INDUSFACE™

ZERO-DAY VULNERABILITY REPORT

• MONTHLY BULLETIN · OCTOBER 2026

Zero-Day Vulnerability Coverage Report

October 2026: AppTrana's WAF rules covered 3,745 newly disclosed vulnerabilities. All were blocked autonomously, keeping the exposure window close to zero.

3,745	100%	19	34
ZERO-DAYS BLOCKED	CATEGORY COVERAGE	CISA KEV BLOCKED	AGENTIC AI / LLM BLOCKED

© 2026 Indusface Pvt. Ltd. All rights reserved.

CONTENTS

In this Report

This report covers the zero-day vulnerabilities AppTrana blocked in October 2026. For each one, you will find exploitation status, severity, and threat-intelligence context.

01 Executive Summary 03

02 Coverage by Category 04

03 Severity Snapshot 05

04 Exploitation & KEV Status 06

05 Agentic AI & LLM Risk Coverage 07

06 Vulnerability Trend 08

07 High-Profile Attacks Blocked 09

08 Every Vulnerability Blocked, by Category 10

RESEARCH BASIS

Real enforcement data, October 2026. Each vulnerability ties to a published advisory and a blocking rule, and many also map to a scanner check.

INDUSFACE™ ©2026 Indusface. All rights reserved.

Zero-Day Exposure Window: 0 Days

AppTrana blocked 3,745 vulnerabilities in October 2026. 3,736 were blocked by its default rule set with no manual tuning; the other 9 were closed by app-specific security rules. For these vulnerabilities, the window between disclosure and protection, where exposure usually lives, was closed before attackers could use it.

3,745

BLOCKED AT THE EDGE

AppTrana blocked 3,745 vulnerabilities, with full coverage of every CVE in this period's data set for Cross-Site Scripting, SQL Injection, Path Traversal, SSRF, Uncontrolled Resource Consumption, Command Injection, Injection, and XML Injection, plus the web-exploitable patterns of Remote Code Execution, file upload, and LDAP injection.

19

CISA KEV CLOSED

CISA confirmed 19 of these vulnerabilities as actively exploited, including flaws in Fortinet FortiMail, Atlassian Data Center, Collabora Online, and Ahsay AhsayCBS.

Day zero

PUBLIC EXPLOIT CLOSED

The Collabora Online CODE Server command injection (CVE-2026-110447, CVSS 9.2) was exploited in the wild in October, with a weaponized proof-of-concept and a public Nuclei template. AppTrana blocked it on default rules, without waiting for a new signature or a vendor patch.

34

AGENTIC AI & LLM CLOSED

AppTrana autonomously blocked 34 AI/LLM-related CVEs in October 2026, spanning SSRF in agent tools, MCP server command injection, prompt injection, and RAG graph injection

INDUSFACE™ ©2026 Indusface. All rights reserved.

Coverage by Category

Cross-Site Scripting was the largest category by volume at 1,221. Remote Code Execution and Command Injection carried the most risk, with 151 and 118 Critical-severity CVEs. Path Traversal and Command Injection each held 4 of the 19 CISA KEV entries, including the Fortinet FortiMail disclosure covered in Section 07.

CATEGORY	BLOCKED	CRITICAL	HIGH	AVG CVSS	PEAK
Cross-Site Scripting	1,221	30	454	6.4	10.0
SQL Injection	553	77	230	7.4	10.0
Path Traversal	544	59	257	7.1	10.0
Remote Code Execution	389	151	147	8.0	10.0
SSRF	335	18	105	6.4	10.0
Uncontrolled Resource Consumption	260	12	126	6.9	9.9
Command Injection	248	118	101	8.5	10.0
Injection	101	12	35	6.9	9.9
Insecure Design (File-Upload, LDAP)	65	20	12	7.3	10.0
XML Injection	25	1	17	7.6	9.6
Identification & Authentication Failures	3	2	1	9.0	9.2
Security Logging & Monitoring Failures	1	0	0	5.3	5.3

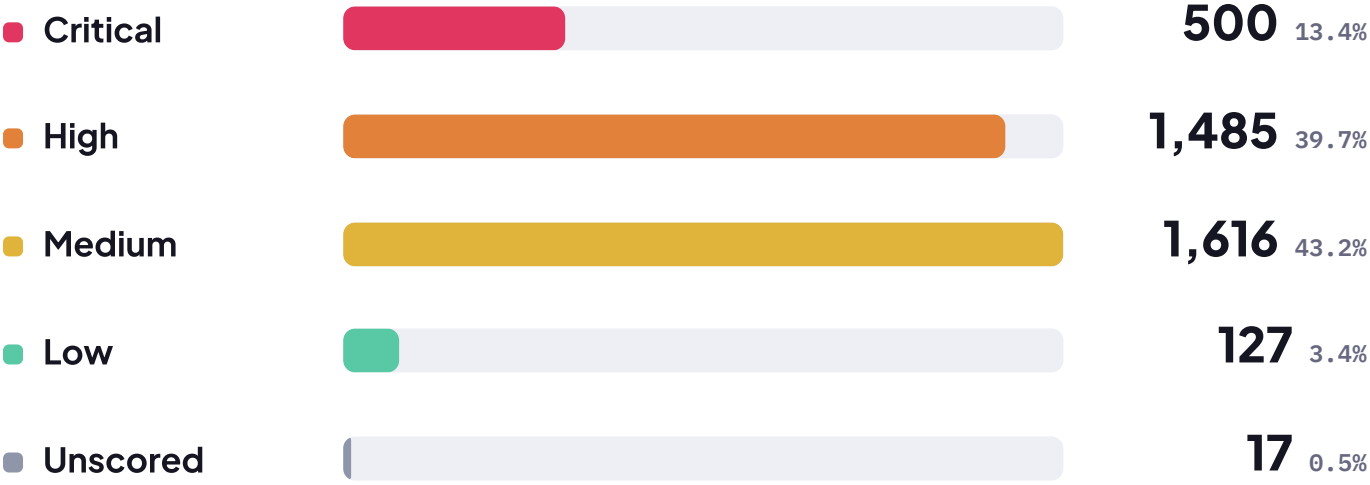
©2026 Indusface. All rights reserved.

Severity Snapshot

1,985 of the 3,745 blocked vulnerabilities (53.0%) were Critical or High, the tier that usually requires emergency patching. They were blocked at the edge, almost all on default rules, without waiting on an emergency patch or an out-of-band change. A further 17 (0.5%) had no published CVSS score yet and were still blocked.



BREAKDOWN BY SEVERITY



1,985

CRITICAL + HIGH SEVERITY

These are the vulnerabilities most organizations rush to patch first. An open exposure window here carries the highest risk. AppTrana blocked these at the edge, giving teams time to patch on a planned schedule instead of an emergency one, with little or no manual configuration.

INDUSFACE™ ©2026 Indusface. All rights reserved.

Exploitation & KEV Status

Of the 3,745 vulnerabilities blocked, 19 were already confirmed by CISA as actively exploited and listed in the Known Exploited Vulnerabilities (KEV) catalog (0.5%). A further 81 had exploitation reported by VulnCheck, and 163 had a public exploit or proof-of-concept.

19
CISA KEV · ACTIVELY EXPLOITED
0.5%

81
VULNCHECK KEV · EXPLOITATION REPORTED
2.2%

163
PUBLIC EXPLOIT / POC AVAILABLE
4.4%

NOTABLE CISA KEV ENTRIES BLOCKED

CVE	SEVERITY / CVSS	CATEGORY
CVE-2026-105134	Critical / 10.0	Command Injection
CVE-2026-104286	Critical / 9.8	Path Traversal
CVE-2026-76519	Critical / 9.8	Path Traversal
CVE-2021-3199	Critical / 9.8	Remote Code Execution
CVE-2026-88772	Critical / 9.5	Remote Code Execution
CVE-2026-114625	Critical / 9.4	SQL Injection
CVE-2026-21589	Critical / 9.3	Insecure Design
CVE-2026-110447	Critical / 9.2	Command Injection

INDUSFACE™ ©2026 Indusface. All rights reserved.

05 • EMERGING RISK

Agentic AI & LLM Risk Coverage

Agentic AI and LLM systems carry a distinct exposure surface: prompt injection, insecure agent-to-tool trust boundaries, and exposed RAG data sources. AppTrana automatically blocked 34 AI/LLM-tagged CVEs in October 2026, led by SSRF (12) and path traversal (7) in LLM tooling such as Docling, Pydantic AI, Dify, and crewai-tools. Of the three Critical CVEs, the most severe was an OS command injection in the pi-llm-wiki MCP tool (CVE-2026-102911, CVSS 9.9). The other two, both CVSS 9.6, were in Progress Autonomous REST Connector GenAI Agents and the NetLicensing MCP Server.

34	3	7.0	9.9
BLOCKED AUTOMATICALLY	CRITICAL SEVERITY	AVG CVSS (BLOCKED)	PEAK CVSS

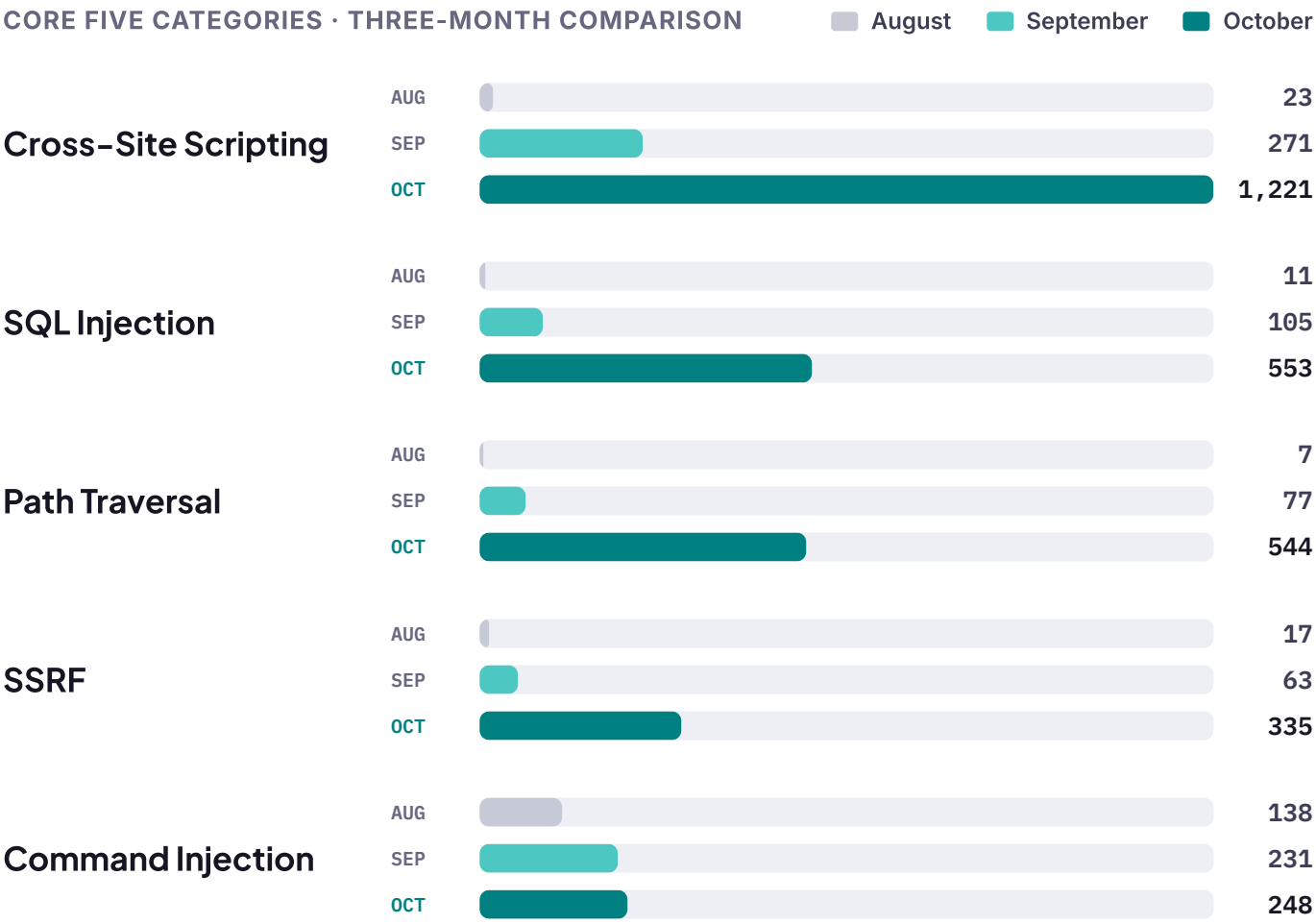
THREAT TAG	CVES	WHAT IT COVERS
General LLM Application Risk	22	LLM application code and integrations
Agent-Framework Risk	9	Autonomous-agent frameworks and trust boundaries
Prompt-Injection Vectors	6	Direct or indirect prompt-injection paths
RAG Data Exposure	1	RAG pipelines and connected data sources

Some CVEs carry more than one threat tag, so tag counts add up to more than 34.

©2026 Indusface. All rights reserved.

Vulnerability Trend

Volume rose sharply again in October. Cross-Site Scripting climbed from 271 in September to 1,221, SQL Injection from 105 to 553, Path Traversal from 77 to 544, and SSRF from 63 to 335. Command Injection held steady at 248. Across these five categories, AppTrana covered every CVE in the monthly data set for all three months, almost entirely on default rules.



INDUSFACE™ ©2026 Indusface. All rights reserved.

High-Profile Attacks Blocked

THREAT	SEVERITY / CVSS	EXPLOITATION
Ahsay AhsayCBS OS Command Injection CVE-2026-105134	Critical / 10.0	CISA KEV
Fortinet FortiMail Unauthenticated File Write CVE-2026-104286	Critical / 9.8	CISA KEV
ONLYOFFICE Document Server Traversal to RCE CVE-2021-3199	Critical / 9.8	CISA KEV
Atlassian Data Center Pre-Auth File Read CVE-2026-21589	Critical / 9.3	CISA KEV
Collabora Online CODE Server RCE CVE-2026-110447	Critical / 9.2	CISA KEV

Ahsay AhsayCBS: command injection in the replication receiver

An OS command injection in the AhsayCBS backup server's Replication Receiver endpoint (CVE-2026-105134, Critical, CVSS 10.0) can be launched remotely. The CVE is on CISA's KEV catalog, a Nuclei template is public, and EPSS puts exploitation probability at 82%. AppTrana's OS Command Injection Protection Policy blocked it by default.

Fortinet FortiMail: unauthenticated arbitrary file write

CVE-2026-104286 (Critical, CVSS 9.8), a path traversal in FortiMail 7.0 through 8.0.1, lets an unauthenticated attacker write arbitrary files through crafted HTTP or HTTPS requests. It is KEV-listed with a public proof-of-concept. AppTrana's Local File Inclusion Protection Policy blocked the request pattern.

ONLYOFFICE: a 2021 flaw newly added to KEV

CISA added CVE-2021-3199 (Critical, CVSS 9.8) to its KEV catalog this cycle. The flaw allows directory traversal to remote code execution through an image upload parameter in ONLYOFFICE Document Server before 5.6.3, and a public exploit is available. AppTrana's default rules blocked it.

Atlassian Data Center: pre-authentication file read with 99% EPSS

CVE-2026-21589 (Critical, CVSS 9.3) lets an unauthenticated attacker read files in the web root of Bitbucket, Confluence, Jira, Bamboo, and Crowd Data Center. It is KEV-listed, with a weaponized proof-of-concept and a 99% EPSS exploitation probability. AppTrana closed it with a dedicated virtual patch, the Atlassian Pre-Auth Arbitrary File Read Policy.

Collabora Online: RCE exploited in the wild

CVE-2026-110447 (Critical, CVSS 9.2) is an OS command injection in the Collabora Online built-in CODE Server for Nextcloud, exploited in the wild in October 2026. It is KEV-listed with a weaponized proof-of-concept and a Nuclei template. AppTrana's OS Command Injection Protection Policy blocked it on default rules.

INDUSFACE™ ©2026 Indusface. All rights reserved.

Blocked Vulnerabilities by Category

Each of the 3,745 vulnerabilities blocked in October 2026 traces back to a published advisory (CVE or GHSA) and a mapped blocking rule, supporting audit or compliance review.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV				
CVE-2026-106102	Quasar Framework: Stored/Reflected XSS via unescaped ...	Critical / 10	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-104252	Vitess vttablet /twopcz reflected XSS	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88804	Unauthenticated update of public UI settings leading to st...	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18516	GitLab: Improper Encoding or Escaping of Output in Craft...	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49243	Webmin: Reflected XSS in the Configuration module	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
GHSA-CG2G-XH64-V4Q7	DOMPurify SAFE_FOR_TEMPLATES bypass: split templat...	Critical / 9.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63354	CVE-2026-63354: Affected devices do not properly valid...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63353	CVE-2026-63353: Affected devices do not properly sanit...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14911	CVE-2026-14911: Improper Neutralization of Input During ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107845	Contao: Cross-site scripting in the comments bundle	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105089	WWBN AVideo through 29.2.0 Stored XSS via trailer1 in Y...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked

INDUSFACE™ ©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-102989	TanStack Router: Unauthenticated reflected XSS in TanSt...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105086	WWBN AVideo 12.4 through 29.2.0 Stored XSS via Doubl...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106630	Adobe Experience Manager | Cross-site Scripting (Stored...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83662	Adobe Experience Manager | Cross-site Scripting (Reflec...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106629	Adobe Experience Manager | Cross-site Scripting (Stored...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100133	Adobe Commerce | Cross-site Scripting (Stored XSS) (C...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91013	Adobe Commerce | Cross-site Scripting (Stored XSS) (C...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70279	Microsoft Exchange Server Spoofing Vulnerability	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101157	Security Advisory 0192	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102147	Kiteworks Core Administrative Account Takeover through...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76475	Cisco Unified Communications Products Hardening Relea...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-14990	IBM DataPower Gateway affected by cross-site scripting	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100720	Froxlor before 2.3.12 Stored XSS via SSL certificate issuer	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84244	IBM Guardium Data Protection Cross-Site Scripting	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101158	Security Advisory 0185	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105293	Legcord 1.1.0 through 1.3.0 Path Traversal via Theme IPC ...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81649	Fundiin <= 3.4.0 - Unauthenticated Payment Gateway Set...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-44977	countly-server: Stored XSS in feedback upload enables a...	Critical / 9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55562	Cronicle: Stored XSS in admin Activity Log via account ful...	Critical / 9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106155	Stored Cross-site Scripting (XSS) in Telerik Report Server...	High / 8.9	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-84261	click5 CRM add-on to Contact Form 7 <= 1.0.4 - Unauthe...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103305	Prenotazioni <= 1.7.5 - Unauthenticated Stored XSS via Se...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84258	click5 CRM add-on to Ninja Forms <= 1.0.1 - Unauthentica...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84260	click5 CRM add-on to Gravity Forms <= 1.0.3 - Unauthenti...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87764	BuddyPress Instant Chat <= 1.6 - Unauthenticated Stored ...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87762	Adwised Web Push Notification <= 2.5.7 - Unauthenticate...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92994	Verge3D < 4.13.1 - Unauthenticated Stored XSS via File St...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56840	PraisonAI: HTTPApproval dashboard renders tool argume...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86609	Download Manager Pro < 7.5.6 - Unauthenticated Stored ...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79799	HPE: Unauthenticated Stored Cross-Site Scripting (XSS) ...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88826	SmugMug Embed <= 3.13 - Unauthenticated Stored XSS ...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87780	LTL Freight Quotes – Old Dominion Edition < 4.2.19 - Unau...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70650	GetSimple CMS: Authenticated Stored XSS in backup vie...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88905	KeyWord Collector <= 1.4 - Unauthenticated Stored XSS a...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88903	Topcontent <= 1.2.1 - Unauthenticated Stored XSS via Co...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85683	Jane Menu < 1.5.1 - Unauthenticated Stored XSS via Store...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96227	Piotnet Forms <= 1.0.30 - Unauthenticated Stored XSS via...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86799	Forms < 3.0.2 - Unauthenticated Stored XSS via Form Su...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103418	Universal XSS via the HTML language attribute in Translati...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85573	All in One Files Upload for WooCommerce 2.0.3 - 2.0.16 - ...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-84259	click5 CRM add-on to WPForms <= 1.0.3 - Unauthenticate...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107126	WP Booking System < 2.1.0.1 - Unauthenticated Stored XS...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87760	Web Vitals Tracking <= 5.4.2 - Unauthenticated Stored X...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88783	Kubio AI Page Builder < 2.9.3 - Unauthenticated Stored X...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86798	HootBoard <= 3.1.4 - Unauthenticated Stored XSS via Boa...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92883	Improper Neutralization of Input During Web Page Genera...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104979	Plane: Cross-tenant stored XSS in intake enables account...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102100	Kiteworks Core stored XSS	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102092	Kiteworks Core stored XSS	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-10632	Zimbra Collaboration Suite Classic Web Client Reflected C...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109960	Froxlor 2.0.0 before 2.3.14 Stored XSS via Customer The...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105409	Stored Cross-site Scripting (XSS) vulnerability affecting T...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105798	SimpleChat: Stored XSS via group document filename in i...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84739	Improper Neutralization of Input During Web Page Genera...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-50053	Zimbra Collaboration Suite RestFilter Request Attribute Ov...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-71542	GetSimple CMS: Stored Cross-Site Scripting (XSS) via th...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105408	Stored Cross-site Scripting (XSS) vulnerability affecting T...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105410	Stored Cross-site Scripting (XSS) vulnerability affecting T...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55872	GYM One admin user list is vulnerable to stored cross-sit...	High / 8.7	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-92911	Adobe Commerce | Cross-site Scripting (Stored XSS) (C...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-54049	Sakai Conversations has a Stored XSS Issue	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55230	Vvveb: Stored XSS in Vvveb via sanitizeHTML() filter byp...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100639	SiYuan before v3.8.4 Cross-Site Scripting via Kramdown I...	High / 8.6	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-100641	SiYuan before v3.8.4 Stored XSS via Unescaped Flashcar...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109633	Frappe ERPNext before 15.119.1 Stored XSS via Public Boo...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97635	Agent Zero Web UI XSS	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101127	Joomla Extension - balbooa.com - Unauthenticated uploa...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102786	Joomla Extension - phoca.cz - Authenticated stored cros...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103292	Ghost 0.5.3 before 6.50.0 Cross-Site Scripting via ghost_...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104414	Ghost from 2.5.0 before 6.64.0 Stored XSS via oEmbed P...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103904	Stored XSS Vulnerability in JTL-Shop	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103846	Dimension | Improper Neutralization of Input During Web ...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14933	Unblu Spark Cross-Site Scripting in Embedded Co-Brows...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103277	Ghost 2.5.0 before 6.34.0 Untrusted Script Execution via ...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14452	Open redirect and XSS via reset_url parameter	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-71432	Frappe ERPNext before 15.83.0 Reflected XSS Leading to ...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100645	SiYuan 3.7.0 before 3.8.4 Stored XSS via Gallery Kanban	High / 8.6	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-109671	Frappe ERPNext before 15.113.0 Stored XSS via Profile Fiel...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104816	Misskey: Cross-site scripting in RSS feed item links	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109653	Frappe ERPNext before 15.119.0 Stored XSS Leading to Ac...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-109558	EdgeEver 1.6.0 through 1.112.0 Stored XSS via TemplatesP...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105269	Satel Netco Design Cross-site Scripting	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102982	Plane: XSS in work item comments	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104413	Ghost 5.94.0 before 6.64.0 Stored XSS via Bookmark Car...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104847	ProseMirror has a XSS vulnerability in prosemirror-view's ...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109673	Frappe ERPNext before 16.12.0 Stored XSS via Crafted Re...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109612	Frappe ERPNext before 15.120.0 Stored XSS via Report Vi...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55214	GLPI: Stored XSS in suppliers	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-71483	Horilla: Reflected Cross-Site Scripting (XSS) in Employee ...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100643	SiYuan before v3.8.4 Stored XSS via Attribute View textarea	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109291	Open WebUI 0.6.33 before 0.11.4 Stored XSS via Citation e...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109604	ERPNext before 15.112.0 Stored XSS via Tool View Record ...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104411	Ghost 6.22.1 before 6.64.0 Stored XSS via Local Storage F...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109290	Open WebUI 0.11.1 before 0.11.4 Stored XSS via DOCX Pre...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107588	Multiple Vulnerabilities in the Highcharts Library Bundled ...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106512	MISP sachertortephp - CakeResponse::download() HTTP ...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-64950	Stored Cross-Site Scripting via Directory Name in File Ma...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109557	EdgeEver through 1.112.0 Stored XSS via setMemoDragPr...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103321	MISP Stored Cross-Site Scripting (XSS) via Unvalidated E...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93886	IBM i is Affected By An Improper Neutralization of Input V...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-106107	Quasar Framework: App Vite SSR and SSG nonce attribut...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87901	CVE-2026-87901: Improper sanitization in the registratio...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100636	SiYuan before v3.8.4 Path Traversal via exportBrowserHT...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100673	Grav Data Manager before 1.4.5 Stored XSS via item-detai...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-76719	HPE OneView - Cross-site scripting vulnerability	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76718	HPE OneView - Cross-site scripting vulnerability	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86016	VNote: Stored XSS via YAML Frontmatter Leading to Local...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104450	YesWiki before 4.6.7 ACL Bypass and Stored XSS via poin...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-17189	Security vulnerabilities have been found in IBM Verify Ide...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97783	Microsoft Office SharePoint Spoofing Vulnerability	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105650	Ghost: Stored XSS via oEmbed Photo Responses	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102126	Kiteworks Core Stored Cross-site Scripting (XSS)	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102831	JupyterLab: Cross-site scripting (XSS) in JupyterLab via ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103493	CVE-2026-103493: In JetBrains YouTrack before 2026.2....	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104937	Shopware version 6.7 allows the upload of attacker-contr...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92922	Adobe Commerce | Cross-site Scripting (Stored XSS) (C...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84096	WP Review Slider Pro < 12.7.12 - Subscriber+ Stored XSS ...	High / 8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84095	WP Review Slider Pro < 12.7.12 - Subscriber+ Stored XSS ...	High / 8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103647	GitLab: Improper Neutralization of Input During Web Page...	High / 8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-89069	MOVEit Transfer Stored XSS Vulnerability in Ad Hoc Pack...	High / 8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-111095	CVE-2026-111095: In JetBrains TeamCity before 2026.2, ...	High / 8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87761	Adwised Web Push Notification <= 2.5.7 - Subscriber+ St...	High / 8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105262	Falang multilanguage for WordPress < 1.4.6 - Subscriber+...	High / 8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78557	CVE-2026-78557: A vulnerability has been identified in In...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91159	Discourse: Stored oEmbed HTML injection via allowed ifr...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116167	SiYuan 2.9.0 before 3.8.7 XSS via check-auth to Parameter	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107303	JHipster: Generated Applications Allow Stored XSS via U...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108260	@tinacms/web-components: `tina-markdown` writes rich...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-53610	GLPI: Reflected XSS in dashboards	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113499	LiteSpeed Cache < 7.9.2 - Unauthenticated Stored XSS vi...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113500	LiteSpeed Cache < 7.9.2 - Unauthenticated Stored XSS vi...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101159	WP Ultimate Review < 2.4.4 - Unauthenticated Stored XS...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97328	WebP Express < 0.25.16 - Unauthenticated Stored XSS vi...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81739	Paytm Payment Gateway < 2.8.9 - Unauthenticated Store...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85081	Multiple elFinder Plugins - DOM-based XSS via postMess...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109936	Otter Blocks < 3.2.8 - Unauthenticated Stored XSS via Dy...	High / 7.5	VULNCHECK KEV	✓ Blocked
CVE-2026-100751	Joomla Extension - regularlabs.com - Privileged stored X...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111574	Redirection for Contact Form 7 2.2.7 - 3.2.11 - Unauthentic...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88784	Weglot < 6.4.3 - Unauthenticated Stored XSS via Translat...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89193	Robin Image Optimizer 2.0.0 - 2.0.7 - Unauthenticated Sto...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-84409	Lantronix G520 Series Cellular Gateway Cross-site Scripti...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103309	GPTranslate < 2.34.14 - Unauthenticated Stored XSS via R...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-3295	IBM Cloud Pak System Cross-Site Scripting	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-64946	CSRF Bypass Leading to Stored Cross-Site Scripting via ...	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-61791	OCO-Server: Stored XSS through agent hostnames in co...	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105643	Ghost: Stored XSS via Embed Card Previews	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88204	Microsoft Office SharePoint Spoofing Vulnerability	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100316	European VAT Compliance Assistant for WooCommerce ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109208	LearnPress <= 4.4.10 - Unauthenticated Stored Cross-Sit...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96660	User Registration & Membership <= 5.2.8 - Unauthenticat...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96649	Frontend Post Submission Manager Lite <= 1.3.4 - Unauth...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
GHSA-G2V6-RQMX-R4W6	@vue/server-renderer: XSS via missing CR in attribute-na...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103899	EU VAT Assistant for WooCommerce <= 2.1.30.260413 - ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81929	Ocean Pro Demos <= 1.5.4 and Ocean eComm Treasure B...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103426	Relevanssi Premium <= 2.31.4 - Unauthenticated Stored ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97342	JetFormBuilder <= 3.6.5.4 - Unauthenticated Stored Cros...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96871	Mang Board <= 2.4.2 - Unauthenticated Stored Cross-Sit...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109987	PixelYourSite (Free & Pro) - Unauthenticated Stored XSS ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96326	HT Contact Form – Drag & Drop Form Builder for WordPre...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96575	Transliterator <= 2.5.8 - Unauthenticated Stored Cross-Si...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-107751	Mang Board <= 2.4.3 - Unauthenticated Stored Cross-Sit...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107631	Record of Consent Extension for Complianz <= 2.5 - Una...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18548	Groundhogg <= 4.5.14 - Unauthenticated Stored Cross-Si...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88043	Mang Board WP <= 2.4.0 - Unauthenticated Stored Cross...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110849	n8n before 1.123.83, 2.41.4, and 2.42.1 Stored XSS via Bin...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18586	Premium Packages <= 7.0.5 - Unauthenticated Stored Cro...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96561	AI Engine <= 3.8.0 - Unauthenticated Stored Cross-Site S...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85679	Extendify <= 3.1.6 - Unauthenticated Stored Cross-Site S...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87111	User Registration PRO <= 6.2.9 - Unauthenticated Stored ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111110	Payment forms, Buy now buttons, and Invoicing System | ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93875	JetAppointment <= 2.5.2.1 - Unauthenticated Stored Cros...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96270	Ultimate Member <= 2.13.1 - Unauthenticated Stored Cros...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92977	Real Cookie Banner: GDPR & ePrivacy Cookie Consent <=...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103422	AnyComment <= 0.3.6 - Unauthenticated Stored Cross-Si...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92244	PDF Invoices & Packing Slips for WooCommerce <= 5.16.1...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85235	Forminator Forms <= 1.57.2 - Unauthenticated Stored Cro...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96573	Appointment Hour Booking <= 1.5.97 - Unauthenticated S...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96813	Form Maker by 10Web <= 1.15.47 - Unauthenticated Store...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14995	Autoptimize <= 3.1.15.1 - Unauthenticated Stored Cross-Si...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93885	Cryptocurrency Donation Box <= 2.2.13 - Unauthenticate...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-94377	Verified Reviews (Avis Vérifiés) <= 2.4.6 - Unauthenticate...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95816	Smart Forms <= 2.6.104 - Unauthenticated Stored Cross-...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83592	Contact Form DB for Enfold <= 2.0.2 - Unauthenticated St...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92144	Forminator Forms <= 1.57.2 - Unauthenticated Stored Cro...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96572	WP Meteor Website Speed Optimization Addon <= 3.4.18 ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96278	WP Photo Album Plus <= 9.3.03.002 - Unauthenticated St...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100147	FunnelKit <= 3.16.0.5 - Unauthenticated Stored Cross-Sit...	High / 7.2	VULNCHECK KEV	✓ Blocked
CVE-2026-101920	Molongui Authorship <= 5.2.12 - Unauthenticated Stored ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96765	WPO365 | SEAMLESS WORDPRESS + MICROSOFT INTE...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100178	WPAdverts <= 2.3.4 - Unauthenticated Stored Cross-Site ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107657	HivePress <= 1.7.31 - Unauthenticated Stored Cross-Site ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107758	Colibri Page Builder <= 1.0.390 - Unauthenticated Stored ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109998	Mang Board <= 2.4.3 - Unauthenticated Stored Cross-Sit...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104828	HtmlUnit Neko: Mutation XSS (mXSS) in HTMLWriterFilter...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96570	Schema & Structured Data for WP & AMP <= 1.67 - Unaut...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103999	Ultra Addons for Contact Form 7 <= 3.5.54 - Unauthentic...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104000	Simply Schedule Appointments <= 1.6.12.35 - Unauthenti...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109990	Flying Scripts: Delay JavaScript to Improve Site Speed & ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97339	Complianz GDPR/CCPA Cookie Consent Banner <= 7.5.5 ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109207	RSS Aggregator by Feedzy <= 5.2.11 - Unauthenticated St...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-102626	LimeSurvey Community Edition 7.4.0 - Stored XSS throug...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100186	User Profile Builder <= 4.0.3 - Unauthenticated Stored Cr...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111122	SiteOrigin CSS <= 1.6.7 - Unauthenticated Stored DOM-B...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89051	Hide My WP Ghost <= 7.0.12 - Unauthenticated Stored Cr...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107764	SiteOrigin CSS <= 1.6.7 - Unauthenticated Stored DOM-B...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109513	NotificationX <= 3.3.3 - Unauthenticated Stored Cross-Sit...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96650	Strong Testimonials <= 3.3.11 - Unauthenticated Stored Cr...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96564	SEOPress <= 10.2 - Unauthenticated Stored Cross-Site S...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97341	Visitor Traffic Real Time Statistics <= 8.16 - Unauthenticat...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93430	GD Rating System <= 3.7.1 - Unauthenticated Stored Cros...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97660	WPC Product Options for WooCommerce <= 4.0.5 - Unau...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87091	Welcart e-Commerce <= 2.12.2 - Unauthenticated Stored ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97661	Business Essentials for Contact Form 7 <= 1.2.1 - Unauthe...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97398	FV Flowplayer Video Player <= 7.5.54.7212 - Unauthentic...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100153	NewStatPress <= 1.4.5 - Unauthenticated Stored Cross-S...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101924	NewStatPress <= 1.4.5 - Unauthenticated Stored Cross-S...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101928	Magic Tooltips For Contact Form 7 <= 1.0.34 - Unauthenti...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93889	Mail logging <= 2.1.12 - Unauthenticated Stored Cross-Sit...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102007	Bit integrations <= 2.10.6 - Unauthenticated Stored Cross...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93367	Visitors Traffic Real Time Statistics Pro <= 11.22 - Unauth...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-56589	HCL BigFix Service Management is affected by multiple s...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-90438	Ninja Forms <= 3.15.4 - Unauthenticated Stored Cross-Sit...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102565	BA Book Everything <= 1.8.28 - Unauthenticated Stored C...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97663	Customer Reviews for WooCommerce <= 5.122.0 - Unaut...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96578	GSpeech TTS <= 3.22.0 - Unauthenticated Stored Cross-...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110701	CP Multi View Events Calendar <= 1.4.42 - Unauthenticat...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107768	TranslatePress <= 3.3.7 - Unauthenticated Stored Cross-...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109193	HivePress <= 1.7.32 - Unauthenticated Stored Cross-Site ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95686	Opti-Behavior <= 1.9.2.1 - Unauthenticated Stored DOM-B...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95809	Opti-Behavior <= 1.9.2.1 - Unauthenticated Stored DOM-B...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109232	Salon Booking System <= 10.31.9 - Unauthenticated Store...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97347	Post Views Stats Counter <= 1.1.7 - Unauthenticated Store...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77114	Document Gallery <= 5.1.1 - Unauthenticated Stored Cros...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102562	AcyMailing <= 11.1.0 - Unauthenticated Stored Cross-Site ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96768	GoSMTP Pro <= 1.2.3 - Unauthenticated Stored Cross-Sit...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109224	SureCart <= 4.9.4 - Unauthenticated Stored Cross-Site S...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107648	WP Sessions Time Monitoring Full Automatic <= 1.1.5 - Un...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97640	WPConsent <= 1.1.9 - Unauthenticated Stored Cross-Site ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104081	KodExplorer < 4.55 Path Traversal via unzip_pre_name() ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96558	Quiz and Survey Master (QSM) <= 11.2.6 - Unauthenticate...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-75962	Post SMTP <= 4.0.1 - Unauthenticated Stored DOM-Base...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96667	Real Estate Manager <= 7.3 - Unauthenticated Stored Cro...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100161	Photo Reviews for WooCommerce <= 1.2.30 - Unauthenti...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14335	Easy Digital Downloads <= 3.6.9 - Unauthenticated Store...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96682	Presto Player <= 4.5.1 - Unauthenticated Stored Cross-Sit...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93775	Podlove Podcast Publisher <= 4.5.6 - Unauthenticated St...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100196	LazyLoad Plugin <= 2.4.0 - Unauthenticated Stored Cross...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107742	10Web Booster <= 2.34.8 - Unauthenticated Stored Cross...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96840	Post Grid Gutenberg Blocks <= 5.1.0 - Unauthenticated St...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95684	VikBooking Hotel Booking Engine & PMS <= 1.8.15 - Unaut...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100182	Download Monitor <= 5.2.10 - Unauthenticated Stored Cr...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109288	Open WebUI before 0.11.4 Stored XSS via javascript: URLs...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96566	Newsletter <= 9.4.0 - Unauthenticated Stored Cross-Site ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100107	Kubio AI Page Builder <= 2.9.2 - Unauthenticated Stored ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96567	MW WP Form <= 5.1.7 - Unauthenticated Stored Cross-Sit...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97336	CMB2 <= 2.13.0 - Unauthenticated Stored Cross-Site Scri...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93756	Smash Balloon Social Post Feed <= 4.13.0 - Unauthenticat...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95670	No External Links <= 5.2.0 - Unauthenticated Stored Cros...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102772	CMB2 <= 2.13.1 - Unauthenticated Stored Cross-Site Scri...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95817	DoFollow Case by Case <= 3.6.0 - Unauthenticated Store...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-87920	W3 Total Cache <= 2.10.6 - Unauthenticated Stored Cross...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97641	Relevanssi <= 4.28.3 - Unauthenticated Stored Cross-Sit...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102173	Kirki – Freeform Page Builder, Website Builder & Customiz...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109198	Anti-Spam by CleanTalk <= 6.89.1 - Unauthenticated Stor...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89417	OMGF | GDPR/DSGVO Compliant, Faster Google Fonts. E...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-16591	WP Directory Kit < 1.5.8 - Listing Admin+ Stored XSS via ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111830	WordPress WP Mailster plugin <= 1.9.1.0 - Cross Site Scri...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112313	WordPress ACF Extended plugin <= 0.9.2.7 - Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92232	Joomla! Core - [20260916] - Core - XSS filter bypass in In...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92231	Joomla! Core - [20260915] - Core - XSS filter bypass in In...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112379	WordPress Contact Form Email plugin <= 1.3.68 - Cross S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111838	WordPress ThemeHunk Customizer plugin <= 2.8.7 - Cro...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112221	WordPress SureCart plugin <= 4.9.5 - Cross Site Scriptin...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107435	WordPress Strong Testimonials plugin <= 3.3.12 - Cross S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111848	WordPress Geo Mashup plugin <= 1.13.22 - Cross Site Scr...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110899	WordPress Ninja Forms plugin <= 3.15.5 - Cross Site Scrip...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110884	WordPress Live Summary for Gravity Forms plugin <= 1.2....	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112869	WordPress We're Open! plugin <= 2.6 - Cross Site Scripti...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111840	WordPress Paid Videochat Turnkey Site plugin <= 7.5.14 - ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109147	WP Booking System < 2.1.0.3 - Reflected XSS via 'bookin...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-40804	WordPress aBlocks plugin <= 2.16.0 - Cross Site Scripting...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66479	WordPress WPComplete plugin <= 2.9.5.6 - CSRF to Stor...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112207	Download Monitor < 5.3.4 - Reflected XSS via Cross-Orig...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114179	WordPress BP Better Messages plugin <= 3.1.3 - Cross Sit...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112844	WordPress WP Event Solution plugin <= 4.1.26 - Cross Sit...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-61989	WordPress Easy Property Listings plugin <= 3.5.25 - Cros...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114178	WordPress W3 Total Cache plugin <= 2.10.7 - Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114697	WordPress QA Analytics plugin <= 5.3.0.1 - Cross Site Scr...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-61988	WordPress Auction Nudge – Your eBay on Your Site plugi...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112849	WordPress Hostme v2 theme <= 7.0 - Cross Site Scriptin...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112863	WordPress KALLYAS theme <= 4.25.0 - Cross Site Scripti...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115457	baserCMS: Unauthenticated Stored XSS via Shortcode Ex...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112838	WordPress VikRentCar plugin <= 1.4.8 - Cross Site Scripti...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42702	WordPress Tutor LMS plugin <= 4.1.0 - Cross Site Scriptin...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112835	WordPress VikRentCar plugin <= 1.4.8 - Cross Site Scripti...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114694	WordPress Events Manager plugin <= 7.4.8 - Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97260	WordPress MaxGalleria plugin <= 6.5.3 - Cross Site Script...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97273	WordPress Premmerce Wishlist for WooCommerce plugi...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97268	WordPress Premmerce Wishlist for WooCommerce plugi...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102378	WordPress Parallax Section block plugin <= 2.0.4 - Cross ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-103266	Ghost 5.2.0 before 6.62.0 Unauthenticated Stripe Checko...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62116	WordPress Barcode Scanner with Inventory & Order Mana...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105874	WordPress SureCart plugin <= 4.9.3 - Cross Site Scriptin...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92412	Five Star Restaurant Reviews < 2.3.14 - Reflected XSS	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91829	Subscribe to Comments < 2.3.3 - Reflected XSS via 'ref' P...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78532	WordPress LMS theme <= 8.3 - Cross Site Scripting (XSS...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62100	WordPress KuteShop theme <= 4.2.9 - Reflected Cross Si...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57742	WordPress Kids Planet theme <= 2.2.14.2 - Cross Site Scr...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78534	WordPress Educavo theme <= 3.4.2 - Cross Site Scriptin...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102391	WordPress JetFormBuilder plugin <= 3.6.5.4 - Cross Site ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-74920	Document Gallery <= 5.1.1 - Reflected XSS via data-shortc...	High / 7.1	VULNCHECK KEV	✓ Blocked
CVE-2026-109702	WordPress Social Share Buttons plugin <= 1.31 - Cross Sit...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109685	WordPress Link Whisper Free plugin <= 0.9.7 - Cross Site...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94171	WordPress CURCY plugin 2.2.18 - Cross Site Scripting (X...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97290	WordPress Photonic Gallery & Lightbox for Flickr, SmugM...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100510	WordPress Post and Page Builder by BoldGrid plugin <= 1....	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102376	WordPress Branda plugin <= 3.4.32 - Cross Site Scripting...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108484	WordPress Best Payments Plugin for WP plugin <= 4.6.27...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105066	WordPress SimplyRETS Real Estate IDX plugin <= 3.2.9 - ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108483	WordPress Hippoo Mobile App for WooCommerce plugin ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-62034	WordPress Before After Image Comparison – Image comp...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62027	WordPress Team Section Block plugin <= 2.0.4 - Cross Si...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107428	WordPress Paid Videochat Turnkey Site plugin <= 7.5.12 - ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107870	WordPress JetEngine plugin <= 3.8.16 - Cross Site Scripti...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107867	WordPress JetProductTables plugin <= 1.2.4 - Cross Site ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102395	WordPress Easy Google Maps plugin <= 1.14.6 - Cross Sit...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42709	WordPress Food Menu – Restaurant Menu & Online Orderi...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42711	WordPress Slider by 10Web plugin <= 1.2.63 - Cross Site ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42715	WordPress Photo Gallery by 10Web plugin <= 1.8.47 - Cro...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97263	WordPress WPAdverts plugin <= 2.3.4 - Cross Site Scripti...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62037	WordPress Document Embedder plugin <= 2.4.0 - Cross ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62064	WordPress Ambed theme <= 1.0.0 - Reflected Cross Site ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62082	WordPress Pin WP theme <= 7.0 - Reflected Cross Site Sc...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62091	WordPress Armania theme <= 1.4.8 - Reflected Cross Site...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62093	WordPress TechOne theme <= 3.0.3 - Reflected Cross Sit...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62095	WordPress Biolife theme <= 3.2.3 - Reflected Cross Site ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103342	WordPress Unlimited Elements For Elementor (Free Widg...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42632	WordPress Qode Real Estate plugin <= 1.1.7.3 - Cross Site ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42693	WordPress Jannah theme < 7.6.8 - Cross Site Scripting (X...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42697	WordPress Social Share Icons & Social Share Buttons plu...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-42699	WordPress FV Player 8 plugin <= 8.1.8 - Cross Site Scripti...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97271	WordPress WPFunnels plugin <= 3.13.1 - Cross Site Script...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102396	WordPress Ultimate Maps by Supsystic plugin <= 1.5.5 - ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102398	WordPress Popup by Supsystic plugin <= 1.13.1 - Cross Sit...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97289	WordPress Quiz And Survey Master plugin <= 11.2.6 - Cro...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100507	WordPress If-So Dynamic Content Personalization plugin ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97264	WordPress WPAdverts plugin <= 2.3.4 - Cross Site Scripti...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94160	WordPress ThemeStek Extras for LabtechCO Theme plug...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102385	WordPress Ninja Forms plugin <= 3.15.3 - Cross Site Scrip...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97272	WordPress Premmerce Permalink Manager for WooCom...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97253	WordPress LayerSlider plugin <= 8.4.0 - Cross Site Script...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105065	WordPress XStore theme < 9.7.9 - Cross Site Scripting (X...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97250	WordPress Geo Mashup plugin <= 1.13.21 - Cross Site Scri...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97237	WordPress JetEngine plugin <= 3.8.14.3 - Cross Site Scri...	High / 7.1	VULNCHECK KEV	✓ Blocked
CVE-2026-97235	WordPress ThemeREX Addons plugin < 2.45.0 - Cross Sit...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97077	WordPress Ad Inserter plugin <= 2.8.18 - Cross Site Script...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97065	WordPress Happyforms plugin <= 1.26.15 - Cross Site Scr...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104814	WordPress Form Block plugin <= 1.8.1 - Cross Site Scripti...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105061	WordPress WP Mailster plugin <= 1.9.0.0 - Cross Site Scri...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106106	Quasar Framework: SSR/SSG dev error page discloses th...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-42418	WordPress Social Rocket plugin <= 1.3.5 - Cross Site Scri...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42634	WordPress Video Background Block – Use video as backg...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42635	WordPress WooCommerce Simple Auctions plugin <= 3.0...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108498	WordPress BSK PDF Manager plugin <= 3.8.1 - Cross Site ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108491	WordPress Everest Forms plugin <= 3.6.1 - Cross Site Scri...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57806	WordPress Martfury - WooCommerce Marketplace Word...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39799	WordPress WP File Download plugin <= 6.3.6 - Cross Site...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39800	WordPress Additional Order Filters for WooCommerce plu...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40803	WordPress Jotform – AI Chatbot plugin <= 3.8.2 - Cross S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42631	WordPress Qode Music plugin <= 2.1.8.2 - Cross Site Scri...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93951	WordPress Zeinet theme <= 1.0.0 - Reflected Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102388	WordPress Forminator plugin <= 1.57.3 - Cross Site Script...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-15643	WordPress Adsmonetizer plugin <= 3.2.4 - Cross Site Scr...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103354	WordPress Gutenberg Blocks by Kadence Blocks plugin <...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97276	WordPress WP Statistics plugin <= 14.16.14 - Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103062	WordPress TranslatePress plugin <= 3.3.6 - Cross Site Sc...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103344	WordPress Unlimited Elements For Elementor (Free Widg...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94066	WordPress Pond theme <= 2.6.1 - Reflected Cross Site Sc...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105318	WordPress AcyMailing SMTP Newsletter plugin <= 11.1.0 -...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105870	WordPress WP Associate Post R2 plugin <= 5.0.1 - Cross ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-94058	WordPress Treck theme <= 1.0.0 - Reflected Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94059	WordPress Ogency theme <= 1.0.0 - Reflected Cross Site ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94060	WordPress Voldor theme <= 1.0.0 - Reflected Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94061	WordPress Whistle - Sports Club theme <= 4.2 - Reflecte...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94063	WordPress Education Center theme <= 3.6.12 - Reflected ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39731	WordPress Database for CF7 plugin <= 1.2.6 - Cross Site ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39745	WordPress Contact Form to DB by BestWebSoft plugin <=...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39748	WordPress EduMall theme <= 4.5.3 - Reflected Cross Site...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39750	WordPress StoreGrowth: Smart Sales Booster for WooCo...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39758	WordPress Midtrans-WooCommerce plugin <= 2.32.3 - C...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39766	WordPress ARForms plugin <= 7.1.2 - Cross Site Scripting...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39768	WordPress Security & Malware scan by CleanTalk plugin ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32572	WordPress WP User Frontend Pro plugin <= 4.2.13 - Cros...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32574	WordPress Smart Forms plugin <= 2.6.104 - Cross Site Sc...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32575	WordPress SUMO Affiliates Pro plugin <= 11.7.0 - Cross Si...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32577	WordPress Frontend File Manager plugin <= 23.6 - Cross ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39720	WordPress Mapster WP Maps plugin <= 2.0.4 - Cross Sit...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39722	WordPress WPLMS theme <= 4.972 - Reflected Cross Sit...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39724	WordPress HTTP Requests Manager plugin <= 1.3.11 - Cro...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39726	WordPress Lumise Product Designer plugin <= 2.1.1 - Cro...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-39760	WordPress Real 3D FlipBook plugin <= 5.5 - Cross Site Sc...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103346	WordPress Payflex Payment Gateway plugin <= 2.7.1 - Cr...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32569	WordPress WP Media folder plugin <= 6.2.2 - Cross Site ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32570	WordPress Progressify - Progressive Web App (PWA) plu...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96814	WordPress WooCommerce Product Table Lite plugin <= 5...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96816	WordPress Trusted Shops Easy Integration for WooCom...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96819	WordPress oik plugin <= 4.15.4 - Cross Site Scripting (XS...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96820	WordPress Awesome Support plugin <= 6.3.9 - Cross Sit...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96830	WordPress GiveWP plugin <= 4.16.9 - Cross Site Scripting...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96836	WordPress Parsi Date plugin <= 6.3 - Cross Site Scripting ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94078	WordPress Site Reviews plugin <= 8.3.1 - Cross Site Scrip...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94081	WordPress WordPress Persistent Login plugin <= 3.1.3 - ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96351	WordPress Classified Listing plugin <= 6.1.3 - Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96352	WordPress YITH WooCommerce Ajax Search plugin <= 2....	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-27371	WordPress WPFunnels plugin <= 3.13.1 - Reflected Cross ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93512	WordPress JW Player for WordPress plugin <= 2.3.11 - Cr...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93514	WordPress Notification for Telegram plugin <= 3.5.2 - Cro...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93770	WordPress WP Statistics plugin <= 14.16.13 - Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96339	WordPress Houzez theme <= 4.4.0 - Cross Site Scripting ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100515	WordPress Photo Reviews for WooCommerce plugin <= 1...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-104672	WordPress GiveWP plugin <= 4.17.0 - Cross Site Scripting...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95596	WordPress ShopBuilder – Elementor WooCommerce Buil...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95598	WordPress Search in Place plugin <= 1.5.5 - Cross Site Sc...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95609	WordPress Media LIbrary Assistant plugin <= 3.41 - Cross...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94167	WordPress Kubio AI Page Builder plugin <= 2.9.3 - Cross ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94159	WordPress Total Donations plugin <= 2.0.5 - Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94161	WordPress Grand Restaurant theme < 7.0.11 - Reflected Cr...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42636	WordPress WP Cookie Notice for GDPR, CCPA & ePrivacy...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94675	WordPress Fluent Forms Pro Add On Pack plugin <= 6.2.1...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104394	WordPress Charitable plugin <= 1.8.12.3 - Cross Site Scrip...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104395	WordPress picu plugin <= 3.10.1 - Cross Site Scripting (XS...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104670	WordPress LearnPress plugin <= 4.4.9 - Cross Site Script...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39778	WordPress Ansar Import – One Click Starter Sites – for Ele...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39780	WordPress Youzify plugin <= 1.3.7 - Cross Site Scripting (...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39781	WordPress Document Gallery plugin <= 5.1.1 - Cross Site ...	High / 7.1	VULNCHECK KEV	✓ Blocked
CVE-2026-39784	WordPress Hotel Booking plugin <= 3.8 - Cross Site Scrip...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39790	WordPress VikRentCar plugin <= 1.4.7 - Cross Site Scripti...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40806	WordPress Blog, Posts and Category Filter for Elementor ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40807	WordPress CF7 Views – Complete Entry Management for ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96607	WordPress NEX-Forms plugin <= 9.3.1 - Cross Site Scripti...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-94170	WordPress Sassy Social Share plugin <= 3.3.79 - Cross Si...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111948	Profile Builder < 4.0.1 - Reflected XSS via Unconfirmed E...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79627	Advanced File Manager 5.4.13 - 5.4.14 - Authenticated Sto...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113808	Stored XSS on SNS Enrollment Portal	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91832	WP Mobile Menu 2.7.4 - 2.8.8 - Stored XSS via CSRF	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110382	WordPress Simply Schedule Appointments plugin <= 1.6.1...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110379	WordPress Quiz Maker plugin <= 6.7.1.91 - Cross Site Scri...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108485	WordPress eStore theme <= 1.6.13 - Cross Site Scripting (...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110981	WP Photo Album Plus < 9.2.11.002 - Reflected XSS via 'w...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110897	WordPress PowerPack Lite for Beaver Builder plugin <= 1....	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110384	WordPress Fancy Comments WordPress plugin <= 1.2.21 ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109701	WordPress PAYCOMET for WooCommerce plugin <= 5.4...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109895	WordPress Booktics plugin <= 1.0.29 - Cross Site Scriptin...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105316	Magee Shortcodes <= 2.1.1 - Reflected XSS via live_previ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87971	If-So Dynamic Content 1.4.4 - 1.10.1 - Reflected XSS via 'm...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114695	WordPress VOD Infomaniak plugin <= 1.5.14 - Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96761	WordPress Welcart e-Commerce plugin <= 2.12.3 - Cross...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94166	WordPress UpSolution Core plugin <= 8.44 - Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94662	WordPress Unlimited Elements For Elementor plugin <= 2...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94158	WordPress Gloria Admin Panel plugin <= 1.3 - Reflected C...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-94415	WordPress Betheme theme <= 28.5.8 - Cross Site Scripti...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94632	WordPress BlockStrap Page Builder - Bootstrap Blocks pl...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94641	WordPress UsersWP plugin <= 1.2.73 - Cross Site Scripti...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94661	WordPress JetBlog plugin <= 2.4.10 - Cross Site Scripting...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94668	WordPress Salon booking system plugin <= 10.31.5 - Cros...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96332	WordPress Simple Payment plugin <= 2.5.4 - Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96553	WordPress FiboSearch plugin <= 1.34.1 - Cross Site Script...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95608	WordPress HUSKY plugin <= 1.4.3.2 - Cross Site Scriptin...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95591	WordPress VikBooking Hotel Booking Engine & PMS plugi...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94670	WordPress Everest Forms plugin <= 3.6.1 - Cross Site Scri...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95595	WordPress Disable and Remove Google Fonts | GDPR & D...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113810	Stored XSS on SNS Enrollment Portal	High / 7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110847	n8n before 1.123.83, 2.41.4, and 2.42.1 Stored XSS via Cha...	High / 7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-90918	Joomla! Core - [20260908] - Core - XSS in HTML Mail Te...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109266	ImageMagick before 6.9.13-57 and 7.x before 7.1.2-32 XM...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100275	CVE-2026-100275: In JetBrains YouTrack before 2026.2.1...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54701	Markdown Preview Enhanced: Stored XSS via Unsanitize...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103249	n8n before 1.123.80, 2.39.6, and 2.40.1 Stored DOM XSS v...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-11960	Multiple vulnerabilities in FacturaScripts	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-11959	Multiple vulnerabilities in FacturaScripts	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-96878	Cargo Exhibit field alias allows stored XSS	Medium / 6.9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-96877	Reflected XSS through Cargo Drilldown full-text search	Medium / 6.9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-96876	Anonymous reflected XSS in CargoExport invalid-alias err...	Medium / 6.9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-96875	Reflected XSS in Cargo Drilldown hierarchy filters	Medium / 6.9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-96654	Plex Media Server URL injection	Medium / 6.9	CISA KEV	✓ Blocked
CVE-2026-96531	Optimole 4.0.0 - 4.2.12 - Author+ Stored XSS via Video Pl...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111979	GiveWP < 4.19.0.1 - Give Worker+ Stored XSS via Form Te...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78392	Link Library < 7.9.6 - Contributor+ Stored XSS via 'link_tar...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104652	Envira Gallery < 1.16.1 - Author+ Stored XSS via Gallery Im...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111971	Photo Engine < 6.5.8 - Author+ Stored XSS via Collection ...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104653	Envira Gallery < 1.16.1 - Author+ Stored XSS via Gallery Cr...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91022	Motors < 1.4.124 - Listing Manager+ Stored XSS via Badg...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13718	Tabs Responsive <= 2.5 - Shop Manager+ Stored XSS via...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89191	Stored Cross-Site Scripting in SQLView KRIS	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85016	Unlimited Elements For Elementor < 2.0.21 - Contributor+ ...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-17005	Horizontal Scrolling Announcements <= 2.6 - Contributor...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81154	Robo Gallery < 5.2.6 - Author+ Stored XSS via Image Alt T...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81153	Robo Gallery < 5.2.6 - Author+ Stored XSS via Image Over...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81155	Robo Gallery < 5.2.6 - Author+ Stored XSS via Gallery Sea...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89006	WPeMatico RSS Feed Fetcher < 2.8.27 - Contributor+ Sto...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-96895	WP YouTube Lyte < 1.7.31 - Contributor+ Stored XSS via E...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94239	Loco Translate < 2.8.9 - Translator+ Stored XSS via Bundl...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85002	EmbedPress < 4.6.7 - Contributor+ Stored XSS via Instagr...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113493	GeoDirectory < 2.8.194 - Contributor+ Stored XSS via gd_...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114429	WP VR 8.5.49 - 9.0.2 - Contributor+ Stored XSS via Hotsp...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104646	Image Photo Gallery Final Tiles Grid < 3.6.14 - Contributor...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115993	Stored XSS in the “Notes” field of project checklists	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92411	WP Delicious < 1.10.8 - Contributor+ Stored XSS via Recip...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97319	PowerPress < 11.17.2 - Contributor+ Stored XSS via Podca...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96899	Optima Express 8.6.0 - 8.7.5 - Author+ Stored XSS via faq...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109933	Otter Blocks < 3.2.8 - Contributor+ Stored XSS via Block ...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105199	Pixel Tag Manager for WooCommerce < 2.2.3 - Contribut...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87777	Hostinger Reach 1.0.6 - 1.8.2 - Contributor+ Stored XSS vi...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88782	Kubio AI Page Builder < 2.9.3 - Contributor+ Stored XSS v...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81813	Elementor < 4.3.5 - Contributor+ Stored XSS via SVG CDA...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107323	Gallery PhotoBlocks 1.3.5 - Contributor+ Stored XSS	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81156	Robo Gallery < 5.2.6 - Contributor+ Stored XSS via Galler...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105261	PublishPress Future 4.10.1 - 4.10.5 - Contributor+ Stored X...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86797	Pricing Table Block 1.0.7 - 2.1.4 - Contributor+ Stored XSS...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107178	Image Photo Gallery Final Tiles Grid < 3.6.16 - Contributor...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-104644	Image Photo Gallery Final Tiles Grid < 3.6.15 - Contributor...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92409	Donation Thermometer 2.2.9 - 2.2.11 - Contributor+ Store...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106469	Gutenverse Form < 3.0.11 - Contributor+ Stored XSS via S...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110033	Salon Booking System < 10.31.11 - Salon Staff+ Stored XS...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-74921	Document Gallery 4.0 - 5.1.1 - Contributor+ Stored XSS via...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106933	Blaze Demo Importer < 1.0.17 - Author+ Stored XSS via SV...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92424	Content Egg < 11.9.0 - Contributor+ Stored XSS via Import...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107790	WP Job Openings < 4.1.1 - Author+ Stored XSS via Job Title	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89269	WP Testimonials <= 1.4.13 - Author+ Stored XSS via wp-te...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85001	EmbedPress 4.4.9 - 4.6.6 - Contributor+ Stored XSS via El...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111966	Profile Builder < 4.0.5 - Contributor+ Stored XSS via redir...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94264	Advanced Custom Fields: Extended 0.8.9.4 - 0.9.2.7 - Co...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85415	Audio Player Block 1.1.0 - 1.6.2 - Contributor+ Stored XSS ...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12980	Post Snippets <= 4.2.4 - Contributor+ Stored XSS via Sni...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111096	CVE-2026-111096: In JetBrains TeamCity before 2026.2, ...	Medium / 6.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113465	Possible DOM XSS in SNS Web Administration Portal	Medium / 6.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108478	WordPress Element Pack Elementor Addons plugin <= 8....	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107862	WordPress Quiz And Survey Master plugin <= 11.2.7 - Cro...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103064	WordPress ElementsKit Elementor addons Lite plugin <= ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103343	WordPress FluentForm plugin <= 6.2.14 - Cross Site Scrip...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-108487	WordPress Books Gallery plugin <= 4.8.4 - Cross Site Scr...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107864	WordPress Ad Inserter plugin <= 2.8.18 - Cross Site Script...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102394	WordPress Essential Addons for Elementor plugin <= 6.8....	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109691	WordPress Prime Slider – Addons For Elementor plugin <...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109697	WordPress SureCart plugin <= 4.9.4 - Cross Site Scriptin...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54870	WordPress Weaver Xtreme theme Support plugin <= 7.0.1 ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108488	WordPress PowerPack Addons for Elementor plugin <= 3....	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103339	WordPress Metform plugin <= 4.3.0 - Cross Site Scripting...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108495	WordPress SureForms plugin <= 2.12.7 - Cross Site Script...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108490	WordPress Premium Addons for Elementor plugin <= 4.11....	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105887	WordPress Robo Gallery plugin <= 5.1.6 - Cross Site Scrip...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103070	WordPress ShortPixel Image Optimizer plugin <= 6.5.6 - ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97294	WordPress Media LIbrary Assistant plugin <= 3.41 - Cross...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103063	WordPress ElementsKit Elementor addons Lite plugin <= ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112867	WordPress H5P plugin <= 1.17.9 - Cross Site Scripting (XS...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114184	WordPress Elementor Addon Elements plugin <= 1.14.4 - ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105871	WordPress Element Pack Elementor Addons plugin <= 8....	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105881	WordPress User Registration plugin <= 5.2.8 - Cross Site ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94674	WordPress Pixel Manager for WooCommerce plugin <= 1....	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94077	WordPress Safe SVG plugin <= 2.5.0 - Cross Site Scriptin...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-62080	WordPress Happy Addons for Elementor plugin <= 3.23.1 ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62079	WordPress Qi Addons For Elementor plugin <= 1.11 - Cros...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62078	WordPress Premium Addons for Elementor plugin <= 4.11....	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107865	WordPress JetMenu plugin <= 3.0.5 - Cross Site Scriptin...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107866	WordPress JetElements For Elementor plugin <= 2.9.2.3 -...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108168	WordPress Custom Query Blocks plugin <= 5.6.0 - Cross ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108482	WordPress Premium Addons for Elementor plugin <= 4.11....	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107422	WordPress WP w3all phpBB plugin <= 3.1.0 - Cross Site S...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105875	WordPress Prime Slider – Addons For Elementor plugin <...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106163	Cross-site Scripting (XSS) in Kendo UI for jQuery FileBro...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-67075	HCL Digital Experience is affected by improper input sanit...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110903	WordPress The Events Calendar plugin <= 6.18.1 - Cross S...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111410	WordPress e2pdf plugin <= 1.32.57 - Cross Site Scripting ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112199	WordPress YITH WooCommerce Wishlist plugin <= 4.18.1 ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105873	WordPress Element Pack Elementor Addons plugin <= 8....	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2023-5648	CVE-2023-5648: In Brocade ASCG before Brocade ASCG...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39788	WordPress Front End PM plugin <= 11.4.6 - Cross Site Scr...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111407	WordPress Tutor LMS plugin <= 4.1.2 - Cross Site Scriptin...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111414	WordPress JetElements For Elementor plugin <= 2.9.2.4 -...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111400	WordPress PowerPack Addons for Elementor plugin <= 3....	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-105884	WordPress Rocket Lazy Load plugin <= 2.4.0 - Cross Site ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104391	WordPress Quiz And Survey Master plugin <= 11.2.7 - Cro...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111405	WordPress MapSVG plugin <= 8.16.1 - Cross Site Scriptin...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42695	WordPress FV Flowplayer Video Player plugin <= 7.5.54.7...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32571	WordPress Ohio Extra plugin <= 3.6.8 - Cross Site Scripti...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105879	WordPress JetElements For Elementor plugin <= 2.9.2.2 -...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104393	WordPress Happy Addons for Elementor plugin <= 3.50.0...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96338	WordPress Profile Builder plugin <= 4.0.2 - Cross Site Scr...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96835	WordPress King Addons for Elementor plugin <= 51.1.85 - ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96829	WordPress The Plus Addons for Elementor Page Builder L...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102393	WordPress Starter Templates plugin <= 4.7.7 - Cross Site ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104396	WordPress Name Directory plugin <= 1.34.2 - Cross Site ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102914	WordPress Presto Player plugin <= 4.5.2 - Cross Site Scri...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103084	WordPress Premium Addons for Elementor plugin <= 4.11....	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105060	WordPress Logo Showcase plugin <= 4.0.4 - Cross Site S...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104673	WordPress MP3 Audio Player for Music, Radio & Podcast ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39727	WordPress WC Fields Factory plugin <= 4.1.12 - Cross Sit...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105056	WordPress eCommerce Product Catalog plugin <= 3.6.2 -...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105069	WordPress QR Redirector plugin <= 2.0.5 - Cross Site Scr...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104404	WordPress GiveWP plugin <= 4.17.0 - Cross Site Scripting...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-104400	WordPress B Blocks plugin <= 2.1.8 - Cross Site Scripting ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97270	WordPress CMB2 plugin <= 2.13.0 - Cross Site Scripting (...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62084	WordPress User Submitted Posts plugin <= 20260810 - C...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102386	WordPress WP Photo Album Plus plugin <= 9.3.02.003 - ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100513	WordPress CF7 Views – Complete Entry Management for ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97301	WordPress Cool Formkit Lite plugin <= 2.7.8 - Cross Site ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109893	WordPress Presto Player plugin <= 4.5.3 - Cross Site Scri...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97298	WordPress King Addons for Elementor plugin <= 51.1.86 - ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97292	WordPress YITH WooCommerce Tab Manager plugin <= ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97288	WordPress OAuth Server plugin <= 4.5.1 - Cross Site Scri...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97286	WordPress Strong Testimonials plugin <= 3.3.11 - Cross Si...	Medium / 6.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-97279	WordPress Polylang plugin <= 3.8.9 - Cross Site Scripting...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108175	WordPress MDTF plugin <= 1.4.0 - Cross Site Scripting (X...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110890	WordPress JetSmartFilters plugin <= 3.8.6 - Cross Site S...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105882	WordPress User Registration plugin <= 5.2.8 - Cross Site ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110375	WordPress Download Monitor plugin <= 5.3.3 - Cross Site...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106604	WordPress YITH WooCommerce Compare plugin <= 3.15....	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97265	WordPress JetEngine plugin <= 3.8.15.3 - Cross Site Scrip...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104409	WordPress Image Photo Gallery Final Tiles Grid plugin <= ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102798	WordPress ThemeREX Addons plugin <= 2.46.0 - Cross ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-97236	WordPress ThemeREX Addons plugin < 2.45.0 - Cross Sit...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97067	WordPress EWWW Image Optimizer plugin <= 8.7.7 - Cro...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114194	WordPress Ad Inserter plugin <= 2.8.18 - Cross Site Script...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114693	WordPress All-in-One Video Gallery plugin <= 4.9.7 - Cro...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114702	WordPress ND Shortcodes For Visual Composer plugin <...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105078	WordPress WP Store Locator plugin <= 3.0.3 - Cross Site ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114700	WordPress Restaurant Menu – Food Ordering System – T...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114701	WordPress Waitlist Woocommerce (Back in stock notifier...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114703	WordPress Extensions for Leaflet Map plugin <= 6.0 - Cro...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97266	WordPress Virtue/Ascend/Pinnacle Toolkit plugin <= 4.9.1...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97262	WordPress Visual Composer Website Builder plugin <= 4...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42700	WordPress Image Slider Widget plugin <= 1.1.130 - Cross ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111844	WordPress Brizy plugin 2.8.23 - Cross Site Scripting (XSS...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112845	WordPress Off-Canvas Sidebars & Menus (Slidebars) plu...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54869	WordPress IMPress for IDX Broker plugin <= 3.3.1 - Cross ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54868	WordPress FV Simpler SEO plugin <= 1.9.7 - Cross Site Sc...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54867	WordPress Responsive Slider plugin <= 0.1.9 - Cross Site ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76972	Cross-Site Scripting (XSS) vulnerability in SAP Manufactu...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62029	WordPress WPFunnels plugin <= 3.13.3 - Cross Site Scrip...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62039	WordPress Html5 Audio Player plugin <= 2.8.8 - Cross Sit...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-94667	WordPress JetReviews plugin <= 3.1.2 - Cross Site Scripti...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94665	WordPress Classified Listing plugin <= 6.1.2 - Cross Site ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62049	WordPress JetBlocks For Elementor plugin <= 1.5.2.1 - Cr...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100509	WordPress RepairBuddy plugin <= 4.1225 - Cross Site Scr...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112833	WordPress Seriously Simple Podcasting plugin <= 3.17.0 -...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111088	Stored XSS in the VPN logs monitor	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111843	WordPress Rootblox plugin <= 1.0.7 - Cross Site Scripting ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112840	WordPress SureCart plugin <= 4.9.5 - Cross Site Scriptin...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105079	WordPress MasterStudy LMS plugin <= 3.7.52 - Cross Sit...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105890	WordPress Gutenberg Blocks by Kadence Blocks plugin <...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62127	WordPress WP plugin Info Card plugin <= 6.3.5 - Cross Si...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-27420	WordPress Zotpress plugin <= 7.4.4 - Cross Site Scripting...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111837	WordPress Contest Gallery plugin <= 34.0.1 - Cross Site S...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114128	Astro: Reflected/Stored XSS via unescaped	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81812	Elementor < 4.3.5 - Author+ Stored XSS via SVG Upload	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-6172	Bold Page Builder <= 5.7.2 - Authenticated (Contributor+) ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88037	Bold Page Builder <= 5.7.2 - Authenticated (Contributor+) ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-11895	HT Mega Addons for Elementor <= 3.1.1 - Authenticated (...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14876	Smart Slider 3 <= 3.5.1.38 - Authenticated (Contributor+) ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-6171	Bold Page Builder <= 5.7.2 - Authenticated (Contributor+) ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-6170	Bold Page Builder <= 5.7.2 - Authenticated (Contributor+) ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-6173	Bold Page Builder <= 5.7.2 - Authenticated (Contributor+) ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96647	Listdom: AI-powered Business Directory with Classifieds ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97338	Download Manager <= 3.3.70 - Authenticated (Subscriber...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18541	IBM Planning Analytics Local is affected by security vulne...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15273	Automatic.css 4.0.0 - Unauthenticated Stored Cross-Site ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77829	Cooked <= 1.16.1 - Authenticated (Contributor+) Stored Cr...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107748	User Profile Builder <= 4.0.3 - Authenticated (Subscriber...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103480	Tourfic <= 3.0.1 - Authenticated (Contributor+) Stored Cro...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93535	WP Dark Mode – Improve Accessibility with AI Powered D...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100158	SQL Chart Builder <= 3.0.6 - Authenticated (Subscriber+) ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109512	Mang Board <= 2.4.4 - Authenticated (Subscriber+) Store...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15795	Responsive Plus <= 3.5.3 - Authenticated (Contributor+) ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92767	Twenty20 Image Before-After <= 2.0.5 - Authenticated (C...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92727	EmbedPress <= 4.6.6 - Authenticated (Contributor+) Stor...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-12828	Ultra Addons Lite for Elementor <= 1.3.2 - Authenticated (...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100148	Rich Showcase for Google Reviews <= 7.1.3 - Authenticat...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101162	WP Ultimate Review < 2.4.4 - Author+ Stored XSS via Rev...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102774	SureDash <= 1.12.1 - Authenticated (Subscriber+) Stored ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97340	Avada | Website Builder For WordPress & WooCommerce ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-103478	Premium Packages <= 7.2.6 - Authenticated (Subscriber+...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-4791	PeproDev Ultimate Profile Solutions <= 8.2.36 - Authentic...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94378	SupportCandy <= 3.5.3 - Authenticated (Subscriber+) Sto...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97344	Wp Social Login and Register Social Counter <= 3.2.1 - Au...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96563	Motors <= 1.4.124 - Authenticated (Subscriber+) Stored C...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97396	Email Marketing for WordPress and WooCommerce <= 1....	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102402	Team <= 6.0.2 - Authenticated (Contributor+) Stored Cro...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-6243	Frontend Admin by DynamiApps <= 3.28.36 - Authenticat...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103427	Simple Membership <= 4.8.4 - Authenticated (Subscriber...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14882	Brizy <= 2.8.18 - Authenticated (Contributor+) Stored Cro...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93878	DiviGear Carousel <= 5.2.0 - Authenticated (Subscriber+)...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-17025	Graphene <= 2.9.4 - Authenticated (Subscriber+) Stored ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96574	User Frontend <= 4.3.12 - Authenticated (Subscriber+) St...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110664	Premium Packages <= 7.2.8 - Authenticated (Subscriber+...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111069	GeoDirectory <= 2.8.192 - Authenticated (Subscriber+) St...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110017	Quick PayPal Payments: Payment Button & Form <= 6.0.4 ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78001	Post and Page Builder by BoldGrid <= 1.27.13 - Authentica...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14572	Kirki <= 6.2.0 - Authenticated (Custom+) Stored Cross-Si...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-9373	PeproDev Branches Map <= 3.0.1 - Authenticated (Contri...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104761	Mang Board <= 2.4.3 - Authenticated (Custom+) Stored C...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-17001	Import and export users and customers <= 2.4.5 - Authen...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78087	VK Blocks <= 1.126.1 - Authenticated (Contributor+) Store...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107756	Meow Lightbox <= 5.6.2 - Authenticated (Subscriber+) St...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107650	GeoDirectory <= 2.8.190 - Authenticated (Subscriber+) St...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107754	GeoDirectory <= 2.8.190 - Authenticated (Subscriber+) St...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103369	Social Share Buttons & Analytics Plugin <= 4.5 - Authentic...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109388	HivePress <= 1.7.32 - Authenticated (Subscriber+) Stored ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100106	FiboSearch <= 1.34.2 - Authenticated (Subscriber+) Store...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96256	Gutenberg Essential Blocks <= 6.4.5 - Authenticated (Co...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-16495	Countdown Timer – Widget Countdown <= 3.0.1 - Authent...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93908	Real Estate Manager <= 7.3 - Authenticated (Subscriber+)...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-14564	Viable URL Media Uploader <= 1.0.0 - Authenticated (Aut...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92712	ReactPress <= 3.4.0 - Authenticated (Subscriber+) Store...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110290	WebberZone Top 10 <= 4.5.2 - Authenticated (Contributor...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93681	Tutor LMS <= 4.1.0 - Authenticated (Subscriber+) Stored ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104726	Name Directory <= 1.34.2 - Authenticated (Contributor+) ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100108	Social Share Buttons <= 1.30 - Authenticated (Subscriber...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96870	SureDash <= 1.12.0 - Authenticated (Subscriber+) Stored ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103520	HivePress <= 1.7.31 - Authenticated (Subscriber+) Stored ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94421	Church Admin <= 5.1.2 - Authenticated (Subscriber+) Stor...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-18558	Embed Any Document <= 2.7.13 - Authenticated (Contribu...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91862	Getwid <= 3.0.1 - Authenticated (Contributor+) Stored Cro...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100185	Directorist: AI-Powered Business Directory, Listings & Cla...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109985	xSpeed Cache: AI-Powered Performance Hub with MCP, ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104762	Kadence Blocks <= 3.7.12 - Authenticated (Author+) Store...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97643	GiveWP <= 4.17.0 - Authenticated (Contributor+) Stored C...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14877	Data Tables Generator by Supsystic <= 1.12.03 - Authenti...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104735	RSS Aggregator by Feedzy <= 5.2.10 - Authenticated (Co...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9696	Download Manager <= 3.3.58 - Authenticated (Contributo...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78068	Table Field Add-on for ACF and SCF <= 1.3.35 - Authentic...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-16776	MP3 Audio Player <= 5.14.2 - Authenticated (Contributor+...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14379	GamiPress <= 7.9.4 - Authenticated (Subscriber+) Stored ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93883	Advanced Classifieds & Directory Pro <= 3.4.4 - Authenti...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96743	Table Field Add-on for ACF and SCF <= 1.4.1-RC2 - Authe...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96648	Data Tables Generator by Supsystic <= 1.15.1 - Authenticat...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104993	GeoDirectory <= 2.8.188 - Authenticated (Subscriber+) St...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102401	Download Manager <= 3.3.71 - Authenticated (Contributo...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97630	FV Flowplayer Video Player <= 7.5.54.7212 - Authenticate...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86610	Download Manager < 3.3.71 - Author+ Stored XSS via Pac...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101925	bbp style pack <= 6.4.8 - Authenticated (Subscriber+) Sto...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-111726	Themify Builder <= 7.8.2 - Authenticated (Contributor+) S...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109989	Themify Popup <= 1.4.7 - Authenticated (Author+) Stored...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109983	YMC Filter <= 3.12.19 - Authenticated (Author+) Stored D...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97470	Tourfic <= 3.0.1 - Authenticated (Subscriber+) Stored Cro...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110703	GeoDirectory <= 2.8.191 - Authenticated (Subscriber+) St...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97020	PO/MO Editor <= 1.4.2 - Authenticated (Subscriber+) Stor...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103425	Booking Package <= 1.7.29 - Authenticated (Contributor+...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-90992	Redux Framework <= 4.5.14 - Authenticated (Subscriber+...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96268	Awesome Support <= 6.4.0 - Authenticated (Subscriber+...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89424	Duplicate Post <= 1.5.6 - Authenticated (Subscriber+) Sto...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95807	FV Player 8 <= 8.1.7 - Authenticated (Contributor+) Stored...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115513	OpenCATS before 0.12.0 Stored XSS via MRU Navigation ...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-47790	Privilege Escalation via QuFTP Log-based XSS	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63430	ammonia: mXSS in ammonia via MathML `annotation-xml`...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103388	MISP Stored Cross-Site Scripting via JavaScript URL in G...	Medium / 6.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104906	MISP TAXII Object Viewer Stored XSS via Unescaped JSO...	Medium / 6.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103389	MISP Stored Cross-Site Scripting via Unvalidated Galaxy I...	Medium / 6.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101156	Security Advisory 0192	Medium / 6.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-22896	Stored XSS via Interface Name in Network & Virtual Switc...	Medium / 6.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2024-34326	CVE-2024-34326: ProPhoenix Law RMS v2022.2403.3.1...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-93880	Greenshift <= 13.2.0 - Reflected Cross-Site Scripting via '...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102459	DigiWin | EasyFlow .NET - Reflected Cross-site Scripting	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103909	Calculated Fields Form <= 5.5.1.5 - Reflected DOM-Based...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92826	EWWW Image Optimizer <= 8.7.7 - Reflected Cross-Site ...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103888	WPC Smart Quick View for WooCommerce <= 4.4.0 - Ref...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92974	Photo Gallery by 10Web <= 1.8.46 - Reflected Cross-Site ...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93896	WPFront Notification Bar <= 3.5.1 - Reflected Cross-Site S...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104313	WPC Estimated Delivery Date for WooCommerce <= 4.0.1...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92538	LearnPress <= 4.4.7 - Reflected DOM-Based Cross-Site ...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76975	SAP: Cross-Site Scripting (XSS) vulnerability in SAPUI5 (...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85492	All in One SEO <= 5.0.1.1 - Reflected DOM-Based Cross-Si...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94402	IBM vulnerable to cross-site scripting (XSS) via unsanitize...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97652	WP Statistics <= 14.16.14 - Reflected Cross-Site Scripting ...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2024-34321	CVE-2024-34321: ProPhoenix Law RMS v2022.2403.3.10...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87869	Filter Everything — WordPress & WooCommerce Filters <...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103998	Form Maker by 10Web <= 1.15.48 - Reflected Cross-Site S...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100521	Cotonti through 1.0.0 Reflected XSS via search highlight p...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103481	Gwolle Guestbook <= 5.1.1 - Reflected Cross-Site Scriptin...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113787	odf-kit: HTML injection leading to XSS in odtToHtml() via ...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2024-5139	Cross-Site Scripting via Authentication Endpoint in Multip...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked

INDUSFACE™ ©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-84925	Avada | Website Builder For WordPress & WooCommerce ...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-38671	CVE-2026-38671: Cross Site Scripting vulnerability in Ellu...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92243	Ivory Search <= 5.5.18 - Reflected DOM-Based Cross-Sit...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92551	Paid Membership Plugin, Ecommerce, User Registration F...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88963	Tutor LMS <= 4.0.8 - Authenticated (Subscriber+) Reflect...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2023-38375	IBM Cloud Pak System Cross-Site Scripting	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111601	Hippoo Mobile App for WooCommerce <= 1.12.0 - Reflect...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102258	CVE-2026-102258: Post-authentication Stored Cross-Sit...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110306	fast-uri vulnerable to URI scheme spoofing via percent-e...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111059	Mercury: Stored / DOM Cross-Site Scripting (XSS): mr.Ma...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-4413	IBM Concert Software Cross-Site Scripting	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94154	Aurora Heatmap <= 1.7.2 - Unauthenticated Stored Cross-...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12054	Download Manager <= 3.3.57 - Unauthenticated DOM-Ba...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89117	Cross-Site Scripting (XSS) vulnerability in SAP NetWeave...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89427	Ad Inserter <= 2.8.18 - Reflected Cross-Site Scripting via '...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108925	Cohesity - CWE-80: Improper Neutralization of Script-Rel...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89047	Social Media Share Buttons & Social Sharing Icons <= 3.0....	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49264	OAuthLib: Unsafe JSONP callback injection in Revocation...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104250	unstructured: Stored XSS via unescaped HTML generation	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103527	Thelia v2.6.0's Smarty templates (address.html and addre...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2025-27895	DB2 Recovery Expert for Linux, UNIX and Windows Cross...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85967	Cross-site scripting in Progress MarkLogic Server	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-27897	IBM Db2 Recovery Expert for Linux, Unix and Windows Cr...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-27896	IBM Db2 Recovery Expert for Linux, Unix and Windows Cr...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15180	Tracking Code Manager <= 2.6.0 - Reflected Cross-Site S...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104140	QGIS: Stored XSS in WFS3 getFeatures HTML page via un...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106701	CVE-2026-106701: ELADMIN v2.7 and before is vulnerabl...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18557	Photo Gallery by 10Web <= 1.8.42 - Reflected Cross-Site ...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12380	Reflected XSS in Akıllı Ticaret's E-Commerce Pack	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100243	Stored XSS in WikiSEO author and image properties on ac...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100245	Stored XSS on Wikibase Special:SetSiteLink via unescape...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103046	WikifunctionsFragmentRenderer does unsafe string repla...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103045	XSS in Refreshed skin	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103047	XSS through i18n message in CentralAuth	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103049	XSS in Cargo's Special:CargoQuery page due to unsanitiz...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103050	Stored i18n XSS in MassMessage	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103051	Stored i18n XSSs in CentralNotice	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18205	XSS in Ticimax Informatics' Ticimax E-Commerce Platform	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113659	ApostropheCMS: Client-side Prototype Pollution in apos....	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-19902	Ad Inserter <= 2.8.18 - Reflected Cross-Site Scripting via ...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-100179	Calculated Fields Form <= 5.5.1.3 - Reflected DOM-Based...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-69723	CVE-2025-69723: A reflected cross-site scripting (XSS) ...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82382	Apache Roller: Reflected cross-site scripting in the frontp...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86507	Apache Roller: Stored XSS in comment moderation via co...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102333	httpdbg before 2.2.1 Stored Cross-Site Scripting via javas...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102372	GestSup before 3.2.61 Stored XSS via Email Body in LOGI...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102374	GestSup before 3.2.62 Stored XSS via Double-Decoded E...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100238	Flow colon-separator and flow-guidedtour-optin-welcom...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87752	HTML Injection in Rolantis Information Technologies' Age...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89100	Payment Plugins for Stripe WooCommerce <= 4.0.17 - Ref...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-5725	Favicon Rotator <= 1.2.11 - Reflected Cross-Site Scripting ...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95165	CVE-2026-95165: Bacularis 5.4.0 - 6.5.1 is vulnerable to C...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94448	Reset context tracking on consecutive template expressi...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107393	FreeScout: Stored HTML Injection in Administrator Alert E...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96594	Gitea repository media API stored XSS	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93638	Zimbra Collaboration Suite Pre-Authentication Reflected ...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
GHSA-2RQM-H6HV-G79V	odf-kit has HTML injection leading to XSS in odsToHtml() ...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100694	Hugo before 0.166.0 Cross-Site Scripting via text/org	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91206	Apache Roller: Reflected XSS in the optional LDAP comm...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91204	Apache Roller: Stored javascript: URI in HTML comments	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-82546	Apache Roller: Stored cross-site scripting through incomi...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54615	Part-DB: Stored XSS / HTML injection in activity-log Extra ...	Medium / 6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-90914	Joomla! Core - [20260904] - Core - XSS in the generic m...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-90906	Joomla! Core - [20260901] - XSS in HTMLHelper::link me...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2023-54409	Frappe before 13.46.1 XSS via html2text Weak Sanitization	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92225	Joomla! Core - [20260912] - Core - XSS in module list in ...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79363	CVE-2026-79363: Cloudron 9.1.7 and 9.2 contain a stored...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92224	Joomla! Core - [20260911] - Core - XSS in link toolbar lay...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102384	WordPress Supreme Modules Lite plugin <= 2.5.63 - Cros...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-71454	CVE-2026-71454: Improper neutralization of input during...	Medium / 5.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55600	Part-DB: Stored HTML injection in BOM validation results ...	Medium / 5.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76303	Cisco: Stored Cross-Site Scripting (XSS) through App Do...	Medium / 5.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57568	Lychee: Stored XSS via Markdown javascript: Links in Pho...	Medium / 5.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59788	Zabbix: Stored XSS vulnerability in OAuth configuration fo...	Medium / 5.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107889	Keycloak-services: keycloak-services: stored xss on logi...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95717	HPE: Authenticated Stored Cross-Site Scripting (XSS) Vul...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97238	WordPress JetEngine plugin <= 3.8.14.3 - Cross Site Scri...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95166	CVE-2026-95166: In Bacularis v1.0.0 - 6.5.1 when adding ...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106033	Ansible: ansible-ui: ansible ui dom xss in /redirect next pa...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93633	Zimbra Collaboration Suite Briefcase CSS Sanitization Byp...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-82969	Stored XSS in BİMSER's eBA Plus	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75063	IBM Planning Analytics Local is affected by security vulne...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113661	ApostropheCMS: Incomplete CVE-2026-53606: `meta htt...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112951	ApostropheCMS: Color field validation bypass allows stor...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105694	Penpot: Stored XSS via Unsanitised SVG Uploads	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103667	Gitea container registry stored XSS through blob media ty...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2024-31027	CVE-2024-31027: Cross Site Scripting vulnerability in Gre...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13258	IBM DataPower Gateway Cross-Site Scripting	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82387	Apache Roller: Stored cross-site scripting via uploaded m...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110073	Adobe Experience Manager | Cross-site Scripting (Stored...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110037	Adobe Experience Manager | Cross-site Scripting (Stored...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109415	Adobe Experience Manager | Cross-site Scripting (Stored...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107396	Indico: Cross-Site-Scripting in link fields	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92085	Stored XSS in TMT Machine's Talassoft Industrial Manag...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107380	enshrined/svg-sanitize: Stored XSS via DTD Entity / HTM...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79816	HPE: Unauthenticated DOM-Based Cross-Site Scripting (...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106632	Adobe Experience Manager | Cross-site Scripting (DOM-...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110076	Adobe Experience Manager | Cross-site Scripting (DOM-...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106631	Adobe Experience Manager | Cross-site Scripting (Stored...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106628	Adobe Experience Manager | Cross-site Scripting (DOM-...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-106151	Cross-Site Scripting in Validator Validation Messages in K...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106150	Cross-site Scripting (XSS) in Kendo UI for jQuery Splitter, ...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106706	CVE-2026-106706: XXL-JOB through 3.5.0-SNAPSHOT i...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110074	Adobe Experience Manager | Cross-site Scripting (DOM-...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110075	Adobe Experience Manager | Cross-site Scripting (DOM-...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106148	Cross-Site Scripting via TabStrip, Menu, and PanelBar Im...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106147	Cross-Site Scripting via ListBox Bound Text in Kendo UI f...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106149	Cross-site Scripting (XSS) in Kendo UI for jQuery Menu	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106707	CVE-2026-106707: XXL-JOB <=3.5.0-SNAPSHOT contai...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103974	lichess.org: Stored HTML Injection via PGN Annotator Ta...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100630	AVideo Stored XSS via HTML Entity Bypass in trailer1 Field	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110078	Adobe Experience Manager | Cross-site Scripting (DOM-...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102342	ammonia allows stored XSS through unsanitized SVG ani...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106161	Cross-Site Scripting via Badge Text Binding in Kendo UI f...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106633	Adobe Experience Manager | Cross-site Scripting (Stored...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106138	Cross-Site Scripting via Chart Tooltip in KendoReact	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103424	Anti-Spam by CleanTalk <= 6.88 - Unauthenticated Store...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104587	CVE-2026-104587: blob42 gosuki through commit 6e2bf...	Medium / 5.4	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-96450	WordPress pixfort Core plugin < 4.3.3 - Cross Site Scripti...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-52097	CVE-2025-52097: Cross Site Scripting vulnerability in Ins...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-90821	GitLab: Improper Neutralization of Input During Web Page...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103482	Simple Newsletter Plugin <= 4.3.10 - Unauthenticated Sto...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83958	Adobe Experience Manager | Cross-site Scripting (DOM-...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-48398	Adobe Experience Manager | Cross-site Scripting (DOM-...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107682	Adobe Experience Manager | Cross-site Scripting (DOM-...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107305	Adobe Experience Manager | Cross-site Scripting (Stored...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107649	Events Made Easy <= 3.2.22 - Unauthenticated Stored Cr...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110252	WPeMatico RSS Feed Fetcher <= 2.9 - Unauthenticated S...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102295	Quay: quay: dom-based cross-site scripting via oauth loc...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107265	Leaflet - Moderately critical - Cross site scripting - SA-C...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107252	MathJax: LaTeX for Drupal - Critical - Cross site scripting ...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76976	Cross-Site Scripting (XSS) vulnerability in SAP NetWeave...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-58391	OPNsense: Stored XSS in Firewall Rules/NAT pages via a ...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-58392	OPNsense: Stored XSS in Services: NTP GPS	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-67165	HCL Connections is vulnerable to cross-site scripting (XSS)	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78471	Autoptimize <= 3.1.15.1 - Unauthenticated Stored Cross-Si...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110082	Adobe Experience Manager | Cross-site Scripting (Reflec...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106139	Cross-Site Scripting via Chart Tooltip in Kendo UI for Vue	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103421	WPMobile.App <= 11.84 - Unauthenticated Stored Cross-...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110081	Adobe Experience Manager | Cross-site Scripting (Stored...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-110079	Adobe Experience Manager | Cross-site Scripting (DOM-...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110080	Adobe Experience Manager | Cross-site Scripting (DOM-...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110077	Adobe Experience Manager | Cross-site Scripting (DOM-...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78407	Security vulnerabilities have been found in IBM Verify Ide...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82381	Apache Roller: Stored cross-site scripting in the authorin...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93684	Apache Impala: Stored XSS in Impala query plans	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114133	Nuxt server islands render `useHeadSafe` input without s...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-4418	IBM Cloud Pak System HTML Injection	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109131	Ansible-ui: ansible-ui: stored xss via unsafe javascript url ...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100180	Jeg Kit for Elementor <= 3.2.19 - Unauthenticated Stored ...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83960	Adobe Experience Manager | Cross-site Scripting (DOM-...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-19810	Cross-Site Scripting (XSS) in Symantec Endpoint Detecti...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12241	Advanced Woo Labels – Product Labels & Badges for Woo...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106153	Cross-site Scripting (XSS) in Kendo UI for jQuery Calenda...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112958	ApostropheCMS: Stored XSS via Unescaped Widget Styl...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103871	pulp_python: Simple index renders project names without...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105829	League CommonMark 1.3.0 before 2.10.2 Stored XSS via ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107797	Jivejdon through 5.0 Reflected XSS via postThread.jsp to ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116203	YesWiki before 4.7.0 Stored XSS via filtertags Action Para...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109565	Rapyd Admin 9.4.0 before 9.20.0 Stored XSS via select-li...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-100381	UploadWizard Flickr collection and set titles allow DOM X...	Medium / 5.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-63355	CVE-2026-63355: Affected devices do not properly sanit...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115351	Mistune 3.2.1 before 3.3.0 CSS Injection via Figure Directi...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104083	SmarterMail < Build 9777 Stored Mutation XSS via MathM...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63169	Omnispace Agora Project < 26.10.0 Stored XSS via Messe...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113654	ApostropheCMS sanitize-html: nonTextTags discard regi...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113442	Cross-Site Scripting in extension "TYPO3 Fluid-Form by ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113583	Cypht 2.0.0 through 2.12.2 Stored DOM XSS via externalR...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2024-58391	Frappe before 15.4.0 XSS via Printview Parameters	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101109	Joomla Extension - ordasoft.com - Reflected Cross-Site ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97165	Joomla Extension - svenbluege.de - Reflected XSS and o...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100753	Joomla Extension - ordasoft.com - Reflected Cross-Site ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107796	Jivejdon through commit ee67a65e Reflected XSS via tag...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105114	OpenAM before 16.1.3 Reflected XSS via OAuth2 Authoriz...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111442	CVE-2026-111442: Backdrop CMS Core 1.35.x before 1.35...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109322	Grav Guestbook before 0.5.2 Stored XSS via AJAX Pagina...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104477	Showdown through 2.1.0 XSS via unescaped quote in href...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-15591	Cross-Site Scripting (XSS) vulnerability identified in Open...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-47096	AJA HELO Plus < 2.1.7 Stored XSS via System Name Para...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63357	CVE-2026-63357: Affected devices do not properly sanit...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-109328	Admidio 5.0.0 before 5.0.15 Unauthenticated Stored XSS ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104900	MISP Stored XSS via Unescaped Count Field Value in Re...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105124	W (wcms) through 3.18.0 Unauthenticated Stored XSS via ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63352	CVE-2026-63352: Affected devices do not properly sanit...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102426	Joomla Extension - joomshaper.com - Reflected XSS in th...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102778	Joomla Extension - svenbluege.de - Cross-site scripting ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116206	YesWiki 4.2.0 before 4.7.0 Stored XSS via Comment Raw-...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100380	Reflected XSS in Wikibase Special:SetLabel language vali...	Medium / 5.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-63356	CVE-2026-63356: Affected devices do not properly sanit...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63351	CVE-2026-63351: Affected devices do not properly valid...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109352	LibreNMS before 26.9.0 Stored XSS via wireless sensor d...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109355	LibreNMS before 26.9.0 Stored XSS via Tools Oxidized N...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101111	Joomla Extension - ordasoft.com - Reflected Cross-Site ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105831	EspoCRM before 10.0.6 Unauthenticated Stored HTML Inj...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114404	PHPPresentation 1.2.0 XSS via Writer\HTML Text Runs, H...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115350	Mistune before 3.3.0 Stored XSS via Include Directive HT...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109662	Frappe ERPNext before 15.112.0 Stored XSS via Public Por...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-58394	OPNsense: Stored XSS in Administration Settings via Cert...	Medium / 5.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-5782	Reflected XSS in MRV Technology's TurkHotspot	Medium / 5.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110626	ClipBucket v5 through 5.5.3-#206 Reflected XSS via edit_...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-63168	Omnispace Agora Project < 26.10.0 Stored XSS via Neste...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63157	Omnispace Agora Project < 26.10.0 Stored XSS via Links ...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63156	Omnispace Agora Project < 26.10.0 Reflected XSS via visi...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63148	Omnispace Agora Project < 26.10.0 Stored XSS via Poll-R...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113683	VPL for Moodle before 5.0.0 Reflected XSS via similarity/...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113350	react-admin before 5.15.5 Stored XSS via UrlField and File...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109345	DOMPurify before 3.4.16 XSS via IN_PLACE Returned Raw...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109344	DOMPurify from 3.4.13 before 3.4.16 DOM XSS via IN_PLA...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63147	Omnispace Agora Project < 26.10.0 Stored XSS via Uploa...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109670	Frappe ERPNext before 15.110.0 Stored XSS via Item Reco...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-58403	Reflected Cross-Site Scripting (XSS) in CGM CLININET	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-4952	Stored Cross-Site Scripting in OrderAdministration Portal ...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-4951	Reflected Cross-Site Scripting in CustomerAdministration...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100691	Hugo before 0.166.0 Stored XSS via lineAnchors code blo...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112333	GFI Archiver < 15.14 Stored XSS via MailInsights.aspx	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116139	WWBN AVideo 26.0 through 29.3.0 Stored XSS via Comm...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107798	Jivejdon through commit ee67a65e Stored XSS via Markd...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116169	SiYuan 2.10.0 before 3.8.7 Stored XSS via KaTeX \href in ...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105224	YesWiki before 4.6.7 Stored XSS via Bazar valeur Action	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73641	Multiple Reflected XSS in Dayforce ESS Excelity	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-116202	YesWiki before 4.7.0 Stored XSS via ImageField SVG Uplo...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114407	e107 CMS before 2.3.13 Reflected XSS via search.php aut...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102756	DataEase bar-horizontal Axis Label Tooltip Stored Cross-...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102755	DataEase Datasource/Dataset Folder Name Stored Cross-...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110228	wallabag 2.6.13 through 2.6.14 Stored XSS via Failed HTM...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110224	QloApps through 1.7.0 Reflected XSS via Search Alias Vali...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110221	QloApps through 1.7.0 Reflected XSS via Advanced Price ...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110625	ClipBucket v5 through 5.5.3-#206 Reflected XSS via type...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2023-54408	Frappe before 14.31.0 HTML Injection via Weak Escaping	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2012-20003	Custom Tables WordPress Plugin < 3.4.6 Reflected XSS v...	Medium / 5.1	VULNCHECK KEV	✓ Blocked
CVE-2026-110878	Aureus ERP through 1.6.0 Stored XSS via Inventory Rule A...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111168	LibreDesk before 2.9.0-rc.8 Stored XSS via SVG Upload C...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2014-125132	Blogroll Fun WordPress Plugin < 0.8.5 Reflected XSS via b...	Medium / 5.1	VULNCHECK KEV	✓ Blocked
CVE-2014-125131	DedeCMS 5.6 / 5.7 Reflected XSS via adminDirHand in co...	Medium / 5.1	VULNCHECK KEV	✓ Blocked
CVE-2012-20005	SocialFit WordPress Plugin 1.2.2 Reflected XSS via popup...	Medium / 5.1	VULNCHECK KEV	✓ Blocked
CVE-2012-20004	K-news WordPress Plugin < 1.1.1 Reflected XSS via fontpic...	Medium / 5.1	VULNCHECK KEV	✓ Blocked
CVE-2026-104466	YesWiki before 4.6.7 Stored XSS via Wakka Markdown Im...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104465	YesWiki before 4.6.7 Reflected XSS via field Parameter in ...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104473	YesWiki before 4.5.3 Multiple Reflected XSS via BazaR an...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104901	MISP ID Translator: Unescaped Remote Event ID Enables ...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-111896	phpMyFAQ 4.2.0-alpha before 4.2.0-beta Stored XSS via ...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111903	phpMyFAQ 4.2.0-alpha before 4.2.0-beta Stored XSS via ...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111894	phpMyFAQ 3.2.1 before 4.1.9 and 4.2.0-alpha before 4.2.0...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112111	CVE-2026-112111: The Bootstrap Shortcodes plugin for W...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109300	Open WebUI 0.6.31 before 0.11.4 Stored XSS via Tool-Call ...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110103	bbs-go through 4.4.6 Stored XSS via Image Upload Conte...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110219	QloApps through 1.7.0 Reflected XSS via Additional Facilit...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103589	QloApps through 1.7.0 Reflected XSS via Room Type Editor	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107801	Jivejdon through 5.0 Stored XSS via Attachment Upload C...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107800	Jivejdon through 5.0 Stored XSS via Private Short Messa...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107799	Jivejdon through 5.0 Stored XSS via messageListBody.jsp...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103590	QloApps through 1.7.0 Reflected XSS via Length of Stay Fi...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103588	QloApps through 1.7.0 Reflected XSS via exceptions field	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-4264	Reflected Cross-Site Scripting in BeeTienda eCommerce ...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112289	Koalixcrm through 1.14.0 Stored XSS via Task Title in Djan...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112148	CVE-2026-112148: A vulnerability has been identified in LI...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-53711	MCP ContextForge: Global Prompts stored cross-site scri...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110101	Koillection through 1.8.4 Stored XSS via Datum File Attach...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109392	Pimcore through 2026.3.1 Stored XSS via ExternalImage F...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103587	QloApps through 1.7.0 Reflected XSS via Book Now Searc...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-109327	Admidio 4.0.12 through 4.3.17 and 5.0.0 before 5.0.15 Refl...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103662	MISP Reflected XSS in Taxonomy Tag Confirmation Forms	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63171	Omnispace Agora Project < 26.10.0 Stored XSS via Categ...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97667	Nexus Repository 3 - Stored Cross-Site Scripting in Brow...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105090	CVE-2026-105090: Formbricks before 5.4.4 and 6 before...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104479	Shopclass before 6.2.0 Stored XSS via Listing Description...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104475	IDURAR ERP CRM through 4.1.1 Stored XSS via SVG Upload	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104461	YesWiki before 4.6.7 Stored XSS via Unsanitized SVG Upl...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101890	Prime Mover < 2.2.1 Stored XSS via Package Metadata	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96535	Cross-Site Scripting in the YouMind web application	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105116	OpenAM before 16.1.3 Latent XSS in SAML Load-Balancer ...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2016-20102	JavaMelody < 1.60.0 Reflected XSS via monitoring graph ...	Medium / 5.1	VULNCHECK KEV	✓ Blocked
CVE-2026-108725	Cheshire Cat AI core through 2.0.23 Stored XSS via uploa...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111284	Aureus ERP through 1.6.0 Stored XSS via Time Off Holida...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109597	Hugo v0.60.0 before v0.167.0 Stored XSS via Table of Con...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-71430	Frappe before 15.91.1 Stored XSS via Leaderboard User N...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2016-20098	Moderator Toolbox before 4.0.14 Stored XSS via Removal ...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111713	tarteaucitron.js before 1.37.0 XSS via getElemAttr Attribute...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105397	LearnPress WordPress Plugin through 4.4.9.1 Stored XSS ...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100522	Cotonti through 1.0.0 Reflected XSS via message.php lng ...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-115507	Vikunja 2.2.0 before 2.7.1 HTML Injection via Notification E...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109602	Frappe before v16.31.0 Stored XSS via Dashboard Chart Fi...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109657	Frappe ERPNext 16.x before 16.27.0 Stored XSS via Unesc...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2017-20288	QCubed 3.1.1 Reflected XSS via installer step_2.php	Medium / 5.1	VULNCHECK KEV	✓ Blocked
CVE-2017-20290	Discourse < 1.9.0.beta13 Reflected XSS via /email/unsubs...	Medium / 5.1	VULNCHECK KEV	✓ Blocked
CVE-2020-37284	Sickbeard build-507 Reflected XSS via testNaming patter...	Medium / 5.1	VULNCHECK KEV	✓ Blocked
CVE-2023-54413	WPML Multilingual CMS WordPress Plugin < 4.6.1 Reflect...	Medium / 5.1	VULNCHECK KEV	✓ Blocked
CVE-2024-58394	Retool < 3.88.0 XSS via /api/imageProxy SVG Proxying	Medium / 5.1	VULNCHECK KEV	✓ Blocked
CVE-2026-114570	WordPress Core <= 7.0.2 - Authenticated (Contributor+) ...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101357	SEOPress <= 10.2 - Authenticated (Subscriber+) Stored C...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-11936	Security vulnerabilities have been found in IBM Verify Ide...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107757	Gallery Custom Links <= 2.3.3 - Authenticated (Subscribe...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-64392	CVE-2025-64392: This vulnerability in Veeam Backup En...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-7172	Stored Cross-Site Scripting (XSS) in TPVEnlanube	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59669	Multiple vulnerabilities in the Repasat application	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-4950	Stored Cross-Site Scripting in CustomerAdministration Po...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-7170	Stored Cross-Site Scripting (XSS) in TPVEnlanube	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59668	Multiple vulnerabilities in the Repasat application	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104907	MISP: JavaScript Injection via Remote Tag ID in Event Pre...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111932	Coder before 2.34.2 Stored HTML Injection via Appearan...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-112184	MISP Workflow Module: Reflected XSS via Unescaped mi...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59666	Multiple vulnerabilities in the Repasat application	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-7171	Stored Cross-Site Scripting (XSS) in TPVEnlanube	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59670	Multiple vulnerabilities in the Repasat application	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59667	Multiple vulnerabilities in the Repasat application	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39991	Stored Cross-Site Scripting (XSS) in Note Station file uplo...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59673	Multiple vulnerabilities in the Repasat application	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59672	Multiple vulnerabilities in the Repasat application	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59660	Multiple vulnerabilities in the Repasat application	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59661	Multiple vulnerabilities in the Repasat application	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103664	MISP Reflected Cross-Site Scripting via Unsanitized Anal...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103524	Thelia v2.6.0 is vulnerable to multiple stored XSS vulnera...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-7175	Multiple vulnerabilities in Entradium by Crocantickets	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113355	Chatwoot before 4.14.0 Stored XSS via Help Center Video ...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69194	FileRise: Unsanitized footerHtml in Public Site Config	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-7176	Multiple vulnerabilities in Entradium by Crocantickets	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-7173	Multiple vulnerabilities in Entradium by Crocantickets	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-7174	Multiple vulnerabilities in Entradium by Crocantickets	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111232	Netgate pfSense CE 2.3.0 through 2.9.0 Stored XSS via S...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100383	Stored i18n XSS in WikiLambda's VisualEditor integration	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-48212	Stored XSS in external pages	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59671	Multiple vulnerabilities in the Repasat application	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59665	Multiple vulnerabilities in the Repasat application	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59663	Multiple vulnerabilities in the Repasat application	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113712	Cachet has Stored XSS in Incident Component	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100376	TemplateSandbox can be abused for XSS by asking anoth...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95662	Multiple vulnerabilities in the Repasat application	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59659	Multiple vulnerabilities in the Repasat application	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59664	Multiple vulnerabilities in the Repasat application	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59662	Multiple vulnerabilities in the Repasat application	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106159	Cross-Site Scripting via ToolBar ButtonGroup URLs in Ken...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100184	Calculated Fields Form <= 5.5.1.3 - Reflected DOM-Based...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87970	If-So Dynamic Content 1.8 - 1.10.1 - Reflected XSS via rend...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106444	Handlebars: JavaScript Injection via Unsafe Inline Embed...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100193	Tutor LMS <= 4.1.0 - Reflected Cross-Site Scripting via 'ta...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112949	Vitest: Code injection via unauthenticated manual mock r...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101324	Fluent Forms <= 6.2.14 - Reflected Cross-Site Scripting vi...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101921	WPForms <= 2.0.2.1 - Reflected Cross-Site Scripting via '...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106157	Cross-Site Scripting via PanelBar Item URLs in Kendo UI f...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114718	CVE-2026-114718: Roundcube Webmail before 1.6.20 and...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-106158	Cross-Site Scripting via Scheduler Resource Colors in Ke...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100263	CVE-2026-100263: In JetBrains YouTrack before 2026.2....	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103912	JetFormBuilder <= 3.6.6 - Reflected DOM-Based Cross-S...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106162	Cross-Site Scripting in FileManager Drag Hints in Kendo ...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88208	Microsoft Office SharePoint Spoofing Vulnerability	Medium / 4.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-28330	SolarWinds Observability Self-Hosted Cross-Site Scriptin...	Medium / 4.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102581	Moodle: xss in forum post templates due to insufficient es...	Medium / 4.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105784	Joplin whiteboard card rendering allows CSS injection int...	Medium / 4.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102859	Microsoft Office SharePoint Spoofing Vulnerability	Medium / 4.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55422	conda-forge.org: Stored DOM XSS via unsanitized danger...	Medium / 4.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88209	Microsoft Office SharePoint Spoofing Vulnerability	Medium / 4.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102864	Microsoft Office SharePoint Spoofing Vulnerability	Medium / 4.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107397	Indico: Cross-Site-Scripting in minutes editor	Medium / 4.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89106	SAP: Cross Site Scripting (XSS) vulnerability in SAPUI5	Medium / 4.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103897	Responsive Lightbox & Gallery <= 2.7.9 - Authenticated (E...	Medium / 4.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59994	EspoCRM: Pre-authentication stored HTML injection in str...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102586	Moodle: xss via password reset link due to insufficient us...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-6623	Stored Cross-Site Scripting via XML Input in Multiple WS...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102576	Quay: quay: dom-based cross-site scripting via unvalidat...	Medium / 4.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82326	HTML Injection in Enocta Educational's Enocta Platform	Medium / 4.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-107306	Menu Link Attributes - Moderately critical - Cross-site scr...	Low / 3.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110725	fast-uri vulnerable to scheme injection via an unescaped f...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113657	ApostropheCMS sanitize-html: SMIL animation namespac...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-21833	HCL AION is susceptible to a Missing "Content-Security-...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82127	Schema & Structured Data for WP & AMP < 1.67 - Editor+ ...	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55184	EspoCRM: Stored XSS in wysiwyg template fields if CSP i...	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-71189	Toptech TMS7 and TopHAT Cross-site Scripting	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-60008	Gitea Jupyter notebook UI redress through CSS class inje...	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-80517	WP Ultimate CSV Importer 7.17 - 9.1 - Admin+ Stored XSS ...	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55876	Helium: Stored XSS via Unrestricted SVG File Upload — A...	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104754	Rank Math SEO < 1.0.280 - Admin+ Stored XSS via Redire...	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114555	Data field - Moderately critical - Cross site scripting - SA-...	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89290	HTML Injection in İzometri Informatics' eimzamip	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111737	Speed Optimizer < 7.8.5 - Admin+ Stored XSS via DNS Pr...	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-15705	Contact Form by Supsystic < 1.8.0 - Admin+ Stored XSS	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104119	Simple Shopping Cart < 5.2.6 - Admin+ Stored XSS via Pa...	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-15703	WP Job Openings < 4.0.0 - Admin+ Stored XSS	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76894	ckan-mcp-server: DataStore Table UI resource does not ...	Low / 3.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102279	Laravel: XSS in Debug Page Information	Low / 3.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107308	Country - Moderately critical - Cross-site scripting - SA-...	Low / 3.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-87973	If-So Dynamic Content 1.9.9 - 1.10.1 - Editor+ Stored XSS v...	Low / 3.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-27085	WordPress Astra WordPress theme theme <= 4.13.12 - Co...	Low / 2.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-53575	EspoCRM: Persistent XSS via CSP nonce injection in appli...	Low / 2.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97711	Serialize JavaScript: Cross-site scripting (XSS) via unesc...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105111	Apache Commons BCEL: Class2HTML emits unescaped ...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115754	serialize-javascript 7.0.1 before 7.1.3 XSS via unescaped	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114130	Nuxt: Incomplete fix for GHSA-934w-87qh-qr26: a `javas...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114127	Astro: Arbitrary CSS injection in Astro View Transitions	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115730	i18next-http-backend: Namespace value starting with / fo...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114061	SvelteKit : XSS via untrusted cache-control header in prer...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111233	Netgate pfSense CE 2.7.1 through 2.9.0 Reflected XSS via ...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108722	open-computer-use through commit 610bac8 Stored XSS...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107272	Gophish through 0.12.1 XSS via Unescaped SMTP Server ...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112290	MI6 @ukic/canary-web-components 3.0.0-canary.12 bef...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56599	HCL BigFix Service Management is affected by multiple s...	Low / 2.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115519	Sensitive cookies without 'Secure' and 'HttpOnly' attribut...	Low / 2.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112945	Vite: Cross origin script execution through Vite custom mi...	Low / 2.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110627	ClipBucket v5 through 5.5.3-#206 Reflected XSS via add_...	Low / 2.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108852	Deep Chat through 2.5.1 XSS via Markdown Link Validatio...	Low / 2.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109307	Craft CMS 5.0.0 before 5.10.14 DOM XSS via returnUrl in 2...	Low / 2.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-103923	KaTeX: Existing prototype pollution can bypass trust restri...	Low / 2.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115897	Serialize JavaScript: Cross-site scripting (XSS) via unesc...	Low / 2.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110239	Rapyd Admin before 9.20.0 Stored XSS via rich-text Com...	Low / 2.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103489	CVE-2026-103489: In JetBrains YouTrack before 2026.2....	Low / 2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104808	Mitel MiVoice Office 400 stored Cross-Site Scripting	Low / 1.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104807	Mitel MiVoice Office 400 stored Cross-Site Scripting	Low / 1.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103585	attacker-controlled javascript license URL via XSS	Low / 1.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103445	Stored XSS through PageForms #autoedit redirect links	Low / 1.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103444	Stored XSS through system messages in WikiForum	Low / 1.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103443	API permits session-seeded javascript URL XSS	Low / 1.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103437	ReadingLists imported metadata permits JavaScript URL ...	Low / 1.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103584	attacker-controlled javascript license URL via XSS	Low / 1.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-0316	PAN-OS: Stored Cross-Site Scripting (XSS) Vulnerability	Low / 1.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103438	Various rawParams() and escaped() updates to prevent X...	Low / 0.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103439	Various rawParams() and escaped() updates to prevent X...	Low / 0.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107260	Sector Distribution - Moderately critical - Cross-site scrip...	Low / 0	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110738	Gin Admin Theme - Moderately critical - Cross-site scripti...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108515	Drupal core - Moderately critical - Cross-site scripting - S...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108514	Drupal core - Moderately critical - Cross-site scripting - S...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-64944	Apache Answer: Stored XSS via unsanitized HTML in imp...	Unscored	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 1221 blocked · avg CVSS 6.4 · 1 CISA KEV (continued)				
CVE-2026-114527	UI Icons - Critical - Cross site scripting - SA-CONTRIB-20...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114528	Zero Point - Critical - Cross-site scripting - SA-CONTRIB-...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114526	Black Hole - Critical - Cross-site scripting - SA-CONTRIB-...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114525	ABC - Critical - Cross-site scripting - SA-CONTRIB-2026...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114529	CSV Field - Moderately critical - Cross site Scripting - SA-...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114531	Swiper formatter - Moderately critical - Cross-site scripti...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114532	UI Icons - Moderately critical - Cross-site scripting - SA-...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114534	Block Attributes - Moderately critical - Cross site Scriptin...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114536	USWDS Paragraph Components - Moderately critical - Cr...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114538	Bootstrap - Moderately critical - Cross-site scripting - SA...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV				
CVE-2026-76570	Joomla Extension - joomcode.com - Unauthenticated SQ...	Critical / 10	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-55572	e107: SQL injection in alt_auth plugin (otherdb / e107db ba...	Critical / 10	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-12260	SQL injection in the NetBoard CRM demo platform	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79798	HPE: Authenticated SQL Injection Vulnerabilities in ClearP...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18782	SQL Injection in Trex Digital Manufacturing's Trex MES	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82307	Multiple Vulnerabilities in Dolusoft Software's SOPLOG	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107081	CVE-2026-107081: SQL injection via identifier injection in ...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-64959	Apache Kylin: Missing authentication on certain cache AP...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-111444	CVE-2026-111444: Wheels through 4.1.2 allows SQL injec...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-110911	CVE-2026-110911: Wheels 1.1.8 through 4.1.1 allows SQL in...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-55684	WeGIA: SQL Injection in html/socio/sistema/cadastro_cob...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-97668	Abandoned Cart Pro for WooCommerce <= 10.8.0 - Unaut...	Critical / 9.8	VULNCHECK KEV	✓ Blocked
CVE-2026-55680	WeGIA: Unauthenticated SQL Injection in cadastro_cobra...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-108065	Unauthenticated SQL Injection in Channel Software WebA...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-55683	WeGIA: SQL Injection in html/socio/sistema/cadastro_cob...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-79858	HPE: Unauthenticated SQL Injection Vulnerability in the P...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108474	CVE-2026-108474: In JetBrains Exposed before 1.5.1 sQL ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-80381	Multiple vulnerabilities affect the Sniffer component as pa...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105845	Payload: SQL Injection in SQLite and Postgres	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88424	CVE-2026-88424: FineAdmin v1.0 was discovered to con...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88395	CVE-2026-88395: GouGuOA v6.0.5 and before is vulnera...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107083	CVE-2026-107083: SENAYAN Library Management Syste...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2023-54400	Fumeng Cloud SQL Injection via AjaxMethod.ashx getEm...	Critical / 9.8	VULNCHECK KEV	✓ Blocked
CVE-2026-114625	Security Advisory 0199	Critical / 9.4	CISA KEV	✓ Blocked
CVE-2026-96428	Flowring Agentflow 4.0 - SQL Injection	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109894	WordPress Booktics plugin <= 1.0.29 - SQL Injection vuln...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111852	WordPress Ajax Search Lite plugin <= 4.14.6 - SQL Injecti...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32557	WordPress WooCommerce Appointments plugin <= 5.3.2...	Critical / 9.3	VULNCHECK KEV	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-39785	WordPress Gmedia Photo Gallery plugin <= 1.25.1 - SQL In...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39795	WordPress SendPress Newsletters plugin <= 1.26.1.20 - S...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96429	Flowring Agentflow 4.0 - SQL Injection	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96822	WordPress Books Gallery plugin <= 4.8.3 - SQL Injection ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108497	WordPress Amelia plugin <= 2.4.10 - SQL Injection vulner...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-111472	SQL injection in TSG Profleet	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94388	WordPress Green Popups plugin < 7.6.3 - SQL Injection v...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109698	WordPress Mang Board WP plugin <= 2.4.4 - SQL Injectio...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-103355	WordPress Unlimited Elements For Elementor (Free Widg...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-62071	WordPress WordPress File Upload plugin <= 5.1.10 - SQL I...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-109688	WordPress Link Whisper Free plugin <= 0.9.7 - SQL Inject...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-96330	WordPress tagDiv Opt-In Builder plugin <= 1.7.6 - SQL Inje...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62031	WordPress uListing plugin <= 2.2.0 - SQL Injection vulner...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40800	WordPress ELEX WooCommerce Advanced Bulk Edit Pro...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39746	WordPress Booknetic plugin < 5.10.3 - SQL Injection vuln...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39764	WordPress Radius Booking — Booking Calendar for Appoi...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105889	WordPress Tickera plugin <= 3.6.0.6 - SQL Injection vuln...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96327	WordPress WPLMS plugin < 1.9.9.8.2 - SQL Injection vuln...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96331	WordPress Ajax Search Pro plugin <= 4.29.1 - SQL Injecti...	Critical / 9.3	VULNCHECK KEV	✓ Blocked
CVE-2026-95605	WordPress WP Data Access plugin <= 5.5.82 - SQL Injecti...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-102782	Joomla Extension - ordasoft.com - Unauthenticated SQL i...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-42415	WordPress Porto Theme - Functionality plugin <= 3.9.3 - ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107103	SQL Injection Vulnerability in Manacle Technologies ERP ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111402	WordPress Newsletters plugin <= 4.18.1 - SQL Injection vu...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42417	WordPress ARMember Premium plugin <= 7.8 - SQL Injec...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93947	WordPress Traveler theme <= 3.2.9 - SQL Injection vulne...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96328	WordPress JNews - Pay Writer plugin <= 12.0.1 - SQL Inje...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-41555	WordPress Newsletter Subscription Form – User Subscrip...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102428	Joomla Extension - ordasoft.com - Unauthenticated SQL i...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108107	PHPNuxBill through 2025.3.20 Unauthenticated SQL Inje...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103352	WordPress WP BASE Booking plugin <= 6.4.0 - SQL Injec...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94130	Joomla Extension - joomlaboat.com - Unauthenticated S...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-101110	Joomla Extension - ordasoft.com - Unauthenticated SQL I...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-100752	Joomla Extension - ordasoft.com - Unauthenticated SQL I...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-101108	Joomla Extension - ordasoft.com - Unauthenticated SQL I...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-112327	WordPress Amelia plugin <= 2.4.11 - SQL Injection vulnera...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73640	Time-based SQL Injection in Dayforce ESS Excelity	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112860	WordPress Participants Database plugin <= 2.7.8.5 - SQL I...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112866	WordPress Product Filter by WBW plugin <= 3.4.6 - SQL I...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96809	WordPress EduAdmin Booking plugin < 6.0.0 - SQL Injecti...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-109573	phpMyFAQ before 4.1.9 SQL Injection via api/autocomplet...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115324	mem0 0.1.117 before 1.0.8 SQL Injection via Databricks Ve...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79794	HPE: Authenticated SQL Injection Vulnerability in ClearPa...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79536	CVE-2026-79536: bytebase dbhub v1.2.0 was discovere...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-72510	Toptech TMS7 and TopHAT SQL Injection	Critical / 9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-72507	Toptech TMS7 and TopHAT SQL Injection	Critical / 9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-68068	Toptech TMS7 and TopHAT SQL Injection	Critical / 9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-68954	Toptech TMS7 and TopHAT SQL Injection	Critical / 9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63713	Toptech TMS7 and TopHAT SQL Injection	Critical / 9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100683	Budibase before 3.45.0 SQL Injection via column-rename ...	High / 8.9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-104462	YesWiki before 4.6.7 SQL Injection via nuagetag tags para...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104457	YesWiki before 4.6.7 SQL Injection via filtertags filterN par...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-55239	Tianji: SQL Injection via unsanitized timezone parameter i...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2024-58393	i-Netsolution Readymade Unilevel Ecommerce MLM SQL ...	High / 8.8	VULNCHECK KEV	✓ Blocked
CVE-2026-70266	Microsoft Office SharePoint Elevation of Privilege Vulnera...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88075	Configuration Manager Elevation of Privilege Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89113	SQL Injection vulnerability in SAP Commerce Cloud (OOT...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86595	SQLi in Iron Mountain's enVision	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2022-51021	NotificationX WordPress Plugin < 2.3.12 Unauthenticated ...	High / 8.8	VULNCHECK KEV	✓ Blocked
CVE-2022-51023	PHPOK < 5.4.081 SQL Injection via api.php sort Parameter	High / 8.8	VULNCHECK KEV	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-107375	JHipster: SQL Injection in the Parameter of JHipster-Gene...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-71434	Weaver E-cology < 10.76 Unauthenticated SQL Injection v...	High / 8.8	VULNCHECK KEV	✓ Blocked
CVE-2026-13695	SQL Injection in the Integratec Application	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18443	Smart Manager <= 8.97.0 - Authenticated (Subscriber+) S...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-55681	WeGIA: SQL Injection in html/matPat/restaurar_produto_d...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-80298	SQL Injection in HAVELSAN's Sef - AI Chatbot Platform	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116207	YesWiki 4.6.0 before 4.7.0 SQL Injection via Bazar Entries ...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114621	baserCMS: SQL injection in the admin panel and admin API	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2019-25778	SeaCMS 8.7 SQL Injection via comment/api/index.php rlis...	High / 8.8	VULNCHECK KEV	✓ Blocked
CVE-2015-20128	FooSun DotNetCMS 1.0 / 2.0 SQL Injection via City_ajax.a...	High / 8.8	VULNCHECK KEV	✓ Blocked
CVE-2026-76477	Cisco Unified Communications Products Hardening Relea...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107082	CVE-2026-107082: Slims (Senayan Library Management ...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-108087	Apache Cocoon: SQL Injection	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116211	YesWiki 4.5.0 before 4.7.0 SQL Injection via date_maj_fich...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103946	SQL Injection	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115332	Lotus through 0.10.2 SQL Injection via Subscription Filter ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115330	Lotus through 0.10.2 SQL Injection via Custom SQL Billabl...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104142	DataEase: Stored SQL Injection in group-field binning bou...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63314	SQL Injection in WebCTI	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42093	Redash: SQL Injection via Query Results parameterized q...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-104143	DataEase: Stored SQL Injection via dateFormat field templ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104460	YesWiki before 4.6.7 Unauthenticated Blind SQL Injection ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104141	DataEase: SQL Injection in datasource metadata identifiers	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89196	CVE-2026-89196: A vulnerability has been identified in R...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111686	IceCMS through 4.1.5 SQL Injection via /WebArticle/findar...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55823	Frappe: Possibility of SQL injection in reportview	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63154	Omnispace Agora Project < 26.10.0 SQL Identifier Injectio...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82039	UTMStack < 11.2.16 SQL Injection via searchGroupsByFilter	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113406	YS-infoware | BA-Workflow - SQL Injection	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112238	SQL Injection in extension "File manager" (ameos_fileman...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113407	YS-infoware | BA-Workflow - SQL Injection	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113405	YS-infoware | BA-Workflow - SQL Injection	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111685	IceCMS through 4.1.5 SQL Injection via /WebResource/fin...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115328	JSON-SCADA before 0.65-alpha SQL Injection via OPC Hi...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115331	Lotus through 0.10.2 SQL Injection via Metric Property Na...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100644	SiYuan before v3.8.4 SQL Injection via dailyNoteSavePath	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109608	Frappe ERPNext before 15.121.0 SQL Injection via Unvalid...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89197	CVE-2026-89197: A vulnerability has been identified in R...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63316	SQL Injection in Payload CMS	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89198	CVE-2026-89198: A vulnerability has been identified in R...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-105856	Payload: SQL injection in SQLite/Postgres	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81420	Tcard WP <= 1.8.0 - Unauthenticated SQLi via group_id Pa...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89297	Loja Automática <= 1.0.0 - Unauthenticated SQLi via 'id' P...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89287	ASPL Product Quotation <= 1.1.0 - Unauthenticated SQLi v...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89214	WpCues Basic Quiz <= 1.6.5 - Unauthenticated SQLi via Q...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89299	WP Verify API <= 1.0.0 - Unauthenticated SQLi via 'verify' ...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89302	Post Voting System <= 1.0 - Unauthenticated SQLi via 'id' ...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93484	CVE-2026-93484: Znuny through 7.3.6 constructs a ticke...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112306	NocoBase plugin-collection-sql through 2.2.28 SQL Injec...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92997	Click n Chat < 1.1.3 - Unauthenticated SQLi via 'datacolum...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92998	Click n Chat 1.0.4 - 1.1.2 - Unauthenticated SQLi via 'sort_...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89288	Fast Courier 5.0.0 - 5.2.3 - Unauthenticated SQLi via 'wp_...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103766	ClipBucket v5 through 5.5.3-#197 SQL Injection via ads_m...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103307	Walletdoc Payment Gateway for WooCommerce < 1.8.5 - ...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63165	Omnispace Agora Project < 26.10.0 SQL Injection via sort...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89236	SaveTo Wishlist Lite < 1.1.5 - Unauthenticated SQLi via 'so...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81932	Multiple vulnerabilities affect the Sniffer component as pa...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89195	Site Setup Wizard <= 1.5.8 - Unauthenticated SQLi via ss...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89213	Llavero.io <= 0.1.4 - Unauthenticated Blind SQLi via 'cill_lo...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89234	WP-Partner <= 1.2.1 - Unauthenticated SQLi via 'id' Param...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-89232	RecordBrowser <= 1.1.7 - Unauthenticated SQLi via 'recor...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89285	Datalist it <= 0.0.3 - Unauthenticated SQLi via dli_fronted_...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103695	Mobile Builder <= 1.4.2 - Unauthenticated SQLi via 'vendo...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87781	LTL Freight Quotes – Old Dominion Edition 4.2.11 - 4.2.18 - ...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88930	Social Web Suite <= 4.1.12 - Unauthenticated Blind SQLi vi...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111634	Helical Insight through 7.0.0 SQL Injection via /executeDat...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63152	Omnispace Agora Project < 26.10.0 Second-Order SQL Inj...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89296	Pro Like Button < 2.0 - Unauthenticated SQLi via 'postid' ...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110895	WordPress Support Genix plugin <= 1.4.54 - SQL Injectio...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39747	WordPress Woffice theme <= 5.4.35 - SQL Injection vuln...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105067	WordPress Modern Events Calendar Lite plugin < 7.37.0 - ...	High / 8.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-94115	WordPress Easy Pricing Tables plugin <= 4.1.2 - SQL Injec...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97287	WordPress Event Tickets plugin <= 5.29.5 - SQL Injection...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97293	WordPress Media LIbrary Assistant plugin <= 3.41 - SQL I...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111399	WordPress MapSVG plugin <= 8.16.1 - SQL Injection vulne...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94177	WordPress GamiPress plugin <= 8.0.2 - SQL Injection vul...	High / 8.5	VULNCHECK KEV	✓ Blocked
CVE-2026-102379	WordPress BuildKit – Product Builder for WooCommerce ...	High / 8.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-103338	WordPress Unlimited Elements For Elementor (Free Widg...	High / 8.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-109901	WordPress CP Multi View Event Calendar plugin <= 1.4.41...	High / 8.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-112837	WordPress GamiPress plugin <= 8.0.7 - SQL Injection vul...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-105317	WordPress Paid Member Subscriptions plugin <= 3.1.1 - S...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42416	WordPress UDesign Core plugin <= 4.15.0 - SQL Injection ...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94663	WordPress ProfileGrid plugin <= 6.0.0.2 - SQL Injection v...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39771	WordPress Buddyboss Platform plugin <= 3.1.0 - SQL Inje...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-25434	WordPress WP2LEADS plugin <= 3.5.7 - SQL Injection vul...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42414	WordPress ListingPro plugin <= 2.9.12 - SQL Injection vul...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104389	WordPress Sirv plugin <= 8.2.5 - SQL Injection vulnerability	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42712	WordPress Qode Tours plugin <= 3.1.3.2 - SQL Injection v...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42633	WordPress Events Manager plugin <= 7.4.6 - SQL Injectio...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112822	WordPress Workreap Core plugin < 3.4.4 - SQL Injection ...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95607	WordPress WPLMS theme <= 4.973 - SQL Injection vulne...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95599	WordPress Taskbuilder plugin <= 6.0.5 - SQL Injection vul...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95610	WordPress UpSolution Core plugin <= 9.3 - SQL Injection ...	High / 8.5	VULNCHECK KEV	✓ Blocked
CVE-2026-103066	WordPress WP BASE Booking plugin <= 6.4.0 - SQL Injec...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96329	WordPress tagDiv Opt-In Builder plugin <= 1.7.6 - SQL Inje...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62117	WordPress Barcode Scanner with Inventory & Order Mana...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89200	CVE-2026-89200: A vulnerability has been identified in R...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114081	Trigger.dev before 4.5.6 Cross-Tenant SQL Injection via T...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111389	Frappe HRMS 14.0.0 before 14.38.2 SQL Injection via Miss...	High / 8.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-114084	Trigger.dev before 4.5.6 SQL Injection via tags in Realtime...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-94131	Joomla Extension - acymailing.com - Unauthenticated ar...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97162	Joomla Extension - lomart.fr - Various SQL injection vect...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107829	Jivejdon through 5.0 Unsalted MD5 Password Storage via...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95105	Cloak AES-CTR cipher lacks ciphertext authentication, all...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93621	WordPress WP Data Access plugin <= 5.5.84 - SQL Injecti...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84209	IBM Guardium Data Protection is affected by multiple vuln...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62251	Homer: Authenticated SQL Injection via Unvalidated rawq...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62376	Vikunja: Plaintext storage of password-reset/email-confir...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107384	MariaDB Connector/Node.js: SQL injection through object...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-45871	CVE-2025-45871: LogicalDOC Enterprise up to and for 9....	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93953	Backuply <= 1.5.8 - Authenticated (Subscriber+) Second-...	High / 8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70049	Microsoft Configuration Manager Elevation of Privilege V...	High / 8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-46773	CVE-2025-46773: An Improper Neutralization of Special ...	High / 7.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-4889	SQL Injection (SQLi) in eLoanApp Platform by RDL Techn...	High / 7.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-57739	CVE-2025-57739: An improper neutralization of special e...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
GHSA-9Q4R-4842-93VW	Trigger.dev: Cross-tenant SQL injection in the TSQL quer...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86047	MariaDB: Insufficient quoting in mariadb-dump and SHO...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89201	CVE-2026-89201: A vulnerability has been identified in R...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96534	Modern Events Calendar (Lite & Pro) < 7.37.0 - Subscriber...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102499	Modern Events Calendar (Lite & Pro) < 7.37.0 - Subscriber...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-94082	WordPress Quiz Cat plugin <= 3.1.1 - SQL Injection vulner...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62085	WordPress WP Activity Log plugin <= 5.6.6 - SQL Injectio...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96827	WordPress Admin Notices Manager plugin <= 1.6.0 - SQL ...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96346	WordPress WP ERP plugin <= 1.17.9 - SQL Injection vulner...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-53574	EspoCRM: Blind SQL injection via streamAttachments wh...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62060	WordPress Captivate Sync plugin <= 3.3.2 - SQL Injection...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62059	WordPress Ultimate Member plugin <= 2.13.1 - SQL Injecti...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62097	WordPress Business Directory plugin <= 6.4.27 - SQL Inje...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96345	WordPress Estatik plugin <= 4.3.5 - SQL Injection vulnera...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96828	WordPress Category Discount Woocommerce plugin <= ...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-45440	WordPress WP Ultimate CSV Importer plugin <= 9.2 - SQ...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104408	WordPress Groundhogg plugin <= 4.8.3 - SQL Injection v...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108179	WordPress WOLF plugin <= 1.1.1 - SQL Injection vulnerabil...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42722	WordPress Frontend Admin by DynamiApps plugin <= 3.2...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109687	WordPress Link Whisper Free plugin <= 0.9.7 - SQL Inject...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42717	WordPress Leyka plugin <= 3.32.3 - SQL Injection vulnera...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42713	WordPress Post title marquee scroll plugin <= 9.9 - SQL I...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42721	WordPress affiliate-toolkit plugin <= 3.9.1 - SQL Injection ...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42714	WordPress Pix por Piggly (para Woocommerce) plugin <=...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42708	WordPress WP Post Author plugin <= 4.0.0 - SQL Injectio...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-42710	WordPress Slider by 10Web plugin <= 1.2.63 - SQL Injecti...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105076	WordPress Vitepos plugin <= 3.6.1 - SQL Injection vulnera...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42720	WordPress Dynamic User Directory plugin <= 2.4 - SQL I...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-6806	Motors <= 1.4.109 - Unauthenticated Blind SQL Injection v...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93300	EventON - Subscriber <= 1.4.5 - Unauthenticated SQL Inj...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102796	Unauthenticated SQL injection in UserPageViewTracker vi...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2015-20122	Seeyon A6 OA Unauthenticated SQL Injection via downlo...	High / 7.5	VULNCHECK KEV	✓ Blocked
CVE-2026-32580	WordPress WooCommerce Lottery plugin <= 2.2.9 - SQL ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15090	Link Library <= 7.9.2 - Unauthenticated SQL Injection via '...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96267	WP Visitor Statistics (Real Time Traffic) <= 8.7 - Unauthen...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81809	Paytm Payment Gateway < 2.8.9 - Unauthenticated SQLi ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102251	Abandoned Cart Pro for WooCommerce <= 10.8.0 - Unaut...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-1907	SQL Injection in Clustering Communication (Hybrid Mode)	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100847	AzuraCast before 0.23.8 DQL Injection via sortOrder	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95808	Form Maker by 10Web <= 1.15.48 - Unauthenticated SQL I...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103913	GeoDirectory <= 2.8.186 - Unauthenticated SQL Injection ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92766	Vitepos <= 3.5.1 - Unauthenticated SQL Injection via 'src_...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78193	JTL-Connector for WooCommerce <= 2.4.3 - Unauthenti...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96662	Appointment Booking Plugin <= 5.7.2 - Unauthenticated S...	High / 7.5	VULNCHECK KEV	✓ Blocked
CVE-2026-96661	Gmedia Photo Gallery <= 1.25.1 - Unauthenticated SQL Inj...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-107385	MariaDB Connector/Node.js: SQL injection in the text prot...	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102909	SourceCodester Online Reviewer Management System bt...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102491	mahonelau kykms SqlInjectionUtil QueryGenerator.java Q...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102616	risesoft-y9 WorkFlow-Engine OAuth2 Resource Filter Cu...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102908	SourceCodester Online Reviewer Management System q...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103230	AdithyaYelloju Restaurant-Management-System Order Pl...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103229	AdithyaYelloju Restaurant-Management-System Unauthe...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100315	mathurvishal CloudClassroom-PHP-Project mydetailsfac...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103232	AdithyaYelloju Restaurant-Management-System table_bo...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89076	MOVEit Transfer SQL injection in custom reporting	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-41510	Coraza: Silent argument drop at ArgumentLimit allows by...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75786	SQL Injection in Grafana Integration Endpoint (query.php)	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102098	Kiteworks Core SQL Injection	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104456	YesWiki before 4.6.7 Second-Order SQL Injection via ACL...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105107	Koha SQL injection in reports/cat_issues_top.pl via the Cri...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111619	FilePress through 3.0.1 SQL Injection via asc Parameter in ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102109	Kiteworks Secure Data Forms SQL injection	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112017	JeecgBoot before 3.9.5 SQL Injection via SqlInjectionUtil ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112064	SQL Injection in extension "sgalinski Cookie Consent" (sg...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108100	HortusFox before 6.2 SQL Injection via /api/locations/list i...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-108125	WordPress Post Author Authenticated SQLi	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103248	n8n before 1.123.80, 2.39.6, and 2.40.1 PostgREST Filter In...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102158	Security Advisory 0190	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82045	UTMStack < 11.2.16 JPQL Injection via searchPropertyVal...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85215	SQL Injection in GG Soft's Paperwork	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110609	Dromara Skyeye through commit 65d3ddcede70 SQL Inje...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110614	Yiuman citrus through 0.15.0 ORDER BY SQL Injection via ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111718	AipexBase through commit 690adb9 SQL Injection via /ap...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55386	InvoiceShelf ORDER BY SQL injection through orderByField	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-26244	SQLi#1 SQL Injection in class_videos.php _getFilters	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-26245	SQLi#2 SQL Injection in class_videos.php getSmartVideo...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111669	ZR.Admin.NET through 3.8.2 SQL Injection via PagerInfo....	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111700	WebVella ERP through 1.8.8 SQL Injection via EQL Query ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32581	WordPress Mooberry Book Manager plugin 4.16.2 - SQL I...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109639	Frappe ERPNext before 15.102.0 SQL Injection via Unvalid...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109646	Frappe ERPNext before 15.106.0 SQL Injection via Missing...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109674	Frappe ERPNext before 16.6.0 SQL Injection via Missing In...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109638	Frappe ERPNext before 15.110.0 SQL Injection via Missing ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110083	Adobe Experience Manager | Improper Neutralization of S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109649	Frappe ERPNext before 15.102.0 SQL Injection via Unvalid...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-109648	Frappe ERPNext before 15.106.0 SQL Injection via Missing...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109647	Frappe ERPNext before 15.106.0 SQL Injection via Missing...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109663	Frappe ERPNext before 15.113.0 SQL Injection via Unvalid...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109631	Frappe ERPNext before 15.119.1 SQL Injection via Missing ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109353	LibreNMS before 26.9.0 SQL Injection via notification_id i...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109609	Frappe ERPNext before 15.119.1 SQL Injection via Missing I...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109626	Frappe ERPNext before 16.34.2 SQL Injection via Multiple ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109170	LogicalDOC Community Edition through 9.3 HQL Injection...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109169	LogicalDOC Community Edition through 9.3 SQL Injection...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105412	SQL Injection vulnerability affecting Tuleap Enterprise Edi...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109080	SQL injection in Night Shift bulk license plate search allow...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114065	Trigger.dev before 4.7.3 Tenant Filtering Bypass via Quer...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-53629	GLPI: SQL injection in history tab	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101091	SiYuan before v3.8.4 SQL Injection via Block Query Embed	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114664	Frappe before 16.33.0 Blind SQL Injection via get_events	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102569	ClipBucket v5 through 5.5.3-#197 SQL Injection via videoi...	High / 7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110840	n8n before 2.41.4 and 2.42.1 SQL Injection via Microsoft S...	High / 7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103253	n8n before 1.123.80, 2.39.6, and 2.40.1 SQL Injection via O...	High / 7	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-102570	ClipBucket v5 through 5.5.3-#197 SQL Injection via langu...	High / 7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101012	mathurvishal CloudClassroom-PHP-Project makeresult.p...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-114577	oretnom23 php-travel-agency-system Insertion insert.ph...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100874	mathurvishal CloudClassroom-PHP-Project addnewstude...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100875	mathurvishal CloudClassroom-PHP-Project updatedetails...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100739	mathurvishal CloudClassroom-PHP-Project viewresult.ph...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100314	mathurvishal CloudClassroom-PHP-Project updatedetails...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114254	oretnom23 file-management-system-php admin_class.p...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114255	oretnom23 file-management-system-php User Account ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114256	oretnom23 file-management-system-php Folder Manage...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114257	oretnom23 file-management-system-php File Download ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114258	oretnom23 file-management-system-php File Manageme...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114263	ProjectWorlds Advanced Library Management System ind...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116170	SiYuan before v3.8.7 SQL Injection via History Search op ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116060	SourceCodester Performance Indicator System adddeale...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114242	dhikshitha29 Insurance-Management-System editPlan.p...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114243	dhikshitha29 Insurance-Management-System EditPolicy...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114099	Coraza 3.0.0 before 3.8.1 WAF Bypass via JSON Key Colli...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105232	kishor-23 food-waste-management-system Registration ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114441	oretnom23 php-travel-agency-system update.php sql inj...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114440	oretnom23 php-travel-agency-system delete.php sql inje...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101013	mathurvishal CloudClassroom-PHP-Project updateresult...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-115999	mansi-k Restaurant_IMS lsmodal.php mysqli_connect sql ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105169	kishor-23 food-waste-management-system Take Order d...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105172	itsourcecode Online Admission System login1.php sql inje...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105175	SourceCodester Drug Recommendation System Student ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105230	kishor-23 food-waste-management-system deliverymyor...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105185	itsourcecode Online Admission System examinee.php sql...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105184	itsourcecode Online Admission System creteria.php sql in...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105183	itsourcecode Online Admission System confirm.php sql i...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105182	SourceCodester Online Reviewer Management System bt...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105229	kishor-23 food-waste-management-system User Registr...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109522	girishsaraf Online-Appointment-Booking-System Admin ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109521	girishsaraf Online-Appointment-Booking-System change...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105253	itsourcecode Online Admission System Project login1.php...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105247	SourceCodester Online Reviewer Management System bt...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105158	RainyGao DocSys Database Management BaseController.j...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105149	mooSocial all-products sql injection	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105166	kishor-23 food-waste-management-system Food Donati...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108956	code-projects Online Reviewer System User Update btn_f...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108964	SourceCodester Performance Indicator System addprodu...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108965	SourceCodester Performance Indicator System edit_quan...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-108966	SourceCodester Performance Indicator System product.p...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108968	SourceCodester Performance Indicator System sales_hist...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108967	SourceCodester Performance Indicator System edit_cred...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108970	itsmeravitejak Online-Examination-System Registration F...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109115	AdithyaYelloju Restaurant-Management-System Passwor...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105167	kishor-23 food-waste-management-system donate.php s...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108826	Zen Cart PayPal IPN paypaldp.php zen_db_perform sql inj...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109634	Frappe ERPNext before 15.121.0 SQL Injection via Unvalid...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108900	Exponent CMS XML-RPC xmlrpc.php userLogin sql injecti...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109523	girishsaraf Online-Appointment-Booking-System AJAX E...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109620	SourceCodester Online Reviewer System index.php prep...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109606	SourceCodester Art Gallery Management System Accoun...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109607	SourceCodester Online Exam System Login Endpoint logi...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105231	kishor-23 food-waste-management-system Admin Regis...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105246	SourceCodester Online Reviewer Management System bt...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105807	SourceCodester Simple Student Information System sear...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111871	itsmeravitejak Online-Examination-System subjectsdb.ph...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103231	AdithyaYelloju Restaurant-Management-System Order Ca...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116049	krupalshah EmployeeRecruitmentSystem Registration Wi...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111873	itsmeravitejak Online-Examination-System AJAX Endpoin...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-111872	itsmeravitejak Online-Examination-System database.php ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105918	Kusalkasilva Learning-Management-System Login Endpo...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116048	krupalshah EmployeeRecruitmentSystem Registration reg...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105920	Kusalkasilva Learning-Management-System Student Regi...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105919	Kusalkasilva Learning-Management-System Administrato...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-71428	Jivejdon through 5.0 SQL Injection via username in userLi...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116062	SourceCodester Performance Indicator System save_pro...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116050	krupalshah Employee Recruitment System Registration re...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111990	kishan0725 Hospital Management System Appointment C...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105776	bhagya3929 Employee-Movement-Tracking-and-Monitor...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105468	girishsaraf Online-Appointment-Booking-System Login m...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112151	vraj404 Criminal Management System Submission Form ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112152	vraj404 Criminal-Management-System Search searchOff....	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112252	Wuxi Wubang Security Software Wubang Five-in-One Saf...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112153	vraj404 Criminal-Management-System Officer Registrati...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113381	Osclass Item Model Item.php findUserItems sql injection	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102910	SourceCodester Online Reviewer Management System e...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105385	onetwothreeneth HospitalManagementSystem transactio...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105386	onetwothreeneth HospitalManagementSystem print.php ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112141	satya-vinay Events-Management-System Registration-Ed...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked

INDUSFACE™ ©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-112139	subhajitkhan online-clinic-management-system Administ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105383	onetwothreeneth HospitalManagementSystem controller....	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105384	UNION HospitalManagementSystem patient_info.php sql i...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102913	SourceCodester Car Driving School Management System...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116061	SourceCodester Performance Indicator System edit_deal...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112150	vraj404 Criminal-Management-System search.php sql inj...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112142	satya-vinay Events-Management-System Registration-D...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105387	girishsaraf Online-Appointment-Booking-System Patient ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110668	cemtan sar2html sar2html.py index sql injection	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111866	nemoTyrant manong func.php arr2sql sql injection	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104609	onetwothreeneth HospitalManagementSystem edit_acco...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110670	cemtan sar2html Archive Processing sar2html.py update...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108571	Xinhu Rainrock RockOA Openkqj Action openkqjAction.p...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105469	girishsaraf Online-Appointment-Booking-System AJAX E...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105471	girishsaraf Online-Appointment-Booking-System Registr...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104123	SourceCodester Online Reviewer Management System bt...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105470	girishsaraf Online-Appointment-Booking-System Doctor ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108807	krupalshah EmployeeRecruitmentSystem Registration ad...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108806	krupalshah EmployeeRecruitmentSystem Forgot Passwor...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108805	krupalshah EmployeeRecruitmentSystem Login loginproc...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-108799	jackq XCMS Password Recovery Mail Endpoint PublicCon...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110179	affiliate-toolkit < 3.8.9 - Editor+ SQL Injection via orderby ...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103696	Mobile Builder <= 1.4.2 - Unauthenticated SQLi via 'delive...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110651	Swift Performance Lite < 2.3.7.4 - Author+ SQLi via Image...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89237	Bluff Post <= 1.1.1 - Unauthenticated SQLi via 'table_name'...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93000	SPS-Suite <= 1.4.0 - Unauthenticated Time-Based SQLi vi...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91833	WX Subscribe <= 1.2.1 - Unauthenticated SQLi via 'attach'...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91074	BSK PDF Manager <= 3.8.1 - Contributor+ SQLi via tags_s...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85568	Unlimited Elements For Elementor 1.5.139 - 2.0.20 - Unaut...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106097	Code Snippets < 3.10.0 - Admin+ SQLi in Migration Import...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89235	Testimonials by BestWebSoft 1.0.5 - 1.0.8 - Unauthenticat...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104953	MPG < 4.2.3 - Editor+ SQLi via Project Import	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104667	Animated Number Counters < 3.1 - Editor+ Second-Order ...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104122	Ukr-To-Lat <= 1.3.5 - Contributor+ SQLi via Term Name	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84097	WP Review Slider Pro < 12.7.12 - Subscriber+ SQLi via Stor...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88397	CVE-2026-88397: ApiAdmin v.5.0 and before is vulnerabl...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101926	Hyyan WooCommerce Polylang Integration <= 1.5.0 - Aut...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55796	Frappe HR: SQL Injection in HRMS Salary Payments via E...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96653	WP Directory Kit <= 1.5.9 - Authenticated (Subscriber+) S...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12951	MultiVendorX <= 5.0.18 - Authenticated (Store Manager+)...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-107712	WP Booking System <= 2.1.0.1 - Authenticated (Subscribe...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-16596	WP Directory Kit <= 1.5.4 - Authenticated (Custom+) SQL ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107803	ProcessMaker has SQL injection in the tasks endpoint thr...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56097	Rubygem-katello: sql injection in registry proxy via labels	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102456	DigiWin | EasyFlow .NET - SQL Injection	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76270	Structured Query Language (SQL) Injection in the SPL2 M...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89304	Paymendo Bank Transfer <= 1.1 - Unauthenticated Blind S...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97634	Event Tickets and Registration <= 5.29.5 - Authenticated ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89305	Paymendo Bank Transfer <= 1.1 - Subscriber+ SQLi via 'or...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55871	GYM One: Improper Neutralization of Special Elements us...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109414	Vitepos <= 3.6.1 - Authenticated (Vendor+) SQL Injection ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94539	SupportCandy <= 3.5.3 - Authenticated (Custom+) SQL I...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95865	Beaver Builder Page Builder <= 2.11.0.5 - Authenticated (...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111106	Mail Mint <= 1.31.4 - Authenticated (Custom+) SQL Injecti...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-23705	CVE-2026-23705: An Improper Neutralization of Special ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-23707	CVE-2026-23707: An Improper Neutralization of Special ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-71298	Maestro: sql identifier injection via properties.* search filt...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89303	Post Voting System <= 1.0 - Subscriber+ SQLi via 'row' Pa...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103114	OS4ED openSIS-Classic Assignment Management Endpo...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86843	Apache Airflow Teradata provider: SQL injection via unvali...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-100312	mathurvishal CloudClassroom-PHP-Project updateguest....	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92923	Unlimited Elements For Elementor 1.5.142 - 2.0.20 - Subsc...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103116	OS4ED openSIS-Classic Student List Search Endpoint Ge...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94298	BuildKit < 1.0.29 - Contributor+ Stored SQLi via list_conte...	Medium / 6.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-5048	CVE-2026-5048: In Brocade SANnav before 3.0.0a, an S...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94348	CVE-2026-94348: Dell PowerScale InsightIQ, versions 5....	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111390	Erupt through 2.3.0 HQL Injection via linkTreeVal in Data T...	Medium / 6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113608	Configurable Reports block for Moodle before 5.3.1 SQL In...	Medium / 6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59508	Interuse i-Bos CWE-89: Improper Neutralization of Speci...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-23706	CVE-2026-23706: An Improper Neutralization of Special ...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104774	Coraza: jsDecode Off-by-One in Octal Escape Handling E...	Medium / 5.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102578	Moodle: sql injection in question bank web service	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-46531	Cacti: Authenticated Stored 2nd-Order SQL Injection in a...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-16830	Security vulnerabilities have been found in IBM Verify Ide...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100899	DevaslanPHP project-management Timesheet Dashboard...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114250	itsourcecode Sales-and-Inventory-System cust_edit.php ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114252	itsourcecode Sales-and-Inventory-System cust_searchfr...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100894	mathurvishal CloudClassroom-PHP-Project updateguest....	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100887	amirsanni Mini-Inventory-and-Sales-Management-Syste...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100898	DevaslanPHP project-management Timesheet Dashboard...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-101105	code-projects Matrimonial System Profile Creation Endpo...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114384	itsourcecode Online Cake Ordering System transactionsa...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55444	Goobi viewer: Solr query injection via the legacy RSS serv...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55465	Goobi viewer: Solr injection via unvalidated region param...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114251	itsourcecode Sales-and-Inventory-System cust_del.php ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114378	itsourcecode Online Cake Ordering System deleteproduc...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114265	ProjectWorlds Advanced Library Management System Se...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114381	itsourcecode Online Cake Ordering System orderdetail.p...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114266	ProjectWorlds Advanced Library Management System pr...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114039	projectworlds Advanced Library Management System rep...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115997	pig-mesh pig SqlFilterArgumentResolver.java orderItem.g...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103115	OS4ED openSIS-Classic Student Search CustomFieldsFn...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113740	itsourcecode Online Cake Ordering System deletecustom...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116055	SourceCodester Performance Indicator System deletepro...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114380	itsourcecode Online Cake Ordering System inserttrans.ph...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108928	itsourcecode Online Admission System sum.php sql injec...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108927	itsourcecode Baptism Information Management System p...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105186	itsourcecode Online Admission System new.php sql injec...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105181	itsourcecode Online Admission System register1.php sql i...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105187	itsourcecode Online Admission System key.php sql injecti...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-108824	DataEase Utils.java Utils.buildCalcField sql injection	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104724	FireBox <= 3.1.13 - Authenticated (Author+) SQL Injection ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112088	Dav-ee dairy-management-system add.php mysqli_quer...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108776	Apache Kylin: tables/names SparkSQL injection	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112090	Dav-ee dairy-management-system pay.php mysqli_real_e...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111992	itsmeravitejak Online-Examination-System Exam exam.ph...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103543	itsourcecode Leave Management System controller.php s...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108779	erzhongxmu JEEWMS WmSttInGoodsController.java Wm...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108781	erzhongxmu JEEWMS PDA WmToMoveGoodsController.j...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104614	CodeAstro Simple Pharmacy Management System delete....	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104613	CodeAstro Simple Pharmacy Management System view.p...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108794	ZKTeco BioTime Database Migration Functionality db_mig...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108782	erzhongxmu JEEWMS Autocomplete CommonServiceIm...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108775	erzhongxmu JEEWMS Search Endpoint WvNoticeControl...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105168	kishor-23 food-waste-management-system Order Assign...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108959	itsourcecode Online Cake Ordering System addtransacde...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105254	itsourcecode Online Admission System schoolyear.php s...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108926	itsourcecode Baptism Information Management System e...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108814	SEMCMS SEMCMS_Banner.php sql injection	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108821	Tencent WeKnora SQL Validator inject.go validateSubque...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-108813	SEMCMS SEMCMS_Download.php sql injection	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108773	erzhongxmu JEEWMS WmOmNoticeHController.java doc...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105388	feelec-yishu feelcrm-os Member Endpoint MemberContr...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105472	girishsaraf Online-Appointment-Booking-System Bookin...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108541	highwarden Super Store Finder index.php sql injection	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108569	Furion .NET Framework StringRenderExtensions.cs Strin...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108774	erzhongxmu JEEWMS MdBinController.java getbinallagv ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108684	erzhongxmu Jeewms Autocomplete Data JeecgFormDe...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104606	itsourcecode Online Admission System Project confirm.p...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104053	itsourcecode Pet Shop Management System admin_reser...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104052	itsourcecode Pet Shop Management System admin_rejec...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103690	itsourcecode Leave Management System controller.php s...	Medium / 5.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-104625	CodeAstro Simple Loan Management System index.php s...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105287	feelec-yishu feelcrm-os getMemberByGroups Endpoint ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112087	itsourcecode Online Cake Ordering System confirm.php s...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105957	SourceCodester Performance Indicator System view_pro...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105921	Kusalkasilva Learning-Management-System search_class...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108778	erzhongxmu JEEWMS Inbound Quality Check Pda WmIn...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108777	erzhongxmu JEEWMS WvGiController.java WvGiControll...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105146	Comsenz Discuz! Admin Medal Moderation mod.php mod...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-105176	SourceCodester Drug Recommendation System edit_clas...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103113	OS4ED openSIS-Classic General Information Tab Student...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101011	aaPanel BaoTa Domain domainMod.py get_domain_status...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101018	dayrui XunruiCMS Group Editing Home.php group_all_edi...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101010	aaPanel BaoTa data.py getData sql injection	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114264	ProjectWorlds Advanced Library Management System edi...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108829	Zen Cart Module Configuration modules.php sql injection	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105177	SourceCodester Drug Recommendation System Drug Cre...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105178	SourceCodester Drug Recommendation System Sympto...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112032	aircheng-org iWebShop-5 util.php search sql injection	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112089	Dav-ee dairy-management-system delete.php mysqli_qu...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15399	Animated Number Counters <= 3.0 - Authenticated (Edito...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107752	Welcart e-Commerce <= 2.12.4 - Authenticated (Editor+) ...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108124	WordPress Post Author Authenticated SQLi	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103518	FluentCart A New Era of eCommerce <= 1.7.0 - Authentic...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104023	Smart Popup by Supsystic <= 1.13.2 - Authenticated (Adm...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62362	PeerBanHelper: SQL injection via ${field} interpolation in ...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111178	WP Booking System <= 2.1.0.1 - Authenticated (Administr...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76452	Cisco Smart Software Manager On-Prem SQL Injection V...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102912	SourceCodester Online Leave Management System page ...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 553 blocked · avg CVSS 7.4 · 1 CISA KEV (continued)				
CVE-2026-103117	OS4ED openSIS-Classic Save Data DatabaseInc.php db_p...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104753	Rank Math SEO < 1.0.280 - Admin+ SQLi via 'per_page' P...	Medium / 4.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101046	Fleet before 4.89.0 SQL Injection via ORDER BY Activity E...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108828	Zen Cart Admin Panel configuration.php eval sql injection	Low / 2.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-51936	CVE-2026-51936: Zetetic SQLCipher before 4.15.0 allows...	Low / 2.1	NO KNOWN EXPLOIT	✓ Blocked
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV				
CVE-2026-55393	Local File Inclusion in Teledyne FLIR Robots running Awar...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-71379	Toptech TMS7 and TopHAT Files or Directories Accessibl...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97163	Joomla Extension - lomart.fr - Unauthenticated remote co...	Critical / 10	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-105037	EnergizeLab Station Middleware Authenticated Path Trav...	Critical / 9.9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-106042	CVE-2026-106042: An External Control of File Name or P...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76531	Files or Directories Accessible to External Parties in Splun...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113672	Argo CD: A Jsonnet import can read files from the repo-s...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85526	Path traversal via Btrfs optimized-backup subvolumes[].p...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115931	Arbitrary file read and backend crash through unrestricte...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104286	CVE-2026-104286: An improper limitation of a pathname ...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2026-105892	WordPress rtMedia for WordPress, BuddyPress and bbPr...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75875	Multiple vulnerabilities affect the Sniffer component as pa...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79805	HPE: Authenticated Path Traversal Vulnerability Leads to ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-62032	WordPress DirectoryPress plugin <= 3.6.27 - Local File In...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-51880	CVE-2026-51880: deeptutor 1.4.0 contains a path travers...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76519	Cisco Secure Email Gateway Arbitrary File Write Vulnerabi...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2026-78799	CVE-2026-78799: Directory Traversal vulnerability in Qua...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112832	WordPress Rootblox plugin <= 1.0.6 - Local File Inclusion ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-51884	CVE-2026-51884: The /knowledge_base/upload_temp_d...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82101	DataStage on Cloud Pak for Data Path Traversal	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82110	DataStage on Cloud Pak for Data Path Traversal	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86360	CVE-2026-86360: Dell System Update, versions prior to ...	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115932	Path traversal in post media lets any registered user read ...	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79866	HPE: Unauthenticated Adjacent Path Traversal Vulnerabili...	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57496	NetLicensing MCP Server: REST Path Traversal Bypasses...	Critical / 9.6	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-85185	Path traversal in LXD btrfs storage driver allows arbitrary f...	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100706	kyverno before 1.19.1 Privilege Escalation via Policy apiCall...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106173	CVE-2026-106173: A improper limitation of a pathname to...	Critical / 9.4	VULNCHECK KEV	✓ Blocked
CVE-2026-115375	Incus 7.0.0 before 7.0.2 and 7.1.0 before 7.5.0 Path Travers...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94620	Classroom 50 vulnerable to arbitrary file overwrite on the ...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107935	Gvisor-tap-vsock: gvisor-tap-vsock: unathenticated arbit...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2021-48014	FineReport 9.0 Unauthenticated Path Traversal File Write ...	Critical / 9.3	VULNCHECK KEV	✓ Blocked
CVE-2026-90530	ColdFusion | Improper Limitation of a Pathname to a Restri...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-115812	Relative path traversal during model archive extraction in ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-41753	Path traversal in dynamically created BACnet File Objects	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82824	Path traversal may allow arbitrary files to be viewed, creat...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103928	Metabase: Arbitrary File Read/Write via Unsafe H2 Built-in...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73642	Path Traversal in Dayforce ESS Excelity	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97161	Joomla Extension - lomart.fr - Various path traversal / file ...	Critical / 9.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-115353	Mistune before 3.3.0 Path Traversal via include Directive	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2016-20101	Issuu Panel WordPress Plugin < 1.6.6 File Inclusion via aja...	Critical / 9.2	VULNCHECK KEV	✓ Blocked
CVE-2026-112005	WhoDB 0.104.0 before 0.135.0 Arbitrary File Read/Write vi...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113613	FlexGet before 3.20.7 Path Traversal (Zip Slip) via decom...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104801	PPOM <= 34.0.10 - Unauthenticated Arbitrary File Deletio...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-51875	CVE-2026-51875: In Devika v1.0, the Feature Agent save_...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9827	CVE-2026-9827: A arbitrary file write vulnerability exists i...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87115	VikAppointments Services Booking Calendar <= 1.2.21 - ...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-51882	CVE-2026-51882: The OpenAI-compatible file upload en...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-51859	CVE-2026-51859: bisheng 2.3.0, 2.4.0, and 2.4.0-beta1 is...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-51864	CVE-2026-51864: DB-GPT v0.7.5 and v0.8.0 contains dir...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-51906	CVE-2026-51906: In TaskingAI v0.3.0 in the DALL-E 3 im...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-51862	CVE-2026-51862: DB-GPT 0.8.0 contains directory traver...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15896	Super Forms <= 6.3.316 - Unauthenticated Path Traversal ...	Critical / 9.1	PUBLIC EXPLOIT/POC	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-103648	GitLab: Improper Limitation of a Pathname to a Restricted ...	Critical / 9.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-101894	@xhmikosr/decompress: Path traversal via symlink chain	Critical / 9.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-76454	Cisco Smart Software Manager On-Prem Unauthenticate...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105772	Arbitrary file read and write in Google ADK TypeScript (@...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-51883	CVE-2026-51883: The knowledge base creation and doc...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-8066	CVE-2026-8066: A directory traversal vulnerability in the ...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62679	Lychee: Path traversal in `SecurePathController` allows au...	High / 8.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102424	Joomla Extension - balbooa.com - Unauthenticated path t...	High / 8.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-44415	CVE-2026-44415: Affected systems do not properly restr...	High / 8.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84421	DataStage on Cloud Pak for Data has several vulnerabilities	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55888	XDG Desktop Portal: Arbitrary file access via SaveFiles "fi...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91012	Apache Karaf: Path Traversal in Config Service Allows Ma...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100597	OpenClaw before 2026.7.1 Path Traversal via Filesystem R...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-51873	CVE-2026-51873: Devika v1.0 is vulnerable to Directory T...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2022-51022	YiShaAdmin 3.1 Unauthenticated Path Traversal via Downl...	High / 8.8	VULNCHECK KEV	✓ Blocked
CVE-2026-114140	nbconvert: File write via path traversal in cell output filena...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-53995	MLflow 3.17.1 and prior Path Traversal via Trace ID API	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-105727	Microsoft Dynamics 365 Business Central Elevation of Pri...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110116	Digital-Infrastructure 9.6.5 through 9.6.11 Path Traversal vi...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85634	Wildfly-core: wildfly-core: deployer rbac role privilege es...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-102226	Dynamics Business Central Elevation of Privilege Vulnera...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116067	Paisa before 0.7.8 Path Traversal via Editor and Sheet API	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83784	Windows Encrypting File System (EFS) Elevation of Privil...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103412	Apache Camel Karavan: project file name path traversal w...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2017-20287	Javo Spot WordPress Theme < 3.0.0 Path Traversal via ad...	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2024-58396	YouDataSum CPAS Audit Management System V4 Path Tr...	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2022-51024	Kavita < 0.5.4.1 Unauthenticated Path Traversal via cover-...	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2026-100520	Laranode before 1.2.1 Path Traversal in File Manager Uplo...	High / 8.7	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2021-48017	OrbiTeam BSCW Server < 5.2.5 / 7.4.4 Path Traversal via ...	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2026-100689	GitPython before 3.1.62 Path Traversal via gitmodules path	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2021-48015	JeeWMS Path Traversal via showOrDownByurl.do	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2026-116191	Rclone before 1.75.2 Path Traversal via serve webdav MK...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2021-48011	Servor 1.0.0 through 4.0.2 Unauthenticated Path Traversal...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78355	Path Traversal in SendSupportBundle allows File Deletion ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110690	Cloud Commander 19.20.2 through 19.21.1 Path Traversal ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63162	Omnispace Agora Project < 26.10.0 Path Traversal via tmp...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-53882	Path Traversal in Virtualization Station VM Import	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108070	Improper Access Control Allows Unauthorized Access to ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55224	MineAdmin: Path Traversal via Unsanitized identifier in Pl...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2024-58388	Sharp Multifunction Printers Local File Inclusion via install...	High / 8.7	VULNCHECK KEV	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-100692	Hugo before v0.166.0 Path Traversal via Symlinked Mount...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2021-48013	Weaver E-cology 8.0 Unauthenticated Path Traversal via l...	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2019-25779	WooThemes Diarise 1.5.9 Local File Disclosure via downlo...	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2018-25439	MetInfo CMS < 6.1.1 Unauthenticated Path Traversal via th...	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2018-25438	Intermesh Group-Office < 3.5.5 Path Traversal via compr...	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2016-20104	EyeLock nano NXT 3.05.1193 Path Traversal via logdownl...	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2026-101024	Satel Netco Design Relative path traversal	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2014-125130	CodeArt Google MP3 Audio Player 1.0.11 Arbitrary File Rea...	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2012-20002	TinyMCE Thumbnail Gallery WordPress Plugin < 1.1.0 Path...	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2015-20123	Aspose Doc Exporter WordPress Plugin < 2.0 Path Traver...	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2014-125134	ChurcHope WordPress Theme < 2.2 Path Traversal via do...	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2014-125133	NativeChurch WordPress Theme < 1.6.2 Arbitrary File Do...	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2026-115355	Mistune before 3.3.0 Path Traversal and XSS via Include D...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114063	SvelteKit 2.10.0 before 3.0.0 Path Traversal via vite previe...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114106	HKUDS Vibe-Trading 0.1.0 before 0.1.7 Path Traversal via r...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114110	Astral uv before 0.11.6 Arbitrary File Deletion via Wheel RE...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2016-20103	Cherry Plugin for WordPress < 1.2.7 Path Traversal via do...	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2015-20124	Aspose Importer & Exporter WordPress Plugin < 3.0 Path ...	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2015-20125	Aspose PDF Exporter WordPress Plugin < 2.0 Path Traver...	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2016-20100	Memphis Documents Library WordPress Plugin < 3.1.6 Pa...	High / 8.7	VULNCHECK KEV	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2025-71437	Astral uv through 0.8.21 Path Traversal via Symlinks in Sdi...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2023-54403	Yonyou U8 CRM Arbitrary File Read via getemaildata.php	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2024-58387	Inspur HCM Cloud Arbitrary File Read via file/download E...	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2026-112904	Vvveb: Path Traversal in nextRestore() and nextBackup()	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103591	DeepWiki-Open through commit d92819a Unauthenticate...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102242	Google: Path Traversal via Symlink Following in allowedLo...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39792	WordPress Simple File List plugin <= 6.3.11 - Arbitrary File ...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85487	CVE-2026-85487: A path traversal vulnerability exists in t...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101155	Security Advisory 0189	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101154	Security Advisory 0189	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114083	Trigger.dev before 4.5.0-rc.3 Path Traversal via Packets P...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109286	Open WebUI 0.7.0 before 0.11.4 Session Token Theft via S...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100372	ClipBucket v5 before 5.5.3-#197 Path Traversal via templa...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95588	WordPress AcyMailing SMTP Newsletter plugin <= 11.0.5 ...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103398	OpenSave through 2.4.0 Arbitrary File Read and Write via ...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96656	Plex Media Server arbitrary file write	High / 8.6	CISA KEV	✓ Blocked
CVE-2026-101888	Prime Mover < 2.2.1 Zip Slip Path Traversal File Write	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-47679	GLPI: arbitrary file deletion	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100633	SiYuan 3.8.0 through 3.8.3 Path Traversal via MCP File Op...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-74043	Wazuh 4.1.1 before 4.14.8 Path Traversal via Cluster Uploa...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-85953	Path traversal and privilege management flaws in Progres...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106486	Backstage has iImproper filesystem validation in Bitbucke...	High / 8.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-63120	PGHoard: Incomplete Path Traversal fix in restore.py allo...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87685	CVE-2026-87685: An arbitrary file manipulation vulnerabi...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104810	Mitel MiVoice Office 400 File Management File Browser p...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104706	Mitel MiVoice Office 400 view system files path traversal	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-74033	Wazuh from 4.1.1 before 4.14.8 Path Traversal in CDB List ...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-58069	CVE-2026-58069: This vulnerability in Veeam Backup & ...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100707	Kyverno before 1.19.1 Namespace Isolation Bypass via Per...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109956	NLTK through 3.10.3 Path Traversal via WekaClassifier Mo...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84315	Nginx UI OTP secure-session step-up is missing on sensi...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100637	SiYuan before v3.8.4 Path Traversal via checkoutRepo se...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112051	Xinference through 4.0.1 Path Traversal via model_name i...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114400	Trudesk through 1.2.11 Missing Authentication for Ticket A...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111234	SimplePie through 1.9.0 Local File Read via file:// Redirect	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111915	Yank Note before 3.93.1 Path Traversal via /api/help Endp...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-43851	CVE-2026-43851: A path traversal vulnerability could allo...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13224	Fireware OS Path Traversal in WebUI Management Agent ...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-19627	IBM Planning Analytics Local is affected by security vulne...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103263	Tornado before 6.5.9 StaticFileHandler Path Traversal via ...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-111854	CVE-2026-111854: An issue was discovered on Tektronix ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82900	IBM Guardium Data Protection is affected by multiple vuln...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84247	IBM Guardium Data Protection is affected by multiple vuln...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103360	Langflow OSS is affected by multiple vulnerabilities	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42724	WordPress CleanSkin theme <= 1.5.0 - Local File Inclusio...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15983	Super Forms <= 6.3.316 - Authenticated (Subscriber+) Ar...	High / 8.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-94062	WordPress Werkstatt theme <= 4.8.3 - Local File Inclusio...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94067	WordPress The Voux theme <= 6.9.5 - Local File Inclusio...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62115	WordPress KuteShop theme <= 4.2.9 - Local File Inclusio...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66566	WordPress Ambient theme <= 1.7 - Local File Inclusion vu...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42704	WordPress Kids Care theme <= 3.2.4 - Local File Inclusio...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104899	GeoDirectory <= 2.8.187 - Unauthenticated Local File Incl...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62066	WordPress Volos theme <= 1.2 - Local File Inclusion vulne...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62065	WordPress Cardea theme <= 2.3 - Local File Inclusion vul...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103257	n8n before 1.123.80, 2.39.6, and 2.40.1 Path Traversal via ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62067	WordPress Kaven theme <= 1.2 - Local File Inclusion vuln...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62069	WordPress Fabius theme <= 1.0 - Local File Inclusion vuln...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62068	WordPress Teoro theme <= 1.1 - Local File Inclusion vulne...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42269	countly-server: Path Traversal in delete_import Endpoint ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104103	Ludwig: Path traversal in dataset archive extraction allows...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-51568	CVE-2026-51568: modelscope Agentscope v1.0.18-v1.0....	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92709	Rsyslog: DynFile Path Traversal → Arbitrary File Write as ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-65103	CVE-2026-65103: NVIDIA AIStore for Linux contains a pat...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83746	Skype for Business Elevation of Privilege Vulnerability	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112820	WordPress Academist Core plugin <= 1.4.1 - Local File Inc...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-51907	CVE-2026-51907: In TaskingAI v0.3.0 in the QR Code Ge...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62099	WordPress Boutique theme <= 2.3.3 - Local File Inclusion...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104909	Mang Board <= 2.4.3 - Unauthenticated Local File Inclusi...	High / 8.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-62096	WordPress Biolife theme <= 3.2.3 - Local File Inclusion vu...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62094	WordPress TechOne theme <= 3.0.3 - Local File Inclusion...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62092	WordPress Armania theme <= 1.4.8 - Local File Inclusion ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62075	WordPress Backhoe theme <= 2.0 - Local File Inclusion v...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62074	WordPress Ozeum theme <= 1.3.0 - Local File Inclusion v...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62070	WordPress Flipmart theme <= 2.8 - Local File Inclusion vu...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-51570	CVE-2026-51570: modelscope Agentscope v1.0.0-v1.0.8 ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103367	ShopMagic <= 4.9.0 - Unauthenticated Local File Inclusio...	High / 8.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-62020	WordPress TouchUp theme < 1.4 - Local File Inclusion vul...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-48194	WordPress DukaMarket theme <= 1.3.0 - Local File Inclusi...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-48193	WordPress Uminex theme <= 1.0.9 - Local File Inclusion v...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42777	WordPress Aalto theme <= 1.8 - Local File Inclusion vulne...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-57113	PraisonAI GitHub template cache path traversal allows out...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84842	IBM Guardium Data Protection is affected by multiple vuln...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112850	WordPress Your Dress theme <= 1.4.1 - Local File Inclusio...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105865	Payload: Incomplete validation during the upload file lifec...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109221	Groundhogg <= 4.9.3 - Authenticated (Sales Representati...	High / 8.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-76479	Cisco Unified Communications Products Hardening Relea...	High / 7.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69783	Windows Update Elevation of Privilege Vulnerability	High / 7.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102875	VLC media player before 3.0.24 Path Traversal via skins2	High / 7.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70222	Windows Shell Elevation of Privilege Vulnerability	High / 7.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83873	Windows Shell Elevation of Privilege Vulnerability	High / 7.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101885	ZeroClaw before 0.8.5 Path Traversal via Plugin Manifest ...	High / 7.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106634	Adobe Experience Manager | Improper Limitation of a Pat...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108120	path traversal inKoozali - SME Server	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111398	WordPress MapSVG plugin <= 8.16.1 - Arbitrary File Deleti...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39752	WordPress Jobs for WordPress plugin <= 2.8.2 - Arbitrary...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105945	Apache Pulsar: Improper Validation of Package Name Co...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103435	Arbitrary File Write via Write-Time Symlink Following (TO...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106047	CVE-2026-106047: A Path Traversal vulnerability in the te...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40805	WordPress PeepSo plugin <= 9.0.5.4 - Arbitrary File Delet...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78530	WordPress FoodBakery theme <= 4.6 - Arbitrary File Dele...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-85964	Path traversal in Progress MarkLogic Server Query Console	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2017-20289	Broadstreet Ad Widget WordPress Plugin < 2.12.0 Local Fi...	High / 7.7	VULNCHECK KEV	✓ Blocked
CVE-2026-113352	uTox through 0.18.1 Path Traversal via Auto-Accepted File ...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105840	lrzsz before 0.13.0 Path Traversal via lrz Restricted Mode ...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112015	Omnigent 0.3.0 before 0.14.0 Path Traversal via Sub-Agen...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100638	SiYuan before v3.8.4 Path Traversal via setNotebookIcon	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-71427	Office-PowerPoint-MCP-Server through 2.0.7 Path Trave...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-41582	countly-server: Unauthenticated Path Traversal via Public...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92390	-J no-clobber guarantee bypassed with 103 early hints	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89294	Simply Schedule Appointments <= 1.6.12.27 - Authenticat...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97244	WordPress Creator LMS plugin <= 1.2.19 - Path Traversal ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103088	CVE-2026-103088: Handlebars.java before 4.5.5 allows d...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105052	IBM Maximo Application Suite Information Disclosure	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75061	IBM Planning Analytics Local is affected by security vulne...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-65161	CVE-2026-65161: NVIDIA AIStore for Linux contains a vul...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75098	Product Designer App <= 1.1.3 - Unauthenticated Arbitrar...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-51852	CVE-2026-51852: agent-zero 1.7, 1.8, 1.9, and 1.10 is vulne...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-51853	CVE-2026-51853: agent-zero 1.7, 1.8, 1.9, and 1.10 is vulne...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94123	WordPress NextGEN Gallery plugin <= 4.5.0 - Arbitrary Fil...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92174	SiteOrigin Widgets Bundle <= 1.73.2 - Authenticated (Con...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-51860	CVE-2026-51860: bisheng 2.3.0, 2.4.0, and 2.4.0-beta1 is...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110284	LifterLMS <= 10.3.1 - Authenticated (Contributor+) Local F...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103507	Arbitrary file-write via log configuration path in P4Search	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-51874	CVE-2026-51874: In Devika v1.0, the Patcher Agent save_...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94664	WordPress PDF for Contact Form 7 plugin <= 7.1.0 - Arbitr...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94666	WordPress Generate PDF using Contact Form 7 plugin <=...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91136	Divi Plus <= 2.4.0 - Unauthenticated Arbitrary File Read vi...	High / 7.5	VULNCHECK KEV	✓ Blocked
CVE-2026-103060	Path traversal in rebar3 via unvalidated dependency app n...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96612	Path traversal in Hex via unvalidated dependency app na...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86147	Apache bRPC: Arbitrary file creation/truncation via /flags ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88392	CVE-2026-88392: Unimall v4 is vulnerable to Directory T...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111833	WordPress weForms plugin <= 1.6.28 - Arbitrary File Dele...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103896	10Web Booster <= 2.34.5 - Unauthenticated Limited File ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111855	CVE-2026-111855: An issue was discovered on Tektronix ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84275	IBM Guardium Data Protection Path Traversal	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95140	CVE-2026-95140: kkFileView v5.0.0 through v5.0.2 conta...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111093	CVE-2026-111093: In JetBrains Datalore before 2026.2.1 u...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-51888	CVE-2026-51888: langflow-ai langflow v1.8.4 is affected ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88394	CVE-2026-88394: WookTeam v1.6.6 and before is vulner...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75028	WPCafe <= 3.0.18 - Authenticated (Contributor+) Local Fil...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked

INDUSFACE™ ©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-107377	datamodel-code-generator: Protobuf weak-import path tr...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-19493	Security vulnerabilities have been found in IBM Verify Ide...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56833	PraisonAI Dynamic Context history and terminal tools rea...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114604	GraphQL Tools: Prototype pollution in mergeIncrementalR...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115365	OpenBao 2.3.0 before 2.6.3 Incorrect Authorization via Po...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115497	Music Store <= 1.4.7 - Unauthenticated Arbitrary File Rea...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102810	Marmite through 0.4.2 Path Traversal via Development Se...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56834	PraisonAI dynamic-context artifact tools read arbitrary ho...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79985	Apache Camel: camel-smb resolved the remote path of a ...	High / 7.4	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-79986	Apache Camel: camel-azure-files resolved the remote pat...	High / 7.4	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-102123	Kiteworks Core Path Traversal	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79984	Apache Camel: camel-mina-sftp resolved the remote pat...	High / 7.4	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-79983	Apache Camel: camel-ftp resolved the remote path of a p...	High / 7.4	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-93695	Arbitrary file write through remote file identifiers in Progre...	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-71168	CVE-2026-71168: Dell System Update, versions prior to 2....	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79809	HPE: Unauthenticated Path Traversal in ClearPass Policy ...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103508	Path traversal via logging configuration in P4Search	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101295	Oc-mirror: oc-mirror: path traversal / arbitrary file write in ...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70161	.NET Elevation of Privilege Vulnerability	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-26243	Arbitrary Folder Deletion in Qsync Central 5.0.0.5	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-55231	Vvveb: Path traversal in Vvveb via sanitizeFileName() byp...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101153	Security Advisory 0188	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114622	baserCMS: Encoded path traversal bypass in the theme fil...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102119	Kiteworks Email Protection Gateway Path Traversal	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108902	pH7Builder before 18.5.0 Path Traversal Arbitrary File Del...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102089	Kiteworks Email Protection Gateway path traversal	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102099	Kiteworks Core arbitrary file write	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115354	Mistune before 3.3.0 Arbitrary Local File Read via Include ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86136	Fireware OS Missing Authorization in wgagent Manageme...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101044	pacquet before 12.0.0-alpha.5 Path Traversal via lockfile a...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97023	Flatpak: flatpak: arbitrary file deletion in root context via p...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-90925	Path Traversal in Innotim Software's Logsign SIEM	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108158	plugNmeet Server through 2.5.2 Path Traversal via /api/w...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103255	n8n before 1.123.80, 2.39.6, and 2.40.1 Path Traversal and ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2022-51025	Penta Security WAPPLES 4.0.54.1 / 5.0 / 6.0 Path Traversa...	High / 7.1	VULNCHECK KEV	✓ Blocked
CVE-2026-109601	Frappe Framework before v16.30.0 Arbitrary File Read via ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-71426	GetSimple CMS: Authenticated Stored Local File Inclusion...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100536	OpenClaw before 2026.8.1 Path Traversal via Structured A...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18228	Hyperscale Path Traversal	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104478	Formwork before 2.3.13 Path Traversal via BackupControll...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-92153	F´: Arbitrary File Write in Svc::FileUplink via attacker-contr...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108694	ConvertX through 0.19.0 Arbitrary File Read via Pandoc C...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105834	Rundeck before 6.2.0 Arbitrary File Read via File Resourc...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113402	ArmorX Global Technology | ArmorX Spam - Local File In...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106560	Backstage: Improper repository path validation in a Scaffo...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92533	Path Traversal in BugTracker.NET	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84823	Org.wildfly.core: wildfly: path traversal in take-snapshot d...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111170	kedro-datasets 9.3.0 through 9.6.0 Path Traversal via Mat...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-5703	Path Traversal in Satel Iberia SenNet Datalogger Serie 200	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106103	Quasar Framework: Path Traversal / Arbitrary File Write vi...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97024	Flatpak: flatpak: arbitrary write in root context via path tra...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107777	Thermo Fisher Torrent Suite Software Path Traversal	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2024-58386	ZoneMinder 1.37.x Path Traversal via files view	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96440	Flowring Agentflow 4.0 - Improper Limitation of a Pathna...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-90915	Joomla! Core - [20260905] - Core - Arbitrary directory d...	High / 7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114492	gin-vue-admin through 2.9.2 Path Traversal via removePl...	High / 7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97164	Joomla Extension - svenbluege.de - Path Traversal in Cle...	High / 7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116195	Rclone before 1.75.2 Path Traversal via translateLink .rclo...	High / 7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114399	Trudesk through 1.2.11 Path Traversal via Backup Delete a...	High / 7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101889	Prime Mover < 2.2.1 Path Traversal via wprime-config.json	High / 7	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-103254	n8n before 1.123.80, 2.39.6, and 2.40.1 Path Traversal via ...	High / 7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-74031	Wazuh 4.1.1 before 4.14.8 Path Traversal File Deletion via R...	High / 7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102262	Newell Brands DYMO ID parent directory open to path tra...	High / 7	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-101069	dbgate Export databaseConnections.js exportModelSql p...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111618	CoAI through 4.0.0 Unauthenticated Path Traversal via Ar...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-5049	CVE-2026-5049: A path traversal vulnerability affects the...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107353	traverse: set() can write to built-in prototypes via an untru...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112144	satya-vinay Events-Management-System project.sql file ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-11319	TickTick Android 8.2.2.0 Path Traversal via ShareReceive...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105751	Docling: Arbitrary local file read via draw:image xlink:href ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101070	dbgate Files Endpoint runners.js files path traversal	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114491	pdfmake 0.3.8 before 0.3.12 Local File Policy Bypass via S...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102252	Google: Path Traversal in VMDK Extractor in OSV-SCALIBR	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101126	Joomla Extension - balbooa.com - File meta data tamperi...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101082	PMWeb downloader.aspx path traversal	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101066	dbgate Archive Link Creation archive.js createLink path tr...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101068	dbgate Create Connection Endpoint zipJsonLinesData.js ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101067	dbgate save-uploaded-file Endpoint files.js saveUploade...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100727	CVE-2026-100727: An improper access control vulnerabil...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97662	Argument injection in the diff scan operation in AWS secu...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-110666	cemtan sar2html File Upload sar2html.py updateDb path t...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110860	GitPython 3.1.62 before 3.2.0 Symlink Path Traversal via S...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108772	bleenco abstruse Cache Endpoint download_cache.go fil...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109309	SiYuan v3.7.0 before v3.8.6 Arbitrary File Read via Plugin ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108156	LobsterAI 2026.5.27 through 2026.9.23 Arbitrary Director...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104417	Ghost 1.20.0 before 6.64.0 Path Traversal via Locale Setting	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105144	Drogon Static File Router StaticFileRouter.cc route path tr...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108258	Shiny for Python - Path traversal in bookmark restore	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110717	Janus WebRTC Server through 1.4.3 Path Traversal via Re...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108940	EricLBuehler Mistral.rs handlers.rs calibration_apply path ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-44414	CVE-2026-44414: A vulnerability has been identified in In...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108938	code-projects Matrimonial System matrimony.sql file acc...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116168	SiYuan before v3.8.7 Path Traversal Local File Read via M...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93347	Wazuh 4.1.1 before 4.14.8 Path Traversal via Cluster get_lis...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109519	YouTransfer Template Rendering template path traversal	Medium / 6.9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-116073	Leon before commit 50df142 Path Traversal via /downloa...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102229	Visual Studio Code Information Disclosure Vulnerability	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66481	WordPress Presto Player Pro plugin <= 3.0.1 - Arbitrary Fil...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55836	Open Zaak: Path traversal / arbitrary server-file read via D...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63266	Arbitrary file write via calcext:data-mappings, sql provide...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-97242	WordPress WEBO MCP plugin <= 3.0.18 - Arbitrary File D...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96824	WordPress Template Kit – Import plugin <= 1.0.16 - Arbitra...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78249	CVE-2026-78249: A path traversal vulnerability exists in t...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109595	Hugo v0.84.0 before v0.167.0 Path Traversal via js.Build E...	Medium / 6.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110235	MP Manager through 1.1.0 Path Traversal via Archive Extra...	Medium / 6.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63268	LFI via calcext:data-mappings, sql provider and sdbc:flat:...	Medium / 6.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63269	LFI and GET SSRF via GStreamer and HLS playlists	Medium / 6.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102141	Kiteworks Core Privilege Escalation through External Con...	Medium / 6.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63267	LFI and GET SSRF via calcext:data-mappings and csv pro...	Medium / 6.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109574	Hugo before v0.167.0 Path Traversal via css.Sass Import F...	Medium / 6.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78851	CVE-2026-78851: Directory Traversal vulnerability in Gra...	Medium / 6.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-85932	Microsoft Office SharePoint Information Disclosure Vulne...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69968	Windows libarchive Tampering Vulnerability	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114623	baserCMS: Path traversal in the BcThemeFile admin scree...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104107	FileRise: Authenticated path traversal escapes configured...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111829	WordPress WP Mailster plugin <= 1.9.1.0 - Local File Inclu...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106219	CVE-2026-106219: In JetBrains TeamCity before 2026.2.1...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-41958	CVE-2026-41958: A path traversal vulnerability exists in t...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93448	Langflow OSS is affected by multiple vulnerabilities	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-90466	Apache Impala: Path traversal executes JARs outside trus...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-93767	Tainacan <= 1.3.0 - Authenticated (Subscriber+) Path Tra...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97348	SiteOrigin Widgets Bundle <= 1.74.3 - Authenticated (Con...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96279	Flatpak: flatpak: path traversal issue in oci archive extracti...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83683	Windows Encrypting File System (EFS) Information Disclo...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85840	Windows Event Viewer Information Disclosure Vulnerability	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69973	Windows libarchive Tampering Vulnerability	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101217	CVE-2026-101217: Dell Unisphere for PowerMax vApp, ve...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70298	Microsoft Office SharePoint Information Disclosure Vulne...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88137	WebDAV Information Disclosure Vulnerability	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82915	Path Traversal in Bimser Solution Software's eBA Plus	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95264	CVE-2026-95264: Feehi CMS 2.1.1 is vulnerable to Direct...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93537	Path traversal in Fleet Helm valuesFiles allows disclosure ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102457	DigiWin | EasyFlow .NET - Arbitrary File Read	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89039	Arbitrary file read via the convert_playwright_script prom...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103884	Keycloak-services: keycloak-services: path traversal in x....	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97671	Langflow OSS is affected by multiple vulnerabilities	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112311	WordPress ACF Extended plugin <= 0.9.2.7 - Arbitrary Fil...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39754	WordPress Piotnet Addons For Elementor plugin <= 7.1.71 ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112948	Vitest: Servers misapply `server.fs.deny`, serving `.env`, ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91395	CVE-2026-91395: Vulnerability in the Oracle Java SE, Ora...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-91396	CVE-2026-91396: Vulnerability in the Oracle Java SE, Ora...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106491	Backstage: Improper input validation in proxy-backend	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113491	GeoDirectory < 2.8.194 - Subscriber+ Media File Disclosu...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112946	Vite: Files outside `server.fs.allow` could be served when ...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106559	Backstage: Improper input validation in Confluence to Ma...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78340	CVE-2026-78340: Dell Secure Connect Gateway (SCG) P...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102783	Joomla Extension - balbooa.com - Path Traversal in imag...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109162	TYPO3 CMS - Security Misconfiguration in Form Framew...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84320	Nginx UI: Auto backup name allows path traversal outside ...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104721	Logback: Incomplete protection against CVE-2026-19880	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105125	LaraDashboard before 1.4.8 Path Traversal via /api/transla...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104871	Angular SSR: Path Traversal to Sibling Directories in Com...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106579	ImageMagick: Policy Bypass when using coder as the do...	Medium / 6.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85518	Openscap: openscap: arbitrary file write via path traversal...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107466	Flatpak-builder: local file exfiltration via `file	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92205	BusyBox libarchive Symlink Directory Traversal Arbitrary ...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105265	Kiloview E3 NDI Encoder Path Traversal	Medium / 6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111978	GiveWP < 4.19.0.1 - Give Manager+ Path Traversal via Cor...	Medium / 6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112950	Vitest: Windows backslash traversal bypasses the @vites...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103061	Path traversal in Gleam via unvalidated package applicatio...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-116171	SiYuan 3.5.4 before 3.8.7 Sensitive Path Bypass via Wind...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79534	CVE-2026-79534: mark3labs mcp-filesystem-server v0.1...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108591	InnoShop 0.9.2 Local File Disclosure via AI Core MCP file_...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104769	Debloat <= 1.3.0 - Unauthenticated Arbitrary File Read via ...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104246	Contact Form 7 Signature Addon <= 4.2.2 - Unauthenticat...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54703	Markdown Preview Enhanced: Arbitrary File Write via upd...	Medium / 5.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106108	Quasar Framework: App Vite SSG page output paths can ...	Medium / 5.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94580	CVE-2026-94580: An arbitrary file and directory deletion ...	Medium / 5.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-71453	CVE-2026-71453: - External Control of File Name or Path ...	Medium / 5.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15953	Path Traversal During Project Archive Import	Medium / 5.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85812	Windows Bind Filter Driver Information Disclosure Vulner...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79715	IBM WebSphere Application Server Liberty Path Traversal	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115207	Patch: filename validation bypass in reversal fallback allo...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42532	CVE-2026-42532: A path traversal vulnerability exists in t...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96419	GitLab: Improper Limitation of a Pathname to a Restricted ...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70084	Windows Projected File System Information Disclosure V...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96857	Windows Projected File System Information Disclosure V...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103820	CAI Content Credentials | Improper Limitation of a Pathna...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
GHSA-4WWP-F6GW-6QM5	SiYuan: TLS Private Keys Readable via getFile (Incomplet...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104806	Mitel MiVoice Office 400 System Logs Path Traversal Info...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-63130	EspoCRM: Admin path traversal in LabelManager (Custom...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100549	OpenClaw before 2026.8.1 Path Traversal via QQBot voice...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-61624	CVE-2025-61624: An Improper Limitation of a Pathname t...	Medium / 5.4	CISA KEV	✓ Blocked
CVE-2026-85985	MariaDB: Unauthorized file access via CONNECT engine ...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62664	FileRise: Authenticated path traversal in createFolder allo...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-90458	CVE-2026-90458: OpenStack Ironic before 39.0.1 allows ...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107321	W3 Total Cache < 2.10.6 - Author+ Path Traversal via CDN...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105820	Vault ACL Policy Cache Vulnerable to Cross-Namespace ...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110253	weForms <= 1.6.28 - Unauthenticated Limited Media File ...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106508	Backstage: Potential file exposure through local TechDoc...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109155	DeepPavlov Model Download untar path traversal	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108543	ag2ai ag2 UserProxyAgent os.path.join path traversal	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108791	westboy CicadasCMS Template Management input Templ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108544	Lippu Docx Reader Office Viewer App path traversal	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108567	InstantSoft icms2 Image image.php files_delete_file path t...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100533	OpenClaw before 2026.8.1 Path Traversal via Unicode Fall...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113738	R6410418 Jackrong-llm-finetuning-guide MTP weight_m...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114376	leomoon-studios wiki-go API editor.go SourceHandler pa...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114375	leomoon-studios wiki-go Files Rename API files.go Rena...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-58415	Apache HTTP Server: mod_dav_fs property database rea...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-86105	Fireware OS Improper Authorization in Access Portal Rev...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101142	Eleveo Quality Management Questionnaire Audio Upload ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55156	Token Optimizer MCP: Unauthenticated Path Traversal in ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114714	CVE-2026-114714: Roundcube Webmail before 1.6.20 and...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114402	Trudesk through 1.2.11 Path Traversal and Authorization B...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105174	Gerapy Project Management views.py project_create pat...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105286	Totolink A3002MU File Upload formUploadFile sub_44B2...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104983	Linux Mint Xreader PDF Attachment Saving ev-window.c ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104982	Linux Mint Xreader EPUB File epub-document.c g_strdup...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105157	RainyGao DocSys Document Controller doGetTmpFile.do ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113743	Tenstorrent tt-metal load_checkpoints.py load_hf_state_di...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109152	jbardin scp.py SCP Receive _recv_pushd path traversal	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109156	SeldonIO MLServer environment_tarball env.py _extract_e...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109153	MosaicML Composer Checkpoint Extraction checkpoint....	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62858	YOURLS: Unauthenticated File Inclusion	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104102	copyparty FTP: upload outside defined volumes (limited p...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84069	WebFacing Email Accounts for cPanel 5.3 - 5.3.6 - Unauth...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116045	1999AZZAR designer-mcp MCP motion-dev-guidelines....	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109354	LibreNMS before 26.9.0 Path Traversal via NFSen channel...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110212	ai-fusion-video through 1.2.0 Path Traversal in Media Upl...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-24718	Path Traversal Vulnerability in Qsync Central's qsyncsrv.cgi	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110766	Colanode Server through 0.4.7 Path Traversal via Avatar ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113505	aaPanel Download Endpoint v2.py send_file path traversal	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113664	ApostropheCMS import-export tar guard misses './..' beca...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94375	Order Export & Order Import for WooCommerce <= 2.7.8 ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107844	Contao: Path traversal in the images controller	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-61702	OpenPrinting CUPS: root-side banner file disclosure	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114379	EKKOLearnAI ekko-studio Media Generation API media.ts...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112302	kiwilan php-archive Extraction ArchiveZip.php extract pat...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113392	DrayTek Vigor2960 Apmupload mainfunction.cgi path tra...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113394	DrayTek Vigor2960 mainfunction.cgi setSWMProfile path...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-19585	Go-getter vulnerable to a path traversal in S3/GCS directo...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112310	docling-core 2.5.0 before 2.103.0 Local File Disclosure via...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105275	Satel Netco Design Relative Path Traversal	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113395	DrayTek Vigor2960 swmconfigupload mainfunction.cgi c...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111635	Helical Insight through 7.0.0 Path Traversal via /getExtern...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114253	oretnom23 file-management-system-php index.php inclu...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87291	CVE-2026-87291: Vulnerability in Oracle Java SE (compo...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114040	DT42 BerryNet Model Package Metadata dlmodelmgr.py ...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112138	diem-project diem dmCodeEditor actions.class.php join p...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-21133	CVE-2026-21133: Path traversal in Samsung Flow prior to ...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108790	westboy CicadasCMS Backend Template Editor save Tem...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-21137	CVE-2026-21137: Path traversal in Smart Switch prior to v...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114377	leomoon-studios wiki-go Comment Deletion comments.g...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103511	Arbitrary file-write via extension installation in P4Search	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102843	gedelumbung HospitalManagement Endpoint data_galeri....	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103290	Ghost 6.14.0 before 6.27.0 Path Traversal via ImageSize	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113737	R6410418 Jackrong-llm-finetuning-guide qwen_mtp_ggu...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112248	grandnode grandnode2 Excel Import ProductImportData...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112372	H3C Magic NX15 upload importprofile path traversal	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101886	Cisco Jabber for Android Path Traversal via Shared Conte...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106034	CVE-2026-106034: A Path Traversal vulnerability in Ivanti...	Medium / 5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103870	Pulp-rpm: distribution tree publish creates directories fro...	Medium / 5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104763	Post Export Import with Media <= 1.17.1 - Authenticated (A...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105676	Ghost: Path Traversal via Locale Setting	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104722	Listdom: AI-powered Business Directory with Classifieds ...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110268	Post Export Import with Media <= 1.17.2 - Authenticated (...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101036	FLB-Music FLB-Music-Player createParsedTrack.ts path.j...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115800	UbiquitousLearning mllm Convertor __init__.py load_mode...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109106	Polaris Office App Document Intake com.infraware.servic...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-110657	Khronos NNEF-Tools nnef through 1.0.10 and nnef-tools t...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108603	slide-maker through 5.8.0 Path Traversal via generate_im...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91375	CVE-2026-91375: Vulnerability in Oracle Java SE (compo...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83865	Windows Internet (wininet.dll) Tampering Vulnerability	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109118	GitLab: Improper Limitation of a Pathname to a Restricted ...	Medium / 4.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113719	virtualenv: Seed replacement does not contain metadata ...	Medium / 4.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106494	Backstage: Improper input validation in cloud storage UR...	Medium / 4.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105748	Docling: Crafted DoclingDocument JSON embeds local i...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-0312	Checkov by Prisma Cloud: Path Traversal Vulnerabilities	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106109	Quasar Framework: App Vite build cleanup can recursivel...	Medium / 4.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91380	CVE-2026-91380: Vulnerability in the Oracle Java SE, Ora...	Medium / 4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105683	Ghost: Path Traversal Vulnerability in Ghost ImageSize Se...	Low / 3.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110458	CVE-2026-110458: A malicious actor with access to the n...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110095	fast-uri vulnerable to improper path equivalence in relativ...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110457	CVE-2026-110457: A malicious actor with access to the n...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114370	Undertow: undertow: pathresourcemanager safepaths ch...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113731	djust: Arbitrary absolute-path file read in the find_handler...	Low / 3.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115569	Fallow: Jest and Vitest `projects` entries let an analyzed r...	Low / 3.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56857	Root.Mkdir(All) can follow junctions out of the root on Win...	Low / 3.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105795	Kiota: Unsafe oauth_card_path references in Kiota-gener...	Low / 3.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 544 blocked · avg CVSS 7.1 · 4 CISA KEV (continued)				
CVE-2026-96282	Flatpak: flatpak: extension metadata path traversal file exi...	Low / 3.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106496	Backstage: Inconsistent enforcement of allowed location ...	Low / 3.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106493	Backstage: Cloud storage catalog locations may cross co...	Low / 3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12660	IBM MQ Path Traversal	Low / 2.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104994	CVE-2026-104994: Trivy before 0.71.0 allows directory tr...	Low / 2.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101080	Tencent AI-Infra-Guard File Access dir_actions.py starts...	Low / 2.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101051	Cloudreve before 4.16.1 Path Traversal via Remote Downlo...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101132	DeepSeek deepseek-harness Bundle Patch profile.ts load...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109247	FreeRDP before 3.32.0 Path Traversal via Clipboard cFile...	Low / 2.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111935	NoteGen through 0.38.3 Local File Disclosure via Chat Im...	Low / 2.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103533	David-Crty databasement database-servers API Endpoint...	Low / 2.1	NO KNOWN EXPLOIT	✓ Blocked
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV				
CVE-2026-79849	HPE: Unauthenticated SQL Injection Vulnerabilities allow ...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105899	ColdFusion | Unrestricted Upload of File with Dangerous ...	Critical / 10	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-102427	Joomla Extension - ordasoft.com - Unauthenticated Rem...	Critical / 10	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-102785	Joomla Extension - yootheme.com - Unauthenticated re...	Critical / 10	VULNCHECK KEV	✓ Blocked
CVE-2026-79848	HPE: Unauthenticated SQL Injection Vulnerabilities allow ...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105857	Payload Form Builder has an RCE issue	Critical / 10	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-112851	WordPress HotLock theme <= 1.3.9 - PHP Object Injectio...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV (continued)				
CVE-2026-112853	WordPress Hallelujah theme <= 1.1.1 - PHP Object Injectio...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112856	WordPress Vagabonds theme <= 1.3.10 - PHP Object Injec...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112857	WordPress Reprizo theme <= 1.0.8 - PHP Object Injection ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112858	WordPress Rhodos theme <= 1.3.3 - PHP Object Injection ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112862	WordPress Participants Database plugin <= 2.7.8.5 - PHP ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79852	HPE: Unauthenticated SQL Injection allows Remote Code ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112855	WordPress Redy theme <= 1.3.5 - PHP Object Injection vu...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97248	WordPress Booking Activities plugin <= 1.18.7.1 - PHP Obj...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100512	WordPress Nested Pages plugin <= 3.3.2 - PHP Object Inj...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110886	WordPress Conversational Forms for ChatBot plugin <= 1....	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79854	HPE: Unauthenticated SQL Injection Vulnerability leads to ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104736	LearnPress <= 4.4.10 - Unauthenticated PHP Object Inject...	Critical / 9.8	VULNCHECK KEV	✓ Blocked
CVE-2026-103768	ELEX WordPress HelpDesk & Customer Ticketing System ...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-62010	WordPress Avventure theme <= 1.1.12 - PHP Object Injecti...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-112846	WordPress Save Life theme <= 1.2.14 - PHP Object Injecti...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109219	Mang Board - 2.4.4 - Unauthenticated Arbitrary File Uploa...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-108587	10Web Booster <= 2.34.10 - Unauthenticated Arbitrary Fil...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-104800	AGE-GATE <= 1.0 - Unauthenticated Remote Code Execut...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-55573	e107: Unsafe deserialization in install.php allows unauthen...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-93388	Printcart Store - Web to Print Product Designer for WooC...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV (continued)				
CVE-2026-110002	Snazzy Social Media Feed <= 2.5 - Unauthenticated Arbit...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-59774	Gitea Org-mode file disclosure and code execution	Critical / 9.8	VULNCHECK KEV	✓ Blocked
CVE-2026-87855	JTL-Connector for WooCommerce <= 2.4.3 - Unauthenti...	Critical / 9.8	VULNCHECK KEV	✓ Blocked
CVE-2026-109686	WordPress Link Whisper Free plugin <= 0.9.7 - PHP Obje...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-104730	Sunshine Photo Cart <= 3.7.4 - Unauthenticated PHP Obj...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-108291	WordPress Affiliates plugin <= 7.0.1 - PHP Object Injection...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-76486	Cisco Nexus 3000 and 9000 Series Switches VXLAN OA...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95606	WordPress The Events Calendar plugin <= 6.17.4 - PHP O...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76465	Cisco Nexus 3000 and 9000 Series Switches MPLS OAM ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76501	Cisco Nexus 9000 Series Switches SRv6 OAM (NGOAM) ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76485	Cisco Nexus 3000 and 9000 Series Switches VXLAN OA...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62124	WordPress N7 | Golf Club Sports & Events theme <= 2.21 ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62125	WordPress Asia Garden theme <= 1.3.1 - PHP Object Injec...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66482	WordPress Drone Media theme <= 2.2.0 - PHP Object Inje...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66483	WordPress Education Center theme <= 3.6.12 - PHP Obje...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66563	WordPress Windsor theme <= 2.10 - PHP Object Injection ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62052	WordPress Tipsy theme <= 1.6 - PHP Object Injection vul...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62053	WordPress Wine House theme <= 3.20 - PHP Object Inje...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62054	WordPress Yacht Rental theme <= 2.6 - PHP Object Inject...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62076	WordPress Kalles theme <= 1.1.7.1 - PHP Object Injection v...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV (continued)				
CVE-2026-62077	WordPress Avala theme <= 1.1.4 - PHP Object Injection vu...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62086	WordPress Juno theme <= 2.25 - PHP Object Injection vu...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62087	WordPress Equadio theme <= 1.1.4 - PHP Object Injection ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62090	WordPress WineShop theme <= 3.20 - PHP Object Injecti...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94589	Extensions For CF7 (Contact form 7 Database, Conditiona...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103889	3D Product configurator for WooCommerce <= 2.16.2 - U...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-62123	WordPress Invetex theme <= 2.18 - PHP Object Injection v...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97283	WordPress Advanced Post Manager plugin <= 4.5.5 - PH...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78535	WordPress Photolia theme <= 1.0.3 - PHP Object Injection...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81797	WordPress Buzz Stone | Magazine & Viral Blog WordPres...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104028	Anton Extensions <= 1.2.2 - Unauthenticated Arbitrary Fil...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66565	WordPress FC United theme <= 1.1.1 - PHP Object Injectio...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66564	WordPress ShiftCV theme <= 3.0.14 - PHP Object Injectio...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66568	WordPress Original theme <= 1.9.0 - PHP Object Injection ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66567	WordPress Anesta theme <= 1.5.3 - PHP Object Injection ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78531	WordPress Jacqueline theme <= 2.22 - PHP Object Inject...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78533	WordPress Qwery theme <= 3.6.1 - PHP Object Injection v...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66569	WordPress Kicker theme <= 2.2.1 - PHP Object Injection v...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78529	WordPress Alliance theme <= 3.11 - PHP Object Injection ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62120	WordPress Law Office theme <= 3.20 - PHP Object Injecti...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV (continued)				
CVE-2026-39797	WordPress GDPR Framework By Data443 plugin <= 2.5.0 ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76754	HPE: Unauthenticated SQL Injection Vulnerability leads to ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112859	WordPress Little Birdies theme <= 1.3.16 - PHP Object Inje...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112847	WordPress ZenSoul theme <= 1.13 - PHP Object Injection ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112854	WordPress Holistic Center theme <= 1.2.6 - PHP Object In...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62001	WordPress Marcell theme <= 1.2.14 - PHP Object Injection...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-62002	WordPress Meals & Wheels theme <= 1.1.13 - PHP Object I...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-62003	WordPress Mission theme <= 1.22 - PHP Object Injection ...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-62004	WordPress Motorix theme <= 1.11 - PHP Object Injection v...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-62005	WordPress Muzicon theme <= 1.15 - PHP Object Injection ...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-62006	WordPress Nuts theme <= 1.12 - PHP Object Injection vuln...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-62012	WordPress Coinpress theme <= 1.0.15 - PHP Object Inject...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-62013	WordPress Edge Decor theme <= 2.9 - PHP Object Injecti...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-62014	WordPress EmojiNation theme <= 1.0.12 - PHP Object Inje...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-62009	WordPress Filmax theme <= 1.1.11 - PHP Object Injection v...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-62015	WordPress Gamezone theme <= 1.1.11 - PHP Object Injecti...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-62016	WordPress Gamic theme <= 1.19 - PHP Object Injection vu...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-62017	WordPress Good Homes theme <= 1.3.13 - PHP Object Inj...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-62018	WordPress Gunslinger theme <= 1.11 - PHP Object Injectio...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2021-3199	CVE-2021-3199: Directory traversal with remote code exe...	Critical / 9.8	CISA KEV	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV (continued)				
CVE-2026-76722	Uncontrolled Format String Vulnerabilities lead to Remote ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112848	WordPress Hostme v2 theme <= 7.0 - PHP Object Injectio...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-46652	Path traversal via HTTP `Content-Disposition` header in E...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62011	WordPress Bonbon theme <= 1.11 - PHP Object Injection v...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-75873	Zella Theme < 2.6.3 - Unauthenticated Arbitrary File Upload	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82901	Ultra Addons for Contact Form 7 <= 3.5.50 - Unauthentic...	Critical / 9.8	VULNCHECK KEV	✓ Blocked
CVE-2026-61998	WordPress Le Truffe theme <= 1.1.7 - PHP Object Injectio...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-94075	WordPress Newsletters plugin <= 4.18.1 - PHP Object Inje...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114196	WordPress Paytium plugin <= 5.0.5 - PHP Object Injectio...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-61997	WordPress Legal Stone theme <= 1.2.11 - PHP Object Inje...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-93933	WordPress Rosalinda theme <= 1.2.4 - PHP Object Injecti...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42719	WordPress Dynamic User Directory plugin <= 2.4 - PHP ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42718	WordPress Booster for WooCommerce plugin <= 8.4.0 - ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42716	WordPress Payever - WooCommerce Gateway plugin <= ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104398	WordPress AFFI – Affiliate Marketing for WooCommerce ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93936	WordPress IPharm theme <= 1.2.4 - PHP Object Injection ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93937	WordPress Hygia theme <= 1.21.0 - PHP Object Injection ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93934	WordPress Partiso theme <= 1.1.13 - PHP Object Injection ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93935	WordPress Let's Play theme <= 1.1.15 - PHP Object Injecti...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62046	WordPress Gutentype theme <= 2.1.12 - PHP Object Inject...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV (continued)				
CVE-2026-93932	WordPress Smart Casa theme <= 1.0.12 - PHP Object Inje...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115806	Prime Mover <= 2.2.1 - Unauthenticated PHP Object Inject...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62008	WordPress Orpheus theme <= 1.8 - PHP Object Injection ...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-93929	WordPress Travesia theme <= 1.1.16 - PHP Object Injectio...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93927	WordPress Veto theme <= 1.6.0 - PHP Object Injection vul...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93942	WordPress Dwell theme <= 1.16.0 - PHP Object Injection v...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93941	WordPress Edema theme <= 1.2.2.2 - PHP Object Injectio...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93940	WordPress Greeny theme <= 2.10.0 - PHP Object Injectio...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93938	WordPress Hogwords theme <= 1.2.7 - PHP Object Injecti...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93931	WordPress Smash theme <= 1.12.0 - PHP Object Injection ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93930	WordPress Tantra theme <= 2.9.0 - PHP Object Injection ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93943	WordPress Convex theme <= 1.16.0 - PHP Object Injectio...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62051	WordPress Stargaze theme <= 1.10 - PHP Object Injection ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62050	WordPress Splendour theme <= 1.23 - PHP Object Injecti...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42723	WordPress CleanSkin theme <= 1.5.0 - PHP Object Injecti...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93944	WordPress Camelia theme <= 1.2.15 - PHP Object Injectio...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93945	WordPress Balance theme <= 1.12.0 - PHP Object Injectio...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62045	WordPress Booklovers theme <= 2.13.0 - PHP Object Inje...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107188	Eptura Archibus Workflow Rule Enables Unauthenticated ...	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102238	Visual Studio Code Remote Code Execution Vulnerability	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV (continued)				
CVE-2026-54630	Part-DB: Authenticated RCE via .phar attachment upload s...	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104849	Tinypool: Prototype Pollution Gadget to RCE in run() optio...	Critical / 9.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104848	Tinypool: Prototype Pollution gadget in worker options le...	Critical / 9.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88772	Memory overflow vulnerability leading to Remote Code E...	Critical / 9.5	CISA KEV	✓ Blocked
CVE-2026-107406	Memory overflow vulnerability leading to Remote Code E...	Critical / 9.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94132	Joomla Extension - acymailing.com - Remote Code Execu...	Critical / 9.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-89310	SQL Command Injection Vulnerability in JTL-WMS	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-48482	GLPI: RCE via Form import	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96408	CVE-2026-96408: A code injection vulnerability exists in ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85520	Unauthenticated arbitrary file write leading to RCE in gmfe...	Critical / 9.3	VULNCHECK KEV	✓ Blocked
CVE-2026-55486	Goobi viewer: IIIF Auth 2.0 origin parameter unsanitized ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-50619	Unauthenticated remote code execution vulnerability	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63146	Omnispace Agora Project < 26.10.0 PHP Code Injection vi...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2023-54405	H3C CVM Unauthenticated File Upload via fileUpload/upl...	Critical / 9.3	VULNCHECK KEV	✓ Blocked
CVE-2026-84411	MikroTik RouterOS Integer Underflow	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101997	Junos OS: SRX Series: A network-based attacker causes ...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109618	PHP: RCE via OOM corruption	Critical / 9.2	CISA KEV	✓ Blocked
CVE-2026-102992	piscina: Prototype-pollution gadget in ThreadPool.option...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-47168	EspoCRM: Authenticated RCE via Unsafe PHP Object Des...	Critical / 9.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-97670	Avada (Fusion) Builder <= 7.16.1 - Unauthenticated Arbitra...	Critical / 9.1	VULNCHECK KEV	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV (continued)				
CVE-2026-54454	OpenCATS: Authenticated RCE in the Import module	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56660	GetSimple CMS: CSRF, SSRF, and Unrestricted Zip Extrac...	Critical / 9.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-93697	CVE-2026-93697: There is a stored XSS vulnerability allo...	Critical / 9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93029	CVE-2026-93029: There is a stored XSS vulnerability allo...	Critical / 9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96837	WordPress CartFlows plugin <= 3.2.0 - Remote Code Exe...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110370	WordPress GS Pins for Pinterest plugin <= 1.9.2 - PHP Obj...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110369	WordPress WordPress Team Members – GS Plugins plugi...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103474	yii2-starter-kit through 4.2.0 Unrestricted File Upload RCE	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-102377	WordPress Photo Gallery by 10Web plugin <= 1.8.46 - PH...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-97291	WordPress Schema & Structured Data for WP & AMP plug...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94678	WordPress Go Live Update Urls plugin <= 7.0.8 - PHP Obj...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94076	WordPress SEO Plugin by Squirrly SEO plugin <= 14.2.5 - ...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96831	WordPress Themify Builder plugin <= 7.8.1 - PHP Object I...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95531	WordPress Conversational Forms for ChatBot plugin <= 1....	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94683	WordPress DesignSetGo plugin <= 2.8.0 - PHP Object Inj...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111408	WordPress Quiz And Survey Master plugin <= 11.2.7 - PH...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82814	Duplicator <= 1.5.17 and Duplicator Pro <= 4.6.10 - Unauth...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94121	WordPress 10Web Booster – Website speed optimization, ...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107436	WordPress Strong Testimonials plugin <= 3.3.12 - PHP Ob...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69943	Microsoft Office SharePoint Remote Code Execution Vuln...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV (continued)				
CVE-2026-106599	WordPress SureCart plugin <= 4.9.3 - PHP Object Injectio...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-86461	FV Flowplayer Video Player <= 7.5.54.7212 - Authenticate...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111311	DoubleScale | All-in-One CRM <= 1.5.1 - Authenticated (S...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-92553	YaySMTP <= 2.7.7 - Authenticated (Subscriber+) Arbitrar...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97284	WordPress Icegram plugin <= 3.1.31 - PHP Object Injectio...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-15700	AWP Classifieds < 4.4.9 - Admin+ Arbitrary File Upload vi...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104392	WordPress Quiz And Survey Master plugin <= 11.2.7 - PH...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95534	WordPress Unlimited Elements For Elementor (Free Widg...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-17196	Super Forms <= 6.3.316 - Authenticated (Subscriber+) Ar...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-103668	CVE-2026-103668: An SQL Injection vulnerability exists i...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105436	WordPress MainWP Child plugin <= 6.2.1 - Deserialization...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70297	Skype for Business Remote Code Execution Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84317	Nginx UI: MCP nginx_config_add skips config directive va...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108980	CVE-2026-108980: Blinko through 1.8.8 allows directory t...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87690	Metasploit Framework ios_image_gather Path Traversal L...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96230	Microsoft Security Advisory CVE-2026-96230 - ASP.NE...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108452	Microsoft Office SharePoint Remote Code Execution Vuln...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-84316	Nginx UI: nginx config directive denylist (ValidateConfigFi...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103535	Thelia v2.6.1 contains path traversal and PHP code injecti...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100511	WordPress VK Google Job Posting Manager plugin <= 1.3....	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV (continued)				
CVE-2026-97257	WordPress Simple Event Planner plugin <= 1.5.7 - PHP Ob...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94064	WordPress Neo | Barber Shop WordPress Theme theme <...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94065	WordPress ColorFolio theme <= 1.3 - PHP Object Injectio...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83526	FV Player 8 <= 8.1.7 - Authenticated (Subscriber+) Arbitra...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104723	LifterLMS <= 10.2.1 - Authenticated (Custom+) PHP Objec...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105701	ACPT (Premium) <= 2.0.66 - Authenticated (Subscriber+)...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97188	String Locator < 2.6.8 - Unauthenticated PHP Object Injec...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62021	WordPress Angio theme <= 1.1.1 - PHP Object Injection vul...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105885	WordPress Slider by 10Web plugin <= 1.2.62 - PHP Object...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12269	Authenticated File Write to RCE via keepalived in DDI Cent...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85134	Arbitrary File Upload Leading to Remote Command Execu...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54675	FreePBX: Authenticated Remote Code Execution via File ...	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2026-115935	Control panel only API response emulation replaces "sec...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116009	Camaleon CMS before 2.9.3 Path Traversal RCE via Media...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108113	ILIAS before 9.24, 10.12, and 11.5 Unrestricted File Upload ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79880	HPE: Authenticated Server-Side Request Forgery leads to...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114109	uv before 0.11.15 Arbitrary File Write via Entry Point Names	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114107	HKUDS Vibe-Trading 0.1.0 before 0.1.7 Indirect Prompt Inj...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114094	Dulwich before 1.2.9 Arbitrary File Write via DOS drive lett...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34015	Remote Code Execution in upload.php of Video Station	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV (continued)				
CVE-2026-105123	W (wcms) through 3.18.0 RCE and Arbitrary File Write via ...	High / 8.7	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-41544	Path Traversal leading to Arbitrary File Move, Docker Esca...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39993	Path Traversal to Root RCE in QNAP Download Station via ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110761	ILIAS before 9.24, 10.12, and 11.5 PHP Object Injection via ...	High / 8.7	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-110385	CVE-2026-110385: A remote code execution vulnerability...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109397	Thelia before 3.1.2 and 3.2.x before 3.2.1 File Upload RCE ...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104069	HortusFox < 6.2 Remote Code Execution via Theme Import	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104418	Ghost from 6.10.3 before 6.64.0 RCE via Theme Translatio...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-64949	Unrestricted File Upload Leading to Remote Code Executi...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114125	Storybook: Missing origin validation in Storybook preview...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-29001	TastyIgniter 4.4.5 PHP Object Injection via Settings Deser...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54708	Authenticated Remote Code Execution via Path Traversal ...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104077	Obsidian Desktop < 1.14.0 RCE via Slides Plugin Markdown	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105220	Twine 2 Desktop through 2.12.0 Arbitrary Code Execution ...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104805	Mitel MiVoice Office 400 Backup Restoration Arbitrary Fil...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12171	auto-changelog: code execution via untrusted in-reposito...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104078	Obsidian Desktop < 1.14.0 RCE via MathJax Safe Filter By...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104811	Mitel MiVoice Office 400 Music on Hold WAV File Upload ...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104809	Mitel MiVoice Office 400 Shared Object Hijacking Leadin...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114727	CVE-2026-114727: Roundcube Webmail before 1.6.20 and...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV (continued)				
CVE-2026-105858	Payload: Remote Code Execution through first-register	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112852	WordPress Helion theme <= 1.1.12 - PHP Object Injection v...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104747	WordPress Haaken theme <= 1.5 - PHP Object Injection v...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92820	Ninja Forms - File Uploads <= 3.3.34 - Unauthenticated A...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97296	WordPress Gravity Forms plugin < 3.1.1 - PHP Object Injec...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104995	BP Profile Search <= 5.9 - Unauthenticated Local File Incl...	High / 8.1	VULNCHECK KEV	✓ Blocked
CVE-2026-105816	Vault Vulnerable to Arbitrary Code Execution via Plugin C...	High / 8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2025-66275	Remote code execution via command injection	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113356	DokuWiki before 2026-07-14c PHP Object Injection via Dr...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-66272	Arbitrary file deletion and remote code execution	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108159	AstronRPA through 1.1.6 RCE via Smart-Component Chat ...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110874	Dolibarr before 23.0.4 PHP Object Injection via jsonOrUns...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95155	CVE-2026-95155: FasterXML Jackson 1.x, confirmed in j...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92532	Unrestricted Upload of File with Dangerous Type in BugTr...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82627	Uncanny Automator – AI + Automation for WordPress | AI ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81655	Ad Inserter 2.8.12 - 2.8.18 - Subscriber+ RCE / Stored XSS...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105744	Docling: Arbitrary file read/write (and command executio...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103831	Insecure deserialization in the TrueLayer Magento 2 plugin	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111221	Netgate pfSense CE through 2.9.0 Command Injection via...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114145	GitPython validates a submodule's ".git" path only after cl...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV (continued)				
CVE-2026-102143	Kiteworks Email Protection Gateway Unrestricted Upload ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105314	CVE-2026-105314: Papermerge 3.5.3 allows remote code...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-64947	CSRF Bypass Leading to Remote Code Execution via Unr...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111219	Netgate pfSense CE through 2.9.0 Command Injection via...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114724	CVE-2026-114724: Roundcube Webmail before 1.6.20 an...	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91844	Remote Code Execution via Unrestricted File Upload in İz...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109556	EdgeEver Desktop 1.92.0 through 1.112.0 Local Program E...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114098	Dulwich 0.22.5 before 1.2.8 Path Traversal via Stash Pop ...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114097	Dulwich 0.23.1 before 1.2.8 Symlink Path Traversal via filte...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94568	WordPress Pay with Vipps for WooCommerce plugin <= 6...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62044	WordPress Super Video Player plugin <= 1.8.13 - PHP Obj...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94676	WordPress Tainacan plugin <= 1.3.0 - PHP Object Injectio...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104752	Rank Math SEO < 1.0.280 - Admin+ Arbitrary File Upload t...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103348	WordPress WP Ultimate Exporter plugin <= 3.0 - PHP Obj...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93617	WordPress Sunshine Photo Cart plugin <= 3.7.1 - PHP Obj...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105677	Ghost: Remote Code Execution via Theme Translation Files	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104890	Kunstmaan CMS: MediaBundle extension blacklist bypass...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114704	WordPress Relevanssi plugin <= 4.28.4 - PHP Object Inje...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106606	WordPress YITH WooCommerce Affiliates plugin <= 3.31....	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12626	Online Scheduling and Appointment Booking System <= ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV (continued)				
CVE-2026-114624	baserCMS: PHP object injection via unguarded unserializ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76728	Authenticated Server-Side Request Forgery Leading to R...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62130	WordPress WooCommerce Multilingual & Multicurrency p...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105872	WordPress Product Configurator for WooCommerce plugi...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88396	CVE-2026-88396: ApiAdmin v5.0 and before is vulnerabl...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96832	WordPress Content Egg plugin <= 6.3.1 - PHP Object Injec...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94677	WordPress Kadence WooCommerce Email Designer plugi...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96343	WordPress WP ERP plugin <= 1.17.9 - PHP Object Injection...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96344	WordPress eCommerce Product Catalog plugin <= 3.6.0 -...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102454	DigiWin | EasyFlow .NET - Arbitrary File Upload	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94390	WordPress Hide Shipping Method For WooCommerce plu...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102130	Kiteworks Email Protection Gateway Remote Code Execut...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94122	WordPress Responsive Slider Gallery plugin <= 1.5.5 - PH...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102392	WordPress Extra Product Options For WooCommerce | C...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96833	WordPress Ultimate Addons for Contact Form 7 plugin <=...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93771	WordPress Cost of Goods for WooCommerce plugin <= 3...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93651	WordPress Minimum and Maximum Quantity for WooCom...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93624	WordPress Music Player for WooCommerce plugin <= 1.9....	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97256	WordPress Page Builder by SiteOrigin plugin <= 2.36.0 - ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102097	Kiteworks Email Protection Gateway remote code execution	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV (continued)				
CVE-2026-104764	Post Export Import with Media <= 1.17.1 - Authenticated (A...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104734	Kirki <= 6.3.2 - Authenticated (Administrator+) PHP Objec...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79811	HPE: Authenticated SQL Injection allows Remote Code Ex...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100506	WordPress WP Spell Check plugin <= 12.1 - PHP Object In...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103349	WordPress Product Feed PRO for WooCommerce plugin ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97278	WordPress Polylang plugin <= 3.8.9 - PHP Object Injectio...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114720	CVE-2026-114720: Roundcube Webmail before 1.6.20 an...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113403	ArmorX Global Technology | ArmorX Spam - Command In...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102169	Security Advisory 0194	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113386	CVE-2026-113386: Roundcube Webmail before 1.6.20 an...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102168	Security Advisory 0194	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103663	Path Traversal leading to Remote Code Execution in Ollama	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102830	JupyterLab: Cross-site scripting (XSS) in JupyterLab via ...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81344	Frontend Admin by DynamiApps <= 3.29.13 - Admin+ PH...	Medium / 6.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91051	EWWW Image Optimizer 8.6.0 - 8.7.7 - Author+ PHP Obje...	Medium / 6.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85015	Unlimited Elements For Elementor < 2.0.21 - Authenticate...	Medium / 6.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86828	BackWPup < 5.7.7 - Admin+ Path Traversal to RCE via Res...	Medium / 6.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57491	FileRise: ZIP extraction writes blocked file extensions to d...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102136	Kiteworks Core Command Execution through Configurati...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104905	FacturaScripts < 2026.7 PHP Object Injection via WidgetS...	Medium / 6.1	PUBLIC EXPLOIT/POC	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV (continued)				
CVE-2026-104843	uv: Path traversal on Windows through wheel extraction	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76147	Genians, Inc Genian NAC/ZTNA Remote Code Execution	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102938	virtualenv writes prompt values into pyvenv.cfg without s...	Medium / 5.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113472	Depicter 4.0.5 - 4.8.1 - Editor+ Arbitrary File Upload via M...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108932	Netcore NR268 DHCP Hostname filter_hosts_dump.cgi e...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105708	imgproxy SVG svg.go sanitizeElement cross site scripting	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105705	SourceCodester Drug Recommendation System add_dru...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105291	feelec-yishu feelcrm-os Department Search Endpoint Gr...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100877	mathurvishal CloudClassroom-PHP-Project registrationfo...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100695	Adminer before 6.0.2 XSS via CONNECTION_ID escalatin...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108931	Netcore NR268 DHCP dhcp_dynamicip_show.cgi eval cro...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
GHSA-86XP-94PG-8R6R	Microsoft Security Advisory CVE-2026-92707 - ASP.NET...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100313	mathurvishal CloudClassroom-PHP-Project updatequery....	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111877	dext34-morgan Books4Cash search.php cross site script...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116047	Privoce Vocechat Query Parameter widget.html cross site...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113741	itsourcecode Online Cake Ordering System 404.php cros...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105288	feelec-yishu feelcrm-os Crm Endpoint functions.php ind...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115982	phpIPAM Rack Link Creation show-rack-popup.php creat...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112092	subhajitkhan online-clinic-management-system Doctor R...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113383	Optimal IdM OptimalCloud Login cross site scripting	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV (continued)				
CVE-2026-108920	SourceCodester Drug Recommendation System Admin R...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108834	Cairo-dock Glx-Dock Query Parameter ww_page.php cro...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105809	SourceCodester Simple Student Information System Profi...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108919	SourceCodester Drug Recommendation System Student ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115534	gedelumbung HospitalManagement Contact Form contac...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115536	gedelumbung HospitalManagement Admin Routing routin...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112093	subhajitkhan online-clinic-management-system feedback...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111987	AUTOMATIC1111 stable-diffusion-webui Extra-Networks ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112247	Wuxi Wubang Security Software Five-in-One Safety Prod...	Medium / 5.3	VULNCHECK KEV	✓ Blocked
CVE-2026-111942	hrisikeshpal Blood_Bank_Management_System abs.php c...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111984	AUTOMATIC1111 stable-diffusion-webui Card Builder ui_e...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104612	SourceCodester Student Result Management System An...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115246	subhajitkhan online-clinic-management-system patdocm...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102264	mwasikz robo-cafe-rms Edit Profile Feature update-acco...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101141	Eleveo Call Recording Software Play Audio audio.jsp cros...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100904	amirsanni mini-inventory-and-sales-management-syste...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112031	Chamilo LMS Ticket TicketManager.php addProject cross...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112096	SourceCodester Inventory System Purchase Records tran...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112097	SourceCodester Inventory System Sales Management tra...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112095	SourceCodester Inventory System Product Management ...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV (continued)				
CVE-2026-116004	onyx-dot-app Onyx PreviewTab.tsx cross site scripting	Medium / 5.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-108898	Netis WF2409E Wireless Settings cross site scripting	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105289	feelec-yishu feelcrm-os Create Customer Endpoint CrmD...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108802	y_project RuoYi Dictionary Data Drawer Preview add rend...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108815	idcCMS member_deal.php cross site scripting	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100880	zhistaredu StarTraining Upload Endpoint MimeTypeUtils.j...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97896	krayin laravel-crm Upload Functionality ConfigurationFor...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100311	mathurvishal CloudClassroom-PHP-Project Faculty Video...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108566	InstantSoft icms2 Private Message index.tpl.php index cr...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112042	diem-project diem dmWidget dmBaseLinkTag.php text cr...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108942	philz1337x clarity-upscaler Extra Networks Card Renderi...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105099	Omega Solution CoinEx Crypto Ticket Attachment Upload...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105173	code-projects Human Resource Management Event Creat...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103686	rhukster dom-sanitizer URL Validation DOMSanitizer.php ...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105950	getformwork URI Sanitizer DomSanitizer.php sanitizeNod...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105808	SourceCodester Simple Student Information System sear...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105188	code-projects Human Resource Management System Liv...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97246	WordPress ShortPixel Image Optimizer plugin <= 6.5.5 - P...	Medium / 4.9	VULNCHECK KEV	✓ Blocked
CVE-2026-115981	phpIPAM index.php cross site scripting	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108936	Edimax BR-6208AC QoS Page formQoS cross site scripting	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV (continued)				
CVE-2026-112249	grandnode grandnode2 Product Description Product.Lay...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108934	Edimax BR-6208AC HTTP Blocking formUrlb cross site s...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108908	Netcore NR268 Web UI I7_call_board_user_set.cgi eval cr...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108933	Edimax BR-6208AC formFilter cross site scripting	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108935	Edimax BR-6208AC Port Forwarding formPortFw cross si...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116148	ImageMagick before 6.9.13-58 and 7.x before 7.1.2-33 Co...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115535	gedelumbung HospitalManagement Settings sistem.php s...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112038	diem-project diem Version Check Service dmAdminCtrl.j...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112039	diem-project diem Administrative Console actions.class.p...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86841	Bookly 23.2 - 28.2 - Bookly Administrator+ PHP Object Inj...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115785	Zimbra Collaboration Suite Data Source Test SMTP Comm...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102847	gedelumbung HospitalManagement Guest Book buku_ta...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102292	coolbeans1212 MateisHomePage-Website users.php cros...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102137	Kiteworks Core Unrestricted Upload of File with Dangero...	Medium / 4.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102290	CodeCanyon Rocket LMS Student Profile Image Upload c...	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97897	Krayin laravel-crm TinyMCE Media Upload Sanitizer.php c...	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100882	Krayin laravel-crm Admin Settings Endpoint index.blade.p...	Low / 2.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111628	10up Distributor before 2.3.2 PHP Object Injection via set_...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100881	zhistaredu StarTraining application.yml cross site scripting	Low / 2.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108827	Zen Cart Administrative Module Management general.ph...	Low / 2.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Remote Code Execution: 389 blocked · avg CVSS 8.0 · 3 CISA KEV (continued)				
CVE-2026-90799	Apache CouchDB: Atom-table exhaustion in _changes se...	Low / 1.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115560	PHP Informational advisory: Session upload progress (CV...	Unscored	PUBLIC EXPLOIT/POC	✓ Blocked
SSRF: 335 blocked · avg CVSS 6.4 · 2 CISA KEV				
CVE-2026-89111	OAuth2 SSRF vulnerability in SAP Cloud SDK for Python	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106622	ColdFusion | Server-Side Request Forgery (SSRF) (CWE-...	Critical / 10	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-102255	CVE-2026-102255: A Pre-authentication SSRF vulnerabili...	Critical / 10	VULNCHECK KEV	✓ Blocked
CVE-2026-77524	KEDA: Privilege escalation from namespace admin to clus...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105636	Plane: SSRF via HTTP redirect in webhook delivery (allow...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-46651	Unauthenticated SSRF and local file inclusion via Downloa...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69435	Azure SRE Agent Elevation of Privilege Vulnerability	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110628	Kan 0.5.5 through 0.6.0 Unauthenticated SSRF via /api/do...	Critical / 9.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-111663	Chaskiq through 2.0.3 SSRF via createUrlUpload GraphQ...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109238	Crawl4AI 0.7.0 before 0.9.4 SSRF via link_preview_config ...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114493	LocalAI v4.6.0 through v4.11.0 SSRF Guard Bypass via HT...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107460	Apache Fesod (Incubating): UrlImageConverter SSRF prot...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107781	Dromara Skyeye Unauthenticated SSRF and File Overwrit...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102105	Kiteworks Email Protection Gateway server-side request f...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102103	Kiteworks Email Protection Gateway server-side request f...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102104	Kiteworks Email Protection Gateway server-side request f...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 335 blocked · avg CVSS 6.4 · 2 CISA KEV (continued)				
CVE-2026-102102	Kiteworks Email Protection Gateway server-side request f...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102095	Kiteworks Email Protection Gateway server-side request f...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100567	OpenClaw before 2026.8.1 DNS Rebinding via CDP Hostn...	High / 8.9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-92222	Joomla! Core - [20260909] - Core - SSRF vectors in vario...	High / 8.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115729	@pdfme/common 5.5.10 before 6.2.6 SSRF via isUrlSafeT...	High / 8.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116176	vLLM 0.9.2 before 0.24.0 SSRF via X-Request-Id in P2pN...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104464	YesWiki before 4.6.7 SSRF via Bazar abonnements sync a...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18660	Jetty proxy blacklist performs case-sensitive matching of...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92931	CWE-918: Server-Side Request Forgery in the Progress Si...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100391	MediaFlow Proxy through 2.4.9 Server-Side Request Forg...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108357	PhpSpreadsheet: XmlScanner Bypass via Double-Encode...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108358	PhpSpreadsheet: XmlScanner Bypass via ISO-2022 Esca...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57143	PraisonAI: Server-Side Request Forgery (SSRF) in SearxN...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2023-54402	iDocView SSRF via /doc/upload Endpoint Hardcoded Token	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2026-104817	Misskey: Lack of rate limiting and size restrictions in RSS f...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-19678	Server-Side Request Forgery (SSRF) Leading to Internal S...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109430	Ellucian WebAdvisor 3.2 Unauthenticated XXE Injection	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54668	Kitodo.Production: XXE in XMLUtils EAD/XML upload par...	High / 8.7	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2020-37278	Weaver e-Bridge Unauthenticated Arbitrary File Read via ...	High / 8.7	VULNCHECK KEV	✓ Blocked
CVE-2026-104976	Plane: SSRF in Gitea OAuth	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 335 blocked · avg CVSS 6.4 · 2 CISA KEV (continued)				
CVE-2026-65101	CVE-2026-65101: NVIDIA AIStore for Linux contains a vul...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-65170	CVE-2026-65170: NVIDIA AIStore for Linux contains a vul...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105897	ColdFusion | Server-Side Request Forgery (SSRF) (CWE-...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95634	CAI Content Credentials | Server-Side Request Forgery (S...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55103	Discourse ActivityPub: Fix inbound actor validation and a...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34634	ColdFusion | Server-Side Request Forgery (SSRF) (CWE-...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100697	Adminer 6.0.0 Server-Side Request Forgery via ClickHou...	High / 8.6	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-85951	Server-side request forgery in Progress MarkLogic Serve...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106459	Backstage: Improper input validation in Sentry scaffolder ...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85952	Server-side request forgery in Progress MarkLogic Serve...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100750	Joomla Extension - regularlabs.com - Arbitrary file read / ...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110255	Dockhand before 1.0.43 SSRF via /api/templates/compos...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101060	python-utcp before 1.1.4 SSRF via unvalidated HTTP redir...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86671	CVE-2026-86671: In Eclipse Che versions 7.29.0 and later...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110868	Renovate before 44.79.0 SSRF via HTTP Preset URLs and ...	High / 8.4	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-100705	Kyverno before 1.19.1 SSRF via legacy apiCall service exec...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104463	YesWiki before 4.6.7 Unauthenticated SSRF via ActivityPu...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101064	Obot before v0.23.0 Server-Side Request Forgery via MCP	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105762	Dify: Unauthenticated Server-Side Request Forgery in /co...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103757	Budibase before 3.41.0 SSRF via uploadUrl in AI Table Ge...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked

INDUSFACE™ ©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 335 blocked · avg CVSS 6.4 · 2 CISA KEV (continued)				
CVE-2026-112308	crewai-tools through 1.15.28 SSRF via SeleniumScrapingT...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94483	Next.js has Server-Side Request Forgery in Image Optimi...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104458	YesWiki before 4.6.7 SSRF Guard Bypass via IPv6 Transiti...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103958	Server-side request forgery in the tool server and remote ...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110718	TurboDocx html-to-docx through 1.23.1 SSRF via img src ...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-61586	Copernik XML Factory (stock JDK provider) has Improper...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116192	rclone from 1.37 before 1.74.2 SSRF via --rc-serve schem...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-80344	Apache Camel: Camel-AS2 Server-Side Request Forgery ...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
GHSA-X8GV-G2G3-65FJ	SiYuan Agent Tools SSRF via DNS-Rebinding TOCTOU (B...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89430	Gitea push mirror SSRF and forced writes to internal Git h...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92287	Apache Arrow C++, PyArrow: Parquet file-controlled KM...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105941	Kroxylicious-kms-provider-azure-key-vault-kms: stream...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92204	Airbyte OneDrive Connector _get_shared_drive_object Se...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59970	Tandoor Recipes: Blind SSRF via AI provider URL (api_base)	High / 7.7	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-106455	Backstage: Improper validation of MkDocs plugin configu...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106557	Backstage: Improper input validation in TechDocs Markdo...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78024	CVE-2026-78024: Dell Secure Connect Gateway (SCG) P...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106498	Backstage: Improper URL validation in catalog entity plac...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34633	ColdFusion | Server-Side Request Forgery (SSRF) (CWE-...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108456	Azure AI Foundry Elevation of Privilege Vulnerability	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 335 blocked · avg CVSS 6.4 · 2 CISA KEV (continued)				
CVE-2026-92203	Airbyte SharePoint Connector _get_shared_drive_object S...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75888	Openshift/console: openshift/console: authenticated ssrf ...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104977	Plane: Incomplete fix of CVE-2026-27706 — SSRF still re...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101027	Gitea migration SSRF through ALLOWED_DOMAINS addr...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
GHSA-XXV7-2VV3-H682	Trigger.dev: Server-side request forgery via unvalidated ...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105628	Plane: OAuth Avatar Redirect SSRF Leads to Internal Data ...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55177	CloudTAK: Authenticated full-read SSRF in /api/esri* rout...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104973	Plane: DNS Rebinding Bypass of CVE-2026-30242 SSRF ...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75748	ColdFusion | Server-Side Request Forgery (SSRF) (CWE-...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55232	Vvveb: Server-side request forgery in Vvveb via IPv6 byp...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95265	CVE-2026-95265: Feehi CMS 2.1.1 contains a Server-Sid...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113728	Bulwark Webmail: DNS-rebinding SSRF in public iCalenda...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102091	Kiteworks Secure Data Forms server-side request forgery	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108086	Apache Cocoon: XEE could lead to SSRF and information ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70251	Microsoft Office SharePoint Elevation of Privilege Vulnera...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88206	Microsoft Office SharePoint Elevation of Privilege Vulnera...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70202	Microsoft Office SharePoint Elevation of Privilege Vulnera...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85963	Server-side request forgery and hard-coded key in Progr...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56661	GetSimple CMS: Server-Side Request Forgery in the Upd...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70357	Gitea repository migration SSRF through DNS rebinding	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 335 blocked · avg CVSS 6.4 · 2 CISA KEV (continued)				
CVE-2026-104636	Gitea SSRF through Git HTTP redirects in mirrors and fetc...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102267	PyJWT: PyJWKClient follows redirects when fetching JW...	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82375	Apache Roller: Server-side request forgery via entry track...	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-3712	PhastPress <= 3.10 - Unauthenticated Server-Side Reque...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92210	NoMachine nxhtd Server-Side Request Forgery Informati...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57114	PraisonAI: Jobs webhook SSRF protection bypass via DN...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-27350	WordPress Builderius plugin <= 1.4-beta - Server Side Re...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-20362	Cisco Finesse Server-Side Request Forgery Vulnerability	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62030	WordPress StreamCast plugin <= 2.4.5 - Server Side Req...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114730	CVE-2026-114730: Roundcube Webmail 1.6.14 before 1.6....	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39719	WordPress PDF Smart Viewer for Elementor plugin <= 1.0....	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39728	WordPress Instapage Plugin plugin <= 3.7.2 - Server Side ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103082	WordPress LA-Studio Element Kit for Elementor plugin <=...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111313	JobOps through 0.13.1 SSRF via POST /api/manual-jobs/fe...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101300	Server-Side Request Forgery in Wegow PDF export	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55787	Flyto2 Core: SSRF guard bypass via IPv6 transition addre...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76001	ColdFusion | Server-Side Request Forgery (SSRF) (CWE-...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107362	Server-Side Request Forgery in Malcolm	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100849	AzuraCast before 0.23.8 SSRF Filter Bypass via Hostnam...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101059	utcp-http before 1.1.4 OAuth2 tokenUrl Trust Boundary By...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked

INDUSFACE™ ©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 335 blocked · avg CVSS 6.4 · 2 CISA KEV (continued)				
CVE-2026-55096	SSRF via DNS-resolution gap in _validate_url_security (file...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100555	OpenClaw before 2026.8.1 DNS Rebinding via attachment ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100848	AzuraCast before 0.23.8 Server-Side Request Forgery via...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110220	Kubeflow Model Registry through 0.3.17 SSRF via Inferen...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116066	Firecrawl before 2.11.586 SSRF Protection Bypass via DN...	High / 7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101907	Axios: maxRedirects: 0 is not enforced by the fetch adapt...	High / 7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101898	Axios: HTTP/2 adapter bypasses configured DNS lookup ...	High / 7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101910	ip-address: no classifier recognizes the NAT64 local-use ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102722	CVE-2026-102722: In the IPv4 PASV path, the FTP Client ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103530	decolua 9Router Search Endpoint ssrfGuard.js fetch serv...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112237	Server-Side Request Forgery in extension "Kitodo.Presen...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113704	a2aproject a2a-rs Push Notification push_notification_sen...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116205	YesWiki before 4.7.0 Unauthenticated SSRF via [[|URL]] R...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116069	NiubiGEO before 0.3.2 Unauthenticated SSRF via /audit-pl...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103243	LightLLM through 1.2.0 Server-Side Request Forgery via ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114062	SvelteKit before 3.0.0 SSRF via Redirects in Server-Side S...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112267	SGLang through 0.5.22 SSRF via bootstrap_host and boot...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111720	fish-island-backend through commit 7c61b78 SSRF via /a...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111320	ValueCell through 0.1.20 Unauthenticated SSRF via /api/v...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109405	conductor-oss conductor KafkaPublishTask.java KafkaPu...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 335 blocked · avg CVSS 6.4 · 2 CISA KEV (continued)				
CVE-2026-105290	feelec-yishu feelcrm-os getCurlData Endpoint GoogleCo...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110222	Razorpay IFSC Ruby gem through 2.0.62 SSRF via IFSC lo...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87890	Potential request forgery via spatial lookup byte values	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104440	YesWiki before 4.6.7 Blind SSRF via bazarlist API idtypean...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111210	bitcoinj Payment Request PaymentSession.java url.openC...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105238	ChatGPTNextWeb NextChat Proxy Fallback proxy.ts prox...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111323	RedAmon through 7.0.1 Unauthenticated SSRF via /tradecr...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105148	SciPhi-AI R2R Retrieval Completion API Endpoint llm.py s...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100251	Wormhole.app SSRF	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104120	modelcontextprotocol mcp-server-fetch/mcp-server-ev...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104441	YesWiki before 4.6.7 Unauthenticated SSRF via valeur Act...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104459	YesWiki before 4.6.7 SSRF via ActivityPub WebFinger act...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104442	YesWiki before 4.6.7 Unauthenticated SSRF via syndicatio...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111662	Chaskiq through 2.0.3 Unauthenticated SSRF via /oembe...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108836	Ollama Pull API name.go IsValid server-side request forgery	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108770	Appwrite Browser Screenshot Service Get.php PublicHos...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109239	Crawl4AI before 0.9.4 Blind SSRF via RobotsParser.can_f...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108939	EricLBuehler mistral.rs media_source.rs is_global_ip serv...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107207	LMCache through 0.5.5 Missing Authentication in Fronten...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108554	PDFMathTranslate through 1.9.11 SSRF via Gradio Web GU...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 335 blocked · avg CVSS 6.4 · 2 CISA KEV (continued)				
CVE-2026-109403	conductor-oss conductor Agent Card Fetching A2AServi...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109404	conductor-oss conductor Agentspan Agent Runtime Age...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108850	Company Research Agent through 2.2.0 SSRF via /genera...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116000	Zylon PrivateGPT URI Artifact Loader uri_loader.py load_fi...	Medium / 6.9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-101058	python-utcp before 1.1.12 SSRF via Remote HTTP Manual	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101005	October CMS SSRF Protection ResizeImages.php validate...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100893	Privoce VoceChat Server open_graphic_parse Endpoint r...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100901	athlon1600 youtube-downloader stream.php stream serv...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100909	OctoberCMS ResizeImages.php getSourcePathForResize...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100696	Adminer before 6.0.2 Unauthenticated SSRF via Elasticse...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100858	heym before 0.0.109 Server-Side Request Forgery via Wo...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102354	BentoPDF: SSRF via DNS Rebinding (TOCTOU) in Cloudfl...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107394	Indico: Incomplete Server-Side Request Forgery (SSRF) c...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107289	Pydantic AI: SSRF cloud-metadata blocklist bypass via IPv...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55385	InvoiceShelf: SSRF via unvalidated Gotenberg PDF render...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102145	Kiteworks Core Server-Side Request Forgery through CR...	Medium / 6.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55190	Event Schedule Vulnerable to SSRF: isUrlSafe() bypassabl...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100859	Heym before 0.0.106 Credential Exfiltration via URL Overri...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2024-34319	CVE-2024-34319: A Server-Side Request Forgery (SSRF)...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93693	Unauthenticated queue manipulation through connector ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 335 blocked · avg CVSS 6.4 · 2 CISA KEV (continued)				
CVE-2026-76274	Cisco: Server-Side Request Forgery (SSRF) through the R...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-17557	Lm-evaluation-harness: lm-evaluation-harness: ssrf via j...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108764	Apache Kylin: job-driver UI proxy SSRF	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96204	Azure Arc Elevation of Privilege Vulnerability	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70259	Microsoft Office SharePoint Information Disclosure Vulne...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100279	CVE-2026-100279: In JetBrains YouTrack before 2026.2.1...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85471	Quay: quay: webhook notification ssrf -- hostname-string...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-28329	SolarWinds Observability Self-Hosted Server-Side Reque...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102797	WordPress ThemeREX Addons plugin <= 2.46.0 - Server ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105790	Microsoft UFO: Authenticated Galaxy device registration ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108360	PhpSpreadsheet: SSRF whitelist bypass via unre-validate...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101913	ip-address: Address6.isLinkLocal() recognizes fe80::/64 ...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110652	ONLYOFFICE DocumentServer before 10.0.0 SSRF via do...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82044	UTMStack < 11.2.16 Server-Side Request Forgery via dow...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94621	AliasVault: Server-Side Request Forgery via DNS rebindin...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112991	MISP html_to_markdown Module SSRF via Incomplete IP ...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102983	Astro: Netlify Image CDN allowlist bypass enables SSRF	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112076	alexta69 MeTube Feed-metadata Thumbnail Fetch ytdl.py...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111171	Web3.py 7.15.0 through 7.16.0 and 8.0.0b2 through 8.0.0 C...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93294	Azure Monitor data source resource proxy allows calls to ...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 335 blocked · avg CVSS 6.4 · 2 CISA KEV (continued)				
CVE-2026-102777	Joomla Extension - svenbluege.de - Server-side request ...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110240	Lancet through 2.3.9 SSRF Protection Bypass via netutil.I...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100681	Budibase before 3.45.0 SSRF and OAuth Token Exfiltratio...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115751	mcp-from-openapi 2.2.0 before 2.9.0 SSRF blockedHosts...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115810	Tandoor Recipes before 2.7.0 SSRF via Pestle Importer Im...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105689	Penpot: SSRF guard bypass via IPv6 transition addresses ...	Medium / 6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78163	Apache Camel: Camel-Docling Unvalidated Message Bod...	Medium / 5.9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-105750	Docling: `enable_local_fetch` is not enforced in HTML bro...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100574	OpenClaw before 2026.8.1 SSRF via Trusted-Host DNS	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96533	Testimonials Widget <= 4.0.4 - Unauthenticated SSRF via ...	Medium / 5.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97316	Broken Link Notifier 1.3.1 - 2.0.0 - Unauthenticated SSRF v...	Medium / 5.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111761	A2A Java SDK has Server-Side Request Forgery (SSRF) i...	Medium / 5.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114609	fpdf2 implicitly loads external URLs and local image paths...	Medium / 5.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78027	CVE-2026-78027: Dell Secure Connect Gateway (SCG) P...	Medium / 5.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100698	Adminer before 6.0.2 Privileged-Port SSRF via host_port ...	Medium / 5.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105713	Microsoft Office SharePoint Spoofing Vulnerability	Medium / 5.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103497	CVE-2026-103497: In JetBrains YouTrack before 2026.2.1...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73599	CVE-2026-73599: Dell Secure Connect Gateway (SCG) P...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114620	Authlib: Unvalidated request_uri fetch in JWT-secured aut...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102923	SparkyFitness: SSRF via unvalidated custom_url in AI serv...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 335 blocked · avg CVSS 6.4 · 2 CISA KEV (continued)				
CVE-2026-104470	YesWiki before 4.6.7 SSRF via Bazar valeur Action url Para...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100576	OpenClaw before 2026.8.1 SSRF via Browser Wait Predica...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111936	Sigma File Manager through 2.2.0 SSRF via Extension Do...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111899	KitchenOwl through 0.7.10 SSRF via Recipe Import scrape...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63045	Apache HTTP Server: mod_proxy_ftp PASV address handl...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101883	OpenClaw Windows Node through 2026.9.4 SSRF via can...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114362	HarnessRouter Targets Test Endpoint app.py server-side ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114074	Trigger.dev before 4.5.10 Webhook SSRF Protection Bypa...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114076	Trigger.dev before 4.5.2 Blind SSRF via Alert Channel We...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114080	Trigger.dev before 4.5.2 Blind SSRF via Alert-Channel We...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114634	WWBN AVideo before 29.4.0 Blind SSRF via getHeaderC...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114374	leomoon-studios wiki-go fetch-metadata Endpoint metad...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108523	Studio-Saelix Sencho git-sources Browse API Endpoint o...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115411	crawlseo before 0.2.4 Server-Side Request Forgery via C...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101048	Cloudreve before 4.17.0 SSRF via Admin.Read OAuth scope	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100577	OpenClaw before 2026.8.1 Server-Side Request Forgery ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100601	ClawHub SSRF via Unchecked DNS Resolution in Profile I...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100861	heym before 0.0.105 SSRF via credential-controlled base ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108542	021is elvix-sdk MCP Request index.ts server-side reques...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108572	Casdoor Proxy Validation cas.go CasP3ProxyValidate ser...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked

INDUSFACE™ ©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 335 blocked · avg CVSS 6.4 · 2 CISA KEV (continued)				
CVE-2026-108735	Miniflux 2.3.0 through 2.3.3 SSRF via Per-Feed Proxy URL	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108719	LLMGateway through 1.20.0 Blind SSRF via Video-Genera...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116056	KodCloud KodExplorer Remote Download web.function.p...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96655	Plex Media Server arbitrary-host SSRF	Medium / 5.3	CISA KEV	✓ Blocked
CVE-2026-96652	Plex Media Server SSRF	Medium / 5.3	CISA KEV	✓ Blocked
CVE-2026-112299	smrealms smr Album Website AlbumEditProcessor.php is...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116182	phpMyFAQ before 4.1.10 SSRF via PDF Export Image Fetc...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112254	agit8or1 clientst0r Property URL Importer property_url_im...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109190	conductor-oss conductor API Tool Configuration ListApiT...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109189	fit2cloud MeterSphere Swagger3 Swagger3ParserApiDef...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55414	NL Portal Backend Libraries: Unauthenticated form resolv...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111321	TaskingAI through 0.3.0 SSRF via OpenAPI servers[0].url ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112297	ptbsare anx-calibre-manager LLM Configuration llm.py LL...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78231	Gitea blind SSRF through OpenID assertion verification	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110100	Jorani before 1.0.4 Missing Authorization and SSRF via Co...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100348	kin-openapi spec loader panics on a self-referential additi...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39989	SSRF in QNAP Download Station	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100297	Server-Side request forgery (SSRF) in Anjvision YSSD-RT...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105438	O2OA General url ActionUploadExcelWithUrl server-side ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109402	conductor-oss conductor MCP Service MCPService.java ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 335 blocked · avg CVSS 6.4 · 2 CISA KEV (continued)				
CVE-2026-76286	Cisco: Server-Side Request Forgery (SSRF) through Cust...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108602	Helicone through v2025.08.21-1 SSRF via Jawn Webhook...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103542	formtools.org Form Tools AJAX Endpoint actions.php sm...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103291	Ghost 3.20.2 before 6.51.0 SSRF via image-size fetch	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110254	Dockhand before 1.0.45 SSRF via IPv6 Transition Address...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107698	FFmpeg before 7.1.4 and 8.0.2 SSRF via RTSP Redirect Ha...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108702	CordysCRM through 1.9.3 Missing Authorization and Blin...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109651	Frappe ERPNext before 15.112.0 Server-Side Request For...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109200	LogicalDOC Community Edition through 9.3 SSRF via XM...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101022	Grid Protection Alliance openPDC and openHistorian Serv...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107273	Gophish 0.11.0 through 0.12.1 SSRF via POST /api/import/s...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109378	SPIP before 4.4.18 SSRF via HTTP Redirects in recuperer_...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108787	houtini-ai voice-analyser-mcp collect_corpus crawler.ts f...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108786	houtini-ai seo-crawler-mcp Crawler CrawlOrchestrator.ts ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105122	OpenAM before 16.1.3 SSRF via OpenID Connect Client jw...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110610	ruoyi-vue-pro through 2026.09 SSRF via Midjourney refe...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82040	UTMStack < 11.2.16 SSRF via IdentityProviderService	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-25946	Gitea OpenID discovery server-side request forgery	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101893	Newell Brands DYMO ID document parsing failing file typ...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103287	Ghost 1.18.0 before 6.27.0 Server-Side Request Forgery vi...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 335 blocked · avg CVSS 6.4 · 2 CISA KEV (continued)				
CVE-2026-101150	Security Advisory 0186	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110225	Shaarli through 0.16.9 SSRF via Thumbnail Retrieval updat...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107597	jwks_uri from the OIDC discovery document is fetched wi...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100900	DevaslanPHP project-management Jira Import jira-import...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108521	Studio-Saelix Sencho Add Remote Node API Endpoint vali...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114064	Snipe-IT before 8.7.0 SSRF Port Scanning via Webhook T...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105263	Shaarli Admin Metadata Endpoint MetadataController.php...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101149	Security Advisory 0186	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100373	OpenMetadata through 2.0.2 SSRF via Webhook URL Vali...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100863	Heym before 0.0.91 SSRF via image fetching and IPv6 vali...	Medium / 5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102879	ClaraVerse through 0.3.1 SSRF Protection Bypass	Medium / 5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106470	WP Data Access < 5.5.88 - Subscriber+ SSRF	Medium / 5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14521	IBM DataPower Gateway affected by server-side request ...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-80464	API Tool Runner SSRF in HAVELSAN's Sef - AI Chatbot Pl...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76083	Redash: JSON data source query URL can bypass base U...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109603	Frappe Framework before 16.17.0 Authenticated SSRF and...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109682	Metasploit Framework HTTP Redirect Server-Side Reque...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101061	utcp-gql and utcp-websocket before 1.1.1 SSRF via URL va...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109681	Metasploit Framework FTP PASV Response SSRF	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102877	Fider before 0.38.0 SSRF via DNS rebinding in webhook v...	Medium / 4.4	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 335 blocked · avg CVSS 6.4 · 2 CISA KEV (continued)				
CVE-2026-96400	Gitea migration SSRF to reserved addresses through ALL...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101029	Gitea migration and pull mirror SSRF through multi-answe...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113671	ApostropheCMS: Host header controls server-side image...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55875	Helium: SSRF via External Calendar URL Allows Authentic...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101087	Nezha 2.0.10 through 2.3.2 SSRF Denylist Bypass IPv6	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100257	CVE-2026-100257: In JetBrains YouTrack before 2026.2.1...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102244	MODSetter SurfSense Document Export Feature editor_r...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102577	Moodle: ssrf risk in url downloader via ipv4-mapped ipv6 ...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84224	Kirki < 6.3.2 - Editor+ Blind SSRF via Remote Template URL	Medium / 4.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85345	FV Player 7.5.44.7212 - 7.5.54.7212 - Contributor+ SSRF vi...	Medium / 4.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89003	WPeMatico RSS Feed Fetcher < 2.8.27 - Contributor+ SS...	Medium / 4.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89000	WPeMatico RSS Feed Fetcher < 2.8.27 - Contributor+ SS...	Medium / 4.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97354	PowerPress 11.13.12 - 11.17.9 - Contributor+ SSRF via Medi...	Medium / 4.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105048	CVE-2026-105048: The Playground feature of Zilliz Attu b...	Medium / 4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105301	Keycloak-services: keycloak-services: blind ssrf via x.50...	Medium / 4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105743	Docling: SSRF guard bypass in remote resource fetching (...	Medium / 4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93694	Untrusted request routing and forged acknowledgements...	Medium / 4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107288	Pydantic AI: web_fetch_tool blocked_domains bypass via ...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105800	i18next-http-backend incomplete URL validation permits ...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100104	Server-Side Request Forgery (SSRF) in GitLab	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 335 blocked · avg CVSS 6.4 · 2 CISA KEV (continued)				
CVE-2026-107449	CVE-2026-107449: linuxