to version 3.3.17, a stored XSS vulnerability exists in the mobile share/web clip flow because attacker-controlled clip metadata is concatenated into HTML without escaping and then rendered with innerHTML inside the mobile share editor WebView. An attacker can control the shared title metadata and inject HTML. When the victim opens the Notesnook share flow and selects Web clip, the payload is inserted into the generated HTML and executed in the mobile editor WebView. This issue has been patched in version 3.3.17.	Patched by core rule	Y
CVE-2026-30526	SourceCodester Zoo Management System Reflected XSS via msg Parameter in Login Page	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Zoo Management System v1.0. The vulnerability is located in the login page, specifically	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		within the msg parameter. The application reflects the content of the msg parameter back to the user without proper HTML encoding or sanitization. This allows remote attackers to inject arbitrary web script or HTML via a crafted URL.		
CVE-2026-3877	VertiGIS FM Reflected XSS via Dashboard Search Functionality	A reflected cross-site scripting (XSS) vulnerability in the dashboard search functionality of the VertiGIS FM solution allows attackers to craft a malicious URL, that if visited by an authenticated victim, will execute arbitrary JavaScript in the victim's context.	Patched by core rule	Y
CVE-2026-21631	Joomla Multilingual Associations Component XSS via Missing Output Escaping	Lack of output escaping leads to a XSS vector in the multilingual associations component.	Patched by core rule	Y
CVE-2026-5255	Simple Laundry System XSS via userid Parameter in delstaffinfo.php	A vulnerability was detected in code-projects Simple Laundry System 1.0. This affects an unknown part of the file /delstaffinfo.php of the component Parameter Handler. The manipulation of the argument userid 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-2026-35057	XenForo Stored XSS via Structured Text Mentions in Legacy Profile Posts	XenForo before 2.3.10 and before 2.2.19 is vulnerable to stored cross-site scripting (XSS) in structured text mentions, primarily affecting legacy profile post content. An attacker can inject malicious scripts through crafted mentions that are stored and executed when other users view the content.	Patched by core rule	Y
CVE-2026-34605	SiYuan XSS via Namespace-Prefixed Element Names Bypassing SanitizeSVG in getDynamicIcon	SiYuan is a personal knowledge management system. From version 3.6.0 to before version 3.6.2, the SanitizeSVG function can be bypassed by using	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		namespace-prefixed element names such as x:script. The Go HTML5 parser records the element's tag as x:script rather than script, so the tag check passes it through. The SVG is served with Content-Type: image/svg+xml and no Content Security Policy; when a browser opens the response directly, its XML parser resolves the prefix to the SVG namespace and executes the embedded script. This issue has been patched in version 3.6.2.		
CVE-2026-34585	SiYuan Stored XSS to RCE via Block Attribute HTML Entity Mixing in .sy Document Import	SiYuan is a personal knowledge management system. Prior to version 3.6.2, a vulnerability allows crafted block attribute values to bypass server-side attribute escaping when an HTML entity is mixed with raw special characters. An attacker can embed a malicious IAL value inside a .sy document, package it as a .sy.zip, and have the victim import it. Once the note is opened, the malicious attribute breaks out of its original HTML context and injects an event handler, resulting in stored XSS. In the Electron desktop client, this XSS reaches remote code execution. This issue has been patched in version 3.6.2.	Patched by core rule	Y
CVE-2026-34448	SiYuan Stored XSS to RCE via Attacker-Controlled coverURL in Gallery/Kanban View	SiYuan is a personal knowledge management system. Prior to version 3.6.2, an attacker who can place a malicious URL in an Attribute View field can trigger stored XSS when a victim opens the Gallery or Kanban view with Cover From Asset Field enabled. The vulnerable code accepts arbitrary http(s) URLs without extensions as images and injects it directly into an img src attribute without	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		escaping. In the Electron desktop client, the injected JavaScript executes with nodeIntegration enabled and contextIsolation disabled, so the XSS reaches arbitrary OS command execution. This issue has been patched in version 3.6.2.		
CVE-2026-34405	Nuxt OG Image XSS via Arbitrary Attribute Injection in Image Generation Component	Nuxt OG Image generates OG Images with Vue templates in Nuxt. Prior to version 6.2.5, the image generation component by the URI /_og/d/ contains a vulnerability that allows injection of arbitrary attributes into the HTML page body. This issue has been patched in version 6.2.5.	Patched by core rule	Y
CVE-2026-34739	WWBN AVideo Reflected XSS via ip Parameter in User_Location testIP.php	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the User_Location plugin's testIP.php page reflects the ip request parameter directly into an HTML input element without applying htmlspecialchars() or any other output encoding. This allows an attacker to inject arbitrary HTML and JavaScript via a crafted URL. Although the page is restricted to admin users, AVideo's SameSite=None cookie configuration allows cross-origin exploitation. At time of publication, there are no publicly available patches.	Patched by core rule	Y
CVE-2026-34716	WWBN AVideo XSS via Caller Display Name in YPTSocket jQuery Toast Heading Parameter	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the AVideo YPTSocket plugin's caller feature renders incoming call notifications using the jQuery Toast Plugin, passing the caller's display name directly as the heading parameter. The toast plugin constructs the heading as raw HTML and inserts it into the DOM via jQuery's .html() method. An attacker can set	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		their display name to an XSS payload and trigger code execution on any online user's browser simply by initiating a call. At time of publication, there are no publicly available patches.		
CVE-2026-34396	WWBN AVideo Stored XSS via Plugin Config Values in jsonToFormElements() Without Encoding	WWBN AVideo is an open source video platform. In versions 26.0 and prior, the AVideo admin panel renders plugin configuration values in HTML forms without applying htmlspecialchars() or any other output encoding. The jsonToFormElements() function in admin/functions.php directly interpolates user-controlled values into textarea contents, option elements, and input attributes. An attacker who can set a plugin configuration value can inject arbitrary JavaScript that executes whenever any administrator visits the plugin configuration page. At time of publication, there are no publicly available patches.	Patched by core rule	Y
CVE-2026-34231	Slippers Django XSS via Unescaped Context Variable in {% attrs %} Template Tag	Slippers is a UI component framework for Django. Prior to version 0.6.3, a Cross-Site Scripting (XSS) vulnerability exists in the {% attrs %} template tag of the slippers Django package. When a context variable containing untrusted data is passed to {% attrs %}, the value is interpolated into an HTML attribute string without escaping, allowing an attacker to break out of the attribute context and inject arbitrary HTML or JavaScript into the rendered page. This issue has been patched in version 0.6.3.	Patched by core rule	Y
CVE-2026-34558	CI4MS Stored DOM XSS via Methods Management Input Fields in Admin and Navigation	CI4MS is a CodeIgniter 4-based CMS skeleton. Prior to version 0.31.0.0, the application fails to properly sanitize user-controlled input	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		within the Methods Management functionality. Multiple input fields accept attacker-controlled JavaScript payloads that are stored server-side without sanitization or output encoding. These stored values are later rendered directly into administrative interfaces and global navigation components without proper encoding. This issue has been patched in version 0.31.0.0.		
CVE-2026-34557	CI4MS Stored XSS via Group and Role Management Fields in Privileged Admin Views	CI4MS is a CodeIgniter 4-based CMS skeleton. Prior to version 0.31.0.0, the application fails to properly sanitize user-controlled input within group and role management functionality. Multiple input fields can be injected with malicious JavaScript payloads, which are stored server-side and later rendered unsafely within privileged administrative views without proper output encoding. This issue has been patched in version 0.31.0.0.	Patched by core rule	Y
CVE-2026-27599	CI4MS Stored XSS via Mail Settings Configuration Fields	CI4MS is a CodeIgniter 4-based CMS skeleton. Prior to version 0.31.0.0, the application fails to properly sanitize user-controlled input within System Settings Mail Settings. Several configuration fields including Mail Server, Mail Port, Email Address, Email Password, Mail Protocol, and TLS settings accept attacker-controlled input that is stored server-side and later rendered without proper output encoding. This issue has been patched in version 0.31.0.0.	Patched by core rule	Y
CVE-2026-32275	Tautulli XSS via Unsanitized JSONP Callback Parameter Enabling API Key Theft	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. From version 1.3.10 to before	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		version 2.17.0, an unsanitized JSONP callback parameter allows cross-origin script injection and API key theft. This issue has been patched in version 2.17.0.		
CVE-2026-30562	SourceCodester Sales and Inventory Reflected XSS via msg in add_stock.php	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the add_stock.php file via the msg parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	Patched by core rule	Y
CVE-2026-30561	SourceCodester Sales and Inventory Reflected XSS via msg in add_purchase.php	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the add_purchase.php file via the msg parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	Patched by core rule	Y
CVE-2026-30560	SourceCodester Sales and Inventory Reflected XSS via msg in add_supplier.php	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the add_supplier.php file via the msg parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	Patched by core rule	Y
CVE-2026-30559	SourceCodester Sales and Inventory Reflected XSS via msg in add_sales.php	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the add_sales.php file via the msg parameter. The application fails to sanitize the input, allowing remote attackers to inject	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		arbitrary web script or HTML via a crafted URL.		
CVE-2026-30558	SourceCodester Sales and Inventory Reflected XSS via msg in add_customer.php	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the add_customer.php file via the msg parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	Patched by core rule	Y
CVE-2026-30557	SourceCodester Sales and Inventory Reflected XSS via msg in add_category.php	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the add_category.php file via the msg parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	Patched by core rule	Y
CVE-2026-30556	SourceCodester Sales and Inventory Reflected XSS via msg in index.php	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the index.php file via the msg parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	Patched by core rule	Y
CVE-2026-30566	SourceCodester Sales and Inventory Reflected XSS via limit in view_customers.php	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the view_customers.php file via the limit parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-30565	SourceCodester Sales and Inventory Reflected XSS via limit in view_supplier.php	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the view_supplier.php file via the limit parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	Patched by core rule	Y
CVE-2026-30564	SourceCodester Sales and Inventory Reflected XSS via limit in view_payments.php	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the view_payments.php file via the limit parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	Patched by core rule	Y
CVE-2026-30563	SourceCodester Sales and Inventory Stored XSS via website Parameter in update_details.php	A Stored Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the update_details.php file. The application fails to sanitize the website parameter provided in a POST request. This allows authenticated attackers to inject arbitrary web script or HTML that is stored in the database and executed whenever the store details page is accessed.	Patched by core rule	Y
CVE-2026-33979	Express XSS Sanitizer Bypass via Silently Ignored Restrictive Configurations	Express XSS Sanitizer is Express middleware which sanitizes user input data to prevent Cross Site Scripting attacks. A vulnerability has been identified in versions prior to 2.0.2 where restrictive sanitization configurations are silently ignored. In version 2.0.2, the validation logic has been updated to respect explicitly provided empty	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		configurations. Now, if allowedTags or allowedAttributes are provided (even if empty), they are passed directly to sanitize-html without being overridden.		
CVE-2026-33976	Notesnook Stored XSS to RCE via Web Clipper Attacker-Controlled Attributes in Electron	Notesnook is a note-taking app. Prior to version 3.3.11 on Web/Desktop and 3.3.17 on Android/iOS, a stored XSS in the Web Clipper rendering flow can be escalated to remote code execution in the desktop app. The clipper preserves attacker-controlled attributes from the source page's root element and stores them inside web-clip HTML. When the clip is later opened, Notesnook renders that HTML into a same-origin, unsandboxed iframe using contentDocument.write. Event-handler attributes execute in the Notesnook origin. In the desktop app, this becomes RCE because Electron is configured with nodeIntegration: true and contextIsolation: false. Version 3.3.11 Web/Desktop and 3.3.17 Android/iOS patch the issue.	Patched by core rule	Y
CVE-2026-33955	Notesnook Stored XSS to RCE via Note History Comparison Viewer via dangerouslySetInnerHTML	Notesnook is a note-taking app. Prior to version 3.3.11 on Web/Desktop, a cross-site scripting vulnerability stored in the note history comparison viewer can escalate to remote code execution in a desktop application. The issue is triggered when an attacker-controlled note header is displayed using dangerouslySetInnerHTML without secure handling. When combined with the full backup and restore feature in the desktop application, this becomes remote code execution because Electron is configured with nodeIntegration: true and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		contextIsolation: false. Version 3.3.11 patches the issue.		
CVE-2026-33941	Handlebars CLI Precompiler JavaScript Injection via Template Filenames and CLI Options	Handlebars provides the power necessary to let users build semantic templates. In versions 4.0.0 through 4.7.8, the Handlebars CLI precompiler concatenates user-controlled strings including template file names and several CLI options directly into the JavaScript it emits, without any escaping or sanitization. An attacker who can influence template filenames or CLI arguments can inject arbitrary JavaScript that executes when the generated bundle is loaded in Node.js or a browser. Version 4.7.9 fixes the issue.	Patched by core rule	Y
CVE-2026-33916	Handlebars XSS via Prototype Pollution Triggering Unsanitized Partial Rendering	Handlebars provides the power necessary to let users build semantic templates. In versions 4.0.0 through 4.7.8, resolvePartial() in the Handlebars runtime resolves partial names via a plain property lookup on options.partials without guarding against prototype-chain traversal. When Object.prototype has been polluted with a string value whose key matches a partial reference in a template, the polluted string is used as the partial body and rendered without HTML escaping, resulting in reflected or stored XSS. Version 4.7.9 fixes the issue.	Patched by core rule	Y
CVE-2026-33739	FOG Stored XSS via Insufficient Sanitization in Management Page Listing Tables	FOG is a free open-source cloning/imaging/rescue suite/inventory management system. Prior to 1.5.10.1812, the listing tables on multiple management pages (Host, Storage, Group, Image, Printer, Snapin) are vulnerable to Stored Cross-Site Scripting, due to insufficient server-side	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		parameter sanitization in record creations/updates and a lack of HTML escaping in listing tables. Version 1.5.10.1812 patches the issue.		
CVE-2026-33045	Home Assistant XSS via Remaining Charge Time Sensor in Mobile Phone Device	Home Assistant is open source home automation software. Starting in version 2025.02 and prior to version 2026.01, the remaining charge time sensor for mobile phones is vulnerable to cross-site scripting, similar to CVE-2025-62172. Version 2026.01 fixes the issue.	Patched by core rule	Y
CVE-2026-33044	Home Assistant XSS via Malicious Device Entity Name in Map Card	Home Assistant is open source home automation software. Starting in version 2020.02 and prior to version 2026.01, an authenticated party can add a malicious name to their device entity, allowing for Cross-Site Scripting attacks against anyone who can see a dashboard with a Map-card which includes that entity. It requires that the victim hovers over an information point. Version 2026.01 fixes the issue.	Patched by core rule	Y
CVE-2026-34375	WWBN AVideo Reflected XSS via plugin Parameter in YPTWallet Stripe Confirmation Page	WWBN AVideo is an open source video platform. In versions up to and including 26.0, the YPTWallet Stripe payment confirmation page directly echoes the $_REQUEST['plugin'] parameter into a JavaScript block without any encoding or sanitization. An attacker can inject arbitrary JavaScript by crafting a malicious URL and sending it to a victim user. The same script block also outputs the current user's username and password hash, meaning a successful XSS exploitation can immediately exfiltrate these credentials. Commit fa0bc102493a15d79fe03f86	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		c07ab7ca1b5b63e2 fixes the issue.		
CVE-2026-30568	SourceCodester Sales and Inventory Reflected XSS via limit in view_purchase.php	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0 in the view_purchase.php file via the limit parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	Patched by core rule	Y
CVE-2026-30567	SourceCodester Sales and Inventory Reflected XSS via limit in view_product.php	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0 in the view_product.php file via the limit parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	Patched by core rule	Y
CVE-2026-30571	SourceCodester Sales and Inventory Reflected XSS via limit in view_category.php	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0 in the view_category.php file via the limit parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	Patched by core rule	Y
CVE-2026-30570	SourceCodester Sales and Inventory Reflected XSS via limit in view_sales.php	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0 in the view_sales.php file via the limit parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.	Patched by core rule	Y
CVE-2026-30569	SourceCodester Sales and Inventory Reflected XSS via limit in view_stock_availability.php	A Reflected Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Sales and Inventory System 1.0. The vulnerability is located in the view_stock_availability.php	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		file via the limit parameter. The application fails to sanitize the input, allowing remote attackers to inject arbitrary web script or HTML via a crafted URL.		
CVE-2026-30527	SourceCodester Online Food Ordering Stored XSS via Category Name in Admin Panel	A Stored Cross-Site Scripting (XSS) vulnerability exists in SourceCodester Online Food Ordering System v1.0 in the Category management module within the admin panel. The application fails to properly sanitize user input supplied to the Category Name field when creating or updating a category. When an administrator or user visits the Category list page, the injected JavaScript executes immediately in their browser.	Patched by core rule	Y
CVE-2025-61190	DSpace JSPUI Reflected XSS via filter_type_1 Parameter in Search/Discover	A Reflected Cross-Site Scripting (XSS) vulnerability has been identified in DSpace JSPUI 6.5 within the search/discover filtering functionality. The vulnerability exists due to improper sanitization of user-supplied input via the filter_type_1 parameter.	Patched by core rule	Y
CVE-2026-33664	Kestra Stored XSS via Flow YAML Metadata Fields Rendered via v-html Without Sanitization	Kestra is an open-source, event-driven orchestration platform. Versions up to and including 1.3.3 render user-supplied flow YAML metadata fields (description, inputs[].displayName, inputs[].description) through the Markdown.vue component instantiated with html: true. The resulting HTML is injected into the DOM via Vue's v-html without any sanitization. This allows a flow author to embed arbitrary JavaScript that executes in the browser of any user who views or interacts with the flow. As of time of publication, it is unclear if a patch is available.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-33653	Ulloady Stored XSS via Malicious Filename During File Upload	Ulloady is a file uploader script with multi-file upload support. A Stored Cross-Site Scripting (XSS) vulnerability exists in versions prior to 3.1.2 due to improper sanitization of filenames during the file upload process. An attacker can upload a file with a malicious filename containing JavaScript code, which is later rendered in the application without proper escaping. When the filename is displayed in the file list or file details page, the malicious script executes in the browser of any user who views the page. Version 3.1.2 fixes the issue.	Patched by core rule	Y
CVE-2026-33742	Invoice Ninja Stored XSS via Product Notes Markdown Rendering Without purify::clean()	Invoice Ninja is a source-available invoice, quote, project and time-tracking app. Product notes fields in Invoice Ninja v5.13.0 allow raw HTML via Markdown rendering, enabling stored XSS. The Markdown parser output was not sanitized with purify::clean() before being included in invoice templates. This is fixed in v5.13.4 by the vendor by adding purify::clean() to sanitize Markdown output.	Patched by core rule	Y
CVE-2026-33738	Lychee Stored XSS via photo description Rendered via Blade Unescaped Output in RSS Feed	Lychee is a free, open-source photo-management tool. Prior to version 7.5.3, the photo description field is stored without HTML sanitization and rendered using Blade unescaped output in the RSS, Atom, and JSON feed templates. The /feed endpoint is publicly accessible without authentication, allowing any RSS reader to execute attacker-controlled JavaScript. Version 7.5.3 fixes the issue.	Patched by core rule	Y
CVE-2026-33525	Authelia Reflected XSS via language Cookie	Authelia is an open-source authentication and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Value in HTML Template Rendering	authorization server. In version 4.39.15, an attacker may potentially be able to inject javascript into the Authelia login page if several conditions are met simultaneously. This is caused by the lack of neutralization of the language cookie value when rendering the HTML template. Unless both the script-src and connect-src CSP directives have been modified, this vulnerability is almost impossible to exploit. Users should upgrade to 4.39.16 or downgrade to 4.39.14 to mitigate the issue.		
CVE-2026-33506	Ory Polis DOM-Based XSS via callbackUrl Parameter Passed to router.push	Ory Polis, formerly known as BoxyHQ Jackson, bridges or proxies a SAML login flow to OAuth 2.0 or OpenID Connect. Versions prior to 26.2.0 contain a DOM-based Cross-Site Scripting (XSS) vulnerability in Ory Polis's login functionality. The application improperly trusts a URL parameter (callbackUrl), which is passed to router.push. An attacker can craft a malicious link that, when opened by an authenticated user, performs a client-side redirect and executes arbitrary JavaScript in the context of their browser. Version 26.2.0 contains a patch.	Patched by core rule	Y
CVE-2026-34071	Stirling-PDF XSS via Unsanitized HTML Email Body in /api/v1/convert/eml/pdf Endpoint	Stirling-PDF is a locally hosted web application that allows you to perform various operations on PDF files. In version 2.7.3, the /api/v1/convert/eml/pdf endpoint with parameter downloadHtml=true returns unsanitized HTML from the email body with Content-Type: text/html. An attacker who sends a malicious email to a Stirling-PDF user can achieve JavaScript execution when that user exports the	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		email using the Download HTML intermediate file feature. Version 2.8.0 fixes the issue.		
CVE-2026-30162	Timo XSS via Crafted Links in Title Field	Cross Site Scripting vulnerability in Timo 2.0.3 via crafted links in the title field.	Patched by core rule	Y
CVE-2026-29934	LightCMS Reflected XSS via Referer Header in /admin/menus Component	A reflected cross-site scripting (XSS) vulnerability in the /admin/menus component of Lightcms v2.0 allows attackers to execute arbitrary Javascript in the context of the user's browser via modifying the referer value in the request header.	Patched by core rule	Y
CVE-2026-29933	YZMCMS Reflected XSS via Referrer Header in Login Page	A reflected cross-site scripting (XSS) vulnerability in the /index/login.html component of YZMCMS v7.4 allows attackers to execute arbitrary Javascript in the context of the user's browser via modifying the referrer value in the request header.	Patched by core rule	Y
CVE-2018-25210	WebOfisi E-Ticaret SQL Injection via urun GET Parameter	WebOfisi E-Ticaret 4.0 contains an SQL injection vulnerability in the urun GET parameter of the endpoint that allows unauthenticated attackers to manipulate database queries. Attackers can inject SQL payloads through the urun parameter to execute boolean-based blind, error-based, time-based blind, and stacked query attacks against the backend database.	Patched by core rule	Y
CVE-2026-4849	Simple Laundry System XSS via firstName Parameter in modify.php	A vulnerability was identified in code-projects Simple Laundry System 1.0. This impacts an unknown function of the file /modify.php of the component Parameter Handler. The manipulation of the argument firstName leads to cross site scripting. The attack may be initiated remotely. The exploit is publicly available and might be used.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-33933	OpenEMR Reflected XSS via Custom Template Editor Allowing Unauthenticated Crafted URL	OpenEMR is a free and open source electronic health records and medical practice management application. Starting in version 7.0.2.1 and prior to version 8.0.0.3, a reflected cross-site scripting (XSS) vulnerability in the custom template editor allows an attacker to execute arbitrary JavaScript in an authenticated staff member's browser session by sending them a crafted URL. The attacker does not need an OpenEMR account. Version 8.0.0.3 patches the issue.	Patched by core rule	Y
CVE-2026-33348	OpenEMR Stored XSS via Eye Exam Form Answers in Patient Encounter Pages	OpenEMR is a free and open source electronic health records and medical practice management application. Versions prior to 8.0.0.3 have a stored cross-site scripting (XSS) vulnerability in the function to display the form answers, allowing any authenticated attacker with the specific role to insert arbitrary JavaScript into the system by entering malicious payloads to the form answers. The JavaScript code is later executed by any user with the form role when viewing the form answers in the patient encounter pages or visit history. Version 8.0.0.3 contains a patch.	Patched by core rule	Y

VULNERABILITY DETAILS

Advanced Injection Types

Advanced injection vulnerabilities include CRLF injection, NoSQL injection, server-side template injection (SSTI), KQL injection, iCalendar injection, FTP command injection, and unsandboxed script execution enabling RCE. These 9 CVEs span a broad range of attack vectors beyond traditional SQL and command injection. All are patched by AppTrana core rules.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-42037	Axios CRLF Header Injection via Unsanitized .type in FormDataPart Content-Type	Axios is a promise based HTTP client for the browser and Node.js. From 1.0.0 to before 1.15.1, the FormDataPart constructor in lib/helpers/formDataToStream.js interpolates value.type directly into the Content-Type header of each multipart part without sanitizing CRLF sequences. An attacker who controls the .type property of a Blob/File-like object can inject arbitrary MIME part headers into the multipart form-data body. This bypasses Node.js v18+ built-in header protections because the injection targets the multipart body structure, not HTTP request headers. This vulnerability is fixed in 1.15.1.	Patched by core rule	Y
CVE-2026-41264	Flowise RCE via Unsandboxed LLM-Generated Python Script Execution in CSV_Agents	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, the specific flaw exists within the run method of the CSV_Agents class. The issue results from the lack of proper sandboxing when evaluating an LLM generated python script.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Using prompt injection techniques, an unauthenticated attacker with the ability to send prompts to a chatflow using the CSV Agent node may convince an LLM to respond with a malicious python script that executes attacker controlled commands on the Flowise server. This vulnerability is fixed in 3.1.0.		
CVE-2026-41469	Beghelli Sicuro24 SicuroWeb Missing CSP Enabling Arbitrary External JavaScript Loading	Beghelli Sicuro24 SicuroWeb does not enforce a Content Security Policy, allowing unrestricted loading of external JavaScript resources from attacker-controlled origins. When chained with the template injection and sandbox escape vulnerabilities present in the same application, the absence of CSP removes the browser-enforced restriction that would otherwise block external script execution, enabling attackers to load arbitrary remote payloads into operator browser sessions.	Patched by core rule	Y
CVE-2026-40352	FastGPT NoSQL Injection via MongoDB Query Operators in Password Change Endpoint	FastGPT is an AI Agent building platform. In versions prior to 4.14.9.5, the password change endpoint is vulnerable to NoSQL injection. An authenticated attacker can bypass the old password verification by injecting MongoDB query operators. This allows an attacker who has gained a low-privileged session to change the password of their account or others without knowing the current one, leading to full account takeover and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		persistence. This issue has been fixed in version 4.14.9.5.		
CVE-2026-40351	FastGPT NoSQL Injection via MongoDB Query Operator in Password Login Enabling Auth Bypass	FastGPT is an AI Agent building platform. In versions prior to 4.14.9.5, the password-based login endpoint uses TypeScript type assertion without runtime validation, allowing an unauthenticated attacker to pass a MongoDB query operator object (e.g., {$ne: ''}) as the password field. This NoSQL injection bypasses the password check, enabling login as any user including the root administrator. This issue has been fixed in version 4.14.9.5.	Patched by core rule	Y
CVE-2026-35601	Vikunja iCalendar Injection via CRLF in Task Titles in CalDAV VTODO Output	Vikunja is an open-source self-hosted task management platform. Prior to 2.3.0, the CalDAV output generator builds iCalendar VTODO entries via raw string concatenation without applying RFC 5545 TEXT value escaping. User-controlled task titles containing CRLF characters break the iCalendar property boundary, allowing injection of arbitrary iCalendar properties such as ATTACH, VALARM, or ORGANIZER. This vulnerability is fixed in 2.3.0.	Patched by core rule	Y
CVE-2026-39983	basic-ftp FTP Command Injection via CRLF Sequences in File Path Parameters	basic-ftp is an FTP client for Node.js. Prior to 5.2.1, basic-ftp allows FTP command injection via CRLF sequences in file path parameters passed to high-level path APIs such as cd(), remove(), rename(),	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		uploadFrom(), downloadTo(), list(), and removeDir(). The library's protectWhitespace() helper only handles leading spaces and returns other paths unchanged, while FtpContext.send() writes the resulting command string directly to the control socket with CRLF appended. This lets attacker-controlled path strings split one intended FTP command into multiple commands. This vulnerability is fixed in 5.2.1.		
CVE-2026-28797	RAGFlow SSTI via Unsandboxed Jinja2 Template in StringTransform and Message Agent Components	RAGFlow is an open-source RAG (Retrieval-Augmented Generation) engine. In versions 0.24.0 and prior, a Server-Side Template Injection vulnerability exists in RAGFlow's Agent workflow Text Processing (StringTransform) and Message components. These components use Python's jinja2.Template (unsandboxed) to render user-supplied templates, allowing any authenticated user to execute arbitrary operating system commands on the server. At time of publication, there are no publicly available patches.	Patched by core rule	Y
CVE-2026-33980	Azure Data Explorer MCP Server KQL Injection via Unsanitized table_name in Query F-Strings	Azure Data Explorer MCP Server is a Model Context Protocol server that enables AI assistants to execute KQL queries and explore Azure Data Explorer databases. Versions up to and including 0.1.1 contain KQL injection vulnerabilities in three MCP tool handlers:	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		get_table_schema, sample_table_data, and get_table_details. The table_name parameter is interpolated directly into KQL queries via f-strings without any validation or sanitization, allowing an attacker or a prompt-injected AI agent to execute arbitrary KQL queries against the Azure Data Explorer cluster. Commit 0abe0ee55279e111281076393e5e966335fffd30 patches the issue.		

VULNERABILITY DETAILS

Remote Code Execution Vulnerability

Remote code execution vulnerabilities allow attackers to execute arbitrary commands on the target server. 1 critical unauthenticated RCE was identified in April 2026 and is patched by AppTrana core rules.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	WAS Coverage
CVE-2026-41268	Flowise Unauthenticated RCE via FILE-STORAGE:: Keyword and NODE_OPTIONS Environment Variable Injection	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, Flowise is vulnerable to a critical unauthenticated remote command execution vulnerability. It can be exploited via a parameter override bypass using the FILE-STORAGE:: keyword combined with a NODE_OPTIONS environment variable injection. This allows for the execution of arbitrary system commands with root privileges within the containerized Flowise instance, requiring only a single HTTP request and no authentication or knowledge of the instance. This vulnerability is fixed in 3.1.0.	Patched by core rule	Y

VULNERABILITY DETAILS

Malicious File Upload Vulnerabilities

File upload vulnerabilities allow attackers to upload and execute malicious files, commonly PHP web shells, by bypassing incomplete extension or MIME type blocklists. All 9 file upload CVEs in April 2026 are patched by AppTrana core rules.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-41269	Flowise RCE via MIME Type Bypass Enabling Malicious JavaScript Web Shell Upload	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, the Chatflow configuration file upload settings can be modified to allow the application/javascript MIME type. This lets an attacker upload .js files even though the frontend does not normally allow JavaScript uploads. This enables attackers to persistently store malicious Node.js web shells on the server, potentially leading to Remote Code Execution. This vulnerability is fixed in 3.1.0.	Patched by core rule	Y
CVE-2026-40488	OpenMage LTS RCE via Incomplete File Extension Blocklist Bypass in Custom Option File Upload	Magento Long Term Support (LTS) is an unofficial, community-driven project providing an alternative to the Magento Community Edition e-commerce platform. Prior to version 20.17.0, the product custom option file upload uses an incomplete blocklist (forbidden_extensions = php,exe) to prevent dangerous file uploads. This blocklist can be trivially bypassed by using alternative PHP-executable extensions such as .phtml, .phar, .php3, .php4, .php5, .php7, and .pht. Files are stored in the publicly accessible media/custom_options/quote/ directory, enabling Remote Code Execution if this directory is not explicitly denied script execution. Version 20.17.0 patches the issue.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-38526	Krayin CRM Authenticated Arbitrary File Upload RCE via /admin/tinymce/upload Endpoint	An authenticated arbitrary file upload vulnerability in the /admin/tinymce/upload endpoint of Webkul Krayin CRM v2.2.x allows attackers to execute arbitrary code via uploading a crafted PHP file.	Patched by core rule	Y
CVE-2026-35164	Brave CMS Authenticated RCE via Unrestricted PHP File Upload in CKEditor Upload	Brave CMS is an open-source CMS. Prior to 2.0.6, an unrestricted file upload vulnerability exists in the CKEditor upload functionality in app/Http/Controllers/Dashboard/CkEditorController.php within the ckupload method. The method fails to validate uploaded file types and relies entirely on user input. This allows an authenticated user to upload executable PHP scripts and gain Remote Code Execution. This vulnerability is fixed in 2.0.6.	Patched by core rule	Y
CVE-2026-5704	tar Hidden File Injection via Malicious Archive Bypassing Pre-Extraction Inspection	A flaw was found in tar. A remote attacker could exploit this vulnerability by crafting a malicious archive, leading to hidden file injection with fully attacker-controlled content. This bypasses pre-extraction inspection mechanisms, potentially allowing an attacker to introduce malicious files onto a system without detection.	Patched by core rule	Y
CVE-2019-25673	UniSharp Laravel File Manager Authenticated Arbitrary File Upload Enabling PHP Code Execution	UniSharp Laravel File Manager v2.0.0-alpha7 and v2.0 contain an arbitrary file upload vulnerability that allows authenticated attackers to upload malicious files by sending multipart form data to the upload endpoint. Attackers can upload PHP files with the type parameter set to Files and execute arbitrary code by accessing the uploaded file through the working directory path.	Patched by core rule	Y
CVE-2016-20052	Snews CMS Unauthenticated Unrestricted PHP File	Snews CMS 1.7 contains an unrestricted file upload vulnerability that allows	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Upload to snews_files Directory	unauthenticated attackers to upload arbitrary files including PHP executables to the snews_files directory. Attackers can upload malicious PHP files through the multipart form-data upload endpoint and execute them by accessing the uploaded file path to achieve remote code execution.		
CVE-2026-30280	Video Player Arbitrary File Overwrite via File Import Process	An arbitrary file overwrite vulnerability in RAREPROB SOLUTIONS PRIVATE LIMITED Video player Play All Videos v1.0.135 allows attackers to overwrite critical internal files via the file import process, leading to arbitrary code execution or information exposure.	Patched by core rule	Y
CVE-2025-32957	baserCMS RCE via Malicious PHP File in ZIP Archive Included via require_once Without Validation	baserCMS is a website development framework. Prior to version 5.2.3, the application's restore function allows users to upload a .zip file, which is then automatically extracted. A PHP file inside the archive is included using require_once without validating or restricting the filename. An attacker can craft a malicious PHP file within the zip and achieve arbitrary code execution when it is included. This issue has been patched in version 5.2.3.	Patched by core rule	Y

VULNERABILITY DETAILS

Code Injection Vulnerabilities

Code injection vulnerabilities allow attackers to inject and execute arbitrary code within the application context. April 2026 recorded 54 code injection CVEs, all protected by AppTrana core rules.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-6989	Tenda F453 Command Injection via TendaTelnet Function in Telnet Service	A vulnerability has been found in Tenda F453 up to 1.0.0.3. Impacted is the function TendaTelnet of the file /goform/telnet of the component Telnet Service. Such manipulation 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-2026-41137	Flowise Command Injection via Custom Pandas CSV Code in CSVAgent	Flowise is a drag & drop user interface to build a customized large language model flow. Prior to 3.1.0, the CSVAgent allows providing a custom Pandas CSV read code. Due to lack of sanitization, an attacker can provide a command injection payload that will get interpolated and executed by the server. This vulnerability is fixed in 3.1.0.	Patched by core rule	Y
CVE-2026-39842	OpenRemote RCE via Unsandboxed JavaScript Rules Engine and Unregistered Groovy Security Filter	OpenRemote is an open-source IoT platform. Versions 1.21.0 and below contain two interrelated expression injection vulnerabilities in the rules engine that allow arbitrary code execution on the server. The JavaScript rules engine executes user-supplied scripts via Nashorn's ScriptEngine.eval() without sandboxing, class filtering, or access restrictions, and the authorization check only restricts Groovy rules to superusers while leaving JavaScript rules unrestricted for any user with the write:rules role. Additionally, the Groovy rules engine has a GroovyDenyAllFilter that is defined but never registered, rendering the SandboxTransformer ineffective for superuser-created Groovy	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		rules. This issue has been fixed in version 1.22.0.		
CVE-2026-40287	PraisonAI Arbitrary Code Execution via Unsanitized Auto-Import of tools.py at Startup	PraisonAI is a multi-agent teams system. Versions 4.5.138 and below are vulnerable to arbitrary code execution through automatic, unsanitized import of a tools.py file from the current working directory. Components including call.py, tool_resolver.py, and CLI tool-loading paths blindly import ./tools.py at startup without any validation, sandboxing, or user confirmation. An attacker who can place a malicious tools.py in the directory where PraisonAI is launched achieves immediate arbitrary Python code execution in the host environment. This issue has been fixed in version 4.5.139.	Patched by core rule	Y
CVE-2026-6219	ytDownloader Command Injection via child_process.exec in Compressor Feature	A vulnerability was determined in aandrew-me ytDownloader up to 3.20.2. This affects the function child_process.exec of the file src/compressor.js of the component Compressor Feature. This manipulation causes command injection. The attack can only be executed locally. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-6110	MetaGPT Code Injection via generate_thoughts Function in Tree-of-Thought Solver	A vulnerability was identified in FoundationAgents MetaGPT up to 0.8.1. This affects the function generate_thoughts of the file metagpt/strategy/tot.py of the component Tree-of-Thought Solver. The manipulation leads to code injection. It is possible to initiate the attack remotely. The exploit is publicly available and might 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-2026-5970	MetaGPT Code Injection via check_solution in HumanEvalBenchmark/MBPPBenchmark	A vulnerability was detected in FoundationAgents MetaGPT up to 0.8.1. This affects the function check_solution of the component HumanEvalBenchmark/MBPPBenchmark. Performing a manipulation results in code injection. The attack may be initiated remotely. The exploit is now public and may be	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		used. The project was informed of the problem early through a pull request but has not reacted yet.		
CVE-2026-34197	Apache ActiveMQ RCE via Jolokia JMX Bridge Loading Remote Spring XML Application Context	Improper Input Validation, Improper Control of Generation of Code vulnerability in Apache ActiveMQ. Apache ActiveMQ Classic exposes the Jolokia JMX-HTTP bridge at /api/jolokia/ on the web console. The default Jolokia access policy permits exec operations on all ActiveMQ MBeans including BrokerService.addNetworkConnector(String) and BrokerService.addConnector(String). An authenticated attacker can invoke these operations with a crafted discovery URI that triggers the VM transport's brokerConfig parameter to load a remote Spring XML application context using ResourceXmlApplicationContext, enabling arbitrary code execution on the broker's JVM. This issue affects Apache ActiveMQ before 5.19.4 and 6.0.0 before 6.2.3.	Patched by core rule	Y
CVE-2026-5594	premsql Code Injection via eval() in followup.py result Argument	A weakness has been identified in premAI-io premsql up to 0.2.1. Affected is the function eval of the file premsql/agents/baseline/workers/followup.py. This manipulation of the argument result causes code injection. 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-2026-5577	cross_browser SQL Injection via ID Argument in details Endpoint	A vulnerability has been found in Song-Li cross_browser up to ca690f0fe6954fd9bcda36d071b68ed8682a786a. This affects an unknown part of the file flask/uniquemachine_app.py of the component details Endpoint. Such manipulation of the argument ID leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-5562	kafka-ui Code Injection via validateAccess in	A vulnerability was identified in provectus kafka-ui up to 0.7.2. This impacts the function	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	/api/smartfilters/testexecutions	validateAccess of the file /api/smartfilters/testexecutions of the component Endpoint. The manipulation leads to code injection. The attack can be initiated remotely. The exploit is publicly available and might be used.		
CVE-2026-5368	Car Rental Project SQL Injection via uname Parameter in login.php	A vulnerability was determined in projectworlds Car Rental Project 1.0. The affected element is an unknown function of the file /login.php of the component Parameter Handler. This manipulation of the argument uname causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-5339	Tenda G103 Command Injection via Multiple Parameters in action_set_net_settings	A vulnerability was detected in Tenda G103 1.0.0.5. The impacted element is the function action_set_net_settings of the file gpon.lua of the component Setting Handler. Performing a manipulation of the argument authLoid/authLoidPassword/authPassword/authSerialNo/authType/oltType/usVlanId/usVlanPriority results in command injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-5338	Tenda G103 Command Injection via lanIp in action_set_system_settings	A security vulnerability has been detected in Tenda G103 1.0.0.5. The affected element is the function action_set_system_settings of the file system.lua of the component Setting Handler. Such manipulation of the argument lanIp leads to command injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-5334	Online Enrollment System SQL Injection via deptid in index.php	A weakness has been identified in itsourcecode Online Enrollment System 1.0. Impacted is an unknown function of the file /enrollment/index.php?view=edit&id=3 of the component Parameter Handler. This manipulation of the argument deptid causes sql	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.		
CVE-2026-5333	Content-Management-System Command Injection via host Argument in /admin/tools.php	A security flaw has been discovered in DefaultFuction Content-Management-System 1.0. This issue affects some unknown processing of the file /admin/tools.php. The manipulation of the argument host results in command 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-2026-1540	SpamProtect WordPress Plugin RCE via PHP File Logging with Crafted Header	The Spam Protect for Contact Form 7 WordPress plugin before 1.2.10 allows logging to a PHP file, which could allow an attacker with editor access to achieve Remote Code Execution by using a crafted header.	Patched by core rule	Y
CVE-2026-29014	MetInfo CMS Unauthenticated PHP Code Injection Enabling Remote Code Execution	MetInfo CMS versions 7.9, 8.0, and 8.1 contain an unauthenticated PHP code injection vulnerability that allows remote attackers to execute arbitrary code by sending crafted requests with malicious PHP code. Attackers can exploit insufficient input neutralization in the execution path to achieve remote code execution and gain full control over the affected server.	Patched by core rule	Y
CVE-2026-5257	Simple Laundry System SQL Injection via userid in delstaffinfo.php	A vulnerability has been found in code-projects Simple Laundry System 1.0. This issue affects some unknown processing of the file /delstaffinfo.php of the component Parameter Handler. Such manipulation of the argument userid leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y
CVE-2026-5256	Simple Laundry System SQL Injection via firstName in modify.php	A flaw has been found in code-projects Simple Laundry System 1.0. This vulnerability affects unknown code of the file /modify.php of the component Parameter Handler. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		manipulation of the argument firstName causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.		
CVE-2026-5184	TRENDnet TEW-713RE Command Injection via admuser in /goform/setSysAdm	A vulnerability was identified in TRENDnet TEW-713RE up to 1.02. The impacted element is an unknown function of the file /goform/setSysAdm. The manipulation of the argument admuser leads to command injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	Patched by core rule	Y
CVE-2026-5183	TRENDnet TEW-713RE Command Injection via dest in sub_421494 of /goform/addRouting	A vulnerability was determined in TRENDnet TEW-713RE up to 1.02. The affected element is the function sub_421494 of the file /goform/addRouting. Executing a manipulation of the argument dest can lead to command injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-5178	Totolink A3300R Command Injection via vlanPriLan3 in setIptvCfg	A security vulnerability has been detected in Totolink A3300R 17.0.0cu.557_b20221024. Affected by this issue is the function setIptvCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument vlanPriLan3 leads to command injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-5177	Totolink A3300R Command Injection via rxRate in setWiFiBasicCfg	A weakness has been identified in Totolink A3300R 17.0.0cu.557_b20221024. Affected by this vulnerability is the function setWiFiBasicCfg of the file /cgi-bin/cstecgi.cgi. Executing a manipulation of the argument rxRate can lead to command injection. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.	Patched by core rule	Y
CVE-2026-34041	act Environment Injection via	act is a project which allows for local running of github actions.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	Deprecated ::set-env:: and ::add-path:: Workflow Commands	Prior to version 0.2.86, act unconditionally processes the deprecated ::set-env:: and ::add-path:: workflow commands, which was disabled due to environment injection risks. When a workflow step echoes untrusted data to stdout, an attacker can inject these commands to set arbitrary environment variables or modify the PATH for all subsequent steps in the job. This issue has been patched in version 0.2.86.		
CVE-2026-5176	Totolink A3300R Command Injection via setSyslogCfg in /cgi-bin/cstecgi.cgi	A security flaw has been discovered in Totolink A3300R 17.0.0cu.557_b20221024. Affected is the function setSyslogCfg of the file /cgi-bin/cstecgi.cgi. Performing a manipulation of the argument provided results in command injection. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y
CVE-2026-5153	Tenda CH22 Command Injection via mac in FormWriteFacMac of /goform/WriteFacMac	A flaw has been found in Tenda CH22 1.0.0.1. The affected element is the function FormWriteFacMac of the file /goform/WriteFacMac. Executing a manipulation of the argument mac can lead to command injection. The attack may be launched remotely. The exploit has been published and may be used.	Patched by core rule	Y
CVE-2026-28505	Tautulli Sandbox Escape via Lambda Nested Code Object Bypassing str_eval() co_names Check	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. Prior to version 2.17.0, the str_eval() function in notification_handler.py implements a sandboxed eval() for notification text templates. The sandbox attempts to restrict callable names by inspecting code.co_names of the compiled code object. However, co_names only contains names from the outer code object. When a lambda expression is used, it creates a nested code object whose attribute accesses are stored in code.co_consts, NOT in code.co_names. The sandbox never inspects nested code	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		objects. This issue has been patched in version 2.17.0.		
CVE-2026-5105	Totolink A3300R Command Injection via pptpPassThru in setVpnPassCfg	A vulnerability was detected in Totolink A3300R 17.0.0cu.557_b20221024. The affected element is the function setVpnPassCfg of the file /cgi-bin/cstecgi.cgi of the component Parameter Handler. Performing a manipulation of the argument pptpPassThru results in command injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-5104	Totolink A3300R Command Injection via ip in setStaticRoute	A security vulnerability has been detected in Totolink A3300R 17.0.0cu.557_b20221024. Impacted is the function setStaticRoute of the file /cgi-bin/cstecgi.cgi. Such manipulation of the argument ip leads to command injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	Patched by core rule	Y
CVE-2026-5103	Totolink A3300R Command Injection via enable in setUPnPCfg	A weakness has been identified in Totolink A3300R 17.0.0cu.557_b20221024. This issue affects the function setUPnPCfg of the file /cgi-bin/cstecgi.cgi. This manipulation of the argument enable causes command injection. 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-2026-5102	Totolink A3300R Command Injection via qos_up_bw in setSmartQosCfg	A security flaw has been discovered in Totolink A3300R 17.0.0cu.557_b20221024. This vulnerability affects the function setSmartQosCfg of the file /cgi-bin/cstecgi.cgi of the component Parameter Handler. The manipulation of the argument qos_up_bw results in command 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-2026-5101	Totolink A3300R Command Injection	A vulnerability was identified in Totolink A3300R 17.0.0cu.557_b20221024. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
	via lanIp in setLanCfg	affects the function setLanCfg of the file /cgi-bin/cstecgi.cgi of the component Parameter Handler. The manipulation of the argument lanIp leads to command injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.		
CVE-2026-5035	Accounting System SQL Injection via en_id in view_work.php	A vulnerability has been found in code-projects Accounting System 1.0. This affects an unknown part of the file /view_work.php of the component Parameter Handler. Such manipulation of the argument en_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-2026-5034	Accounting System SQL Injection via cos_id in edit_costumer.php	A flaw has been found in code-projects Accounting System 1.0. Affected by this issue is some unknown functionality of the file /edit_costumer.php of the component Parameter Handler. This manipulation of the argument cos_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-2026-5033	Accounting System SQL Injection via cos_id in view_costumer.php	A vulnerability was detected in code-projects Accounting System 1.0. Affected by this vulnerability is an unknown functionality of the file /view_costumer.php of the component Parameter Handler. The manipulation of the argument cos_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-2026-5030	Totolink NR1800X Command Injection via host_time in NTPSyncWithHost	A vulnerability has been found in Totolink NR1800X 9.1.0u.6279_B20210910. This issue affects the function NTPSyncWithHost of the file /cgi-bin/cstecgi.cgi of the component Telnet Service. The manipulation of the argument host_time leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2026-5020	Totolink A3600R Command Injection via NoticeUrl in setNoticeCfg	A vulnerability was detected in Totolink A3600R 4.1.2cu.5182_B20201102. Affected by this issue is the function setNoticeCfg of the file /cgi-bin/cstecgi.cgi of the component Parameter Handler. The manipulation of the argument NoticeUrl results in command injection. The attack may be launched remotely. The exploit is now public and may be used.	Patched by core rule	Y
CVE-2026-5019	Simple Food Order System SQL Injection via Status in all-orders.php	A security vulnerability has been detected in code-projects Simple Food Order System 1.0. Affected by this vulnerability is an unknown functionality of the file all-orders.php of the component Parameter Handler. The manipulation of the argument Status 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-2026-5018	Simple Food Order System SQL Injection via Name in register-router.php	A weakness has been identified in code-projects Simple Food Order System 1.0. Affected is an unknown function of the file register-router.php of the component Parameter Handler. Executing a manipulation of the argument Name 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-2026-5017	Simple Food Order System SQL Injection via Status in /all-tickets.php	A security flaw has been discovered in code-projects Simple Food Order System 1.0. This impacts an unknown function of the file /all-tickets.php of the component Parameter Handler. Performing a manipulation of the argument Status 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-2026-33943	Happy DOM RCE via Template Literal Backtick Bypass in ECMAScriptModule Compiler export {} Declarations	Happy DOM is a JavaScript implementation of a web browser without its graphical user interface. In versions 15.10.0 through 20.8.7, a code injection vulnerability in	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		ECMAScriptModuleCompiler allows an attacker to achieve Remote Code Execution by injecting arbitrary JavaScript expressions inside export { } declarations in ES module scripts processed by happy-dom. The compiler directly interpolates unsanitized content into generated code as an executable expression, and the quote filter does not strip backticks, allowing template literal-based payloads to bypass sanitization. Version 20.8.8 fixes the issue.		
CVE-2026-33938	Handlebars RCE via @partial-block AST Overwrite Using Helper-Writable Context Data	Handlebars provides the power necessary to let users build semantic templates. In versions 4.0.0 through 4.7.8, the @partial-block special variable is stored in the template data context and is reachable and mutable from within a template via helpers that accept arbitrary objects. When a helper overwrites @partial-block with a crafted Handlebars AST, a subsequent invocation of {{> @partial-block}} compiles and executes that AST, enabling arbitrary JavaScript execution on the server. Version 4.7.9 fixes the issue.	Patched by core rule	Y
CVE-2026-33881	Windmill Code Injection via Unescaped Single Quotes in Workspace Environment Variables in NativeTS Executor	Windmill is an open-source developer platform for internal code. Workspace environment variable values are interpolated into JavaScript string literals without escaping single quotes in the NativeTS executor. A workspace admin who sets a custom environment variable with a value containing a single quote can inject arbitrary JavaScript that executes inside every NativeTS script in that workspace. Version 1.664.0 patches the issue.	Patched by core rule	Y
CVE-2026-33654	nanobot Indirect Prompt Injection via Malicious Email Enabling Zero-Click LLM Tool Execution	nanobot is a personal AI assistant. Prior to version 0.1.6, an indirect prompt injection vulnerability exists in the email channel processing module, allowing a remote unauthenticated attacker to execute arbitrary LLM instructions and subsequently	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		system tools without any interaction from the bot owner. By sending an email containing malicious prompts to the bot's monitored email address, the bot automatically polls, ingests, and processes the email content as highly trusted input, fully bypassing channel isolation and resulting in a stealthy, zero-click attack. Version 0.1.6 patches the issue.		
CVE-2026-4963	smolagents Code Injection via Incomplete Fix for CVE-2025-9959 in local_python_executor.py	A weakness has been identified in huggingface smolagents 1.25.0.dev0. This affects the function evaluate_augassign/evaluate_call/evaluate_with of the file src/smolagents/local_python_executor.py of the component Incomplete Fix CVE-2025-9959. This manipulation causes code 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-2025-15616	Wazuh Shell Injection via logcollector Config, SMTP Tags, and Kaspersky AR Script Parameters	Wazuh wazuh-agent and wazuh-manager versions 2.1.0 before 4.8.0 contain multiple shell injection and untrusted search path vulnerabilities that allow attackers to execute arbitrary commands through various components including logcollector configuration, maild SMTP server tags, and Kaspersky AR script parameters. Attackers can exploit these vulnerabilities by injecting malicious commands through configuration files, SMTP server settings, and custom flags to achieve remote code execution on affected systems.	Patched by core rule	Y
CVE-2026-32695	Traefik Rule Injection via Unescaped Knative hosts[] and headers[].exact Values in Router Rules	Traefik is an HTTP reverse proxy and load balancer. Prior to versions 3.6.11 and 3.7.0-ea.2, Traefik's Knative provider builds router rules by interpolating user-controlled values into backtick-delimited rule expressions without escaping. In live cluster validation, Knative rules[].hosts[] was exploitable for host restriction bypass, and	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		Knative headers[].exact also allows rule-syntax injection. In multi-tenant clusters, this can route unauthorized traffic to victim services and lead to cross-tenant traffic exposure. Versions 3.6.11 and 3.7.0-ea.2 patch the issue.		
CVE-2026-4908	Simple Laundry System SQL Injection via userid in modstaffinfo.php	A security flaw has been discovered in code-projects Simple Laundry System 1.0. This affects an unknown function of the file /modstaffinfo.php of the component Parameter Handler. The manipulation of the argument userid 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.	Patched by core rule	Y
CVE-2026-33622	PinchTab Arbitrary JavaScript Execution via fn Mode in POST /wait Bypassing allowEvaluate Policy	PinchTab is a standalone HTTP server that gives AI agents direct control over a Chrome browser. PinchTab v0.8.3 through v0.8.5 allow arbitrary JavaScript execution through POST /wait and POST /tabs/{id}/wait when the request uses fn mode, even if security.allowEvaluate is disabled. POST /evaluate correctly enforces the security.allowEvaluate guard, which is disabled by default. However, in the affected releases, POST /wait accepted a user-controlled fn expression, embedded it directly into executable JavaScript, and evaluated it in the browser context without checking the same policy. Exploitation still requires authenticated API access. As of time of publication, a patched version is not yet available.	Patched by core rule	Y
CVE-2026-33148	Tandoor Recipes Parameter Injection via Unencoded query in FDC Search URL Construction	Tandoor Recipes is an application for managing recipes, planning meals, and building shopping lists. In versions prior to 2.6.0, the FDC search endpoint constructs an upstream API URL by directly interpolating the user-supplied query parameter into the URL string without URL-encoding. An attacker can inject additional URL parameters by including & characters in the query value. This	Patched by core rule	Y

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
		allows overriding the API key, manipulating upstream query behavior, and causing server crashes via malformed requests. Version 2.6.0 patches the issue.		
CVE-2026-4850	Simple Laundry System SQL Injection via Long-arm-shirtVol in checkregisitem.php	A security flaw has been discovered in code-projects Simple Laundry System 1.0. Affected is an unknown function of the file /checkregisitem.php of the component Parameter Handler. The manipulation of the argument Long-arm-shirtVol results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	Patched by core rule	Y
CVE-2026-4826	Sales and Inventory System SQL Injection via sid in update_stock.php	A vulnerability was determined in SourceCodester Sales and Inventory System 1.0. This vulnerability affects unknown code of the file /update_stock.php of the component HTTP GET Parameter Handler. This manipulation of the argument sid causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	Patched by core rule	Y
CVE-2026-4825	Sales and Inventory System SQL Injection via sid in update_sales.php	A vulnerability was found in SourceCodester Sales and Inventory System 1.0. This affects an unknown part of the file /update_sales.php of the component HTTP GET Parameter Handler. The manipulation of the argument sid 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

INDUSFACE™

DALLAS | BENGALURU | VADODARA | MUMBAI | NEW DELHI

Contact Us: +1 866 458 3058, +91 265 6133021

sales@indusface.com | indusface.com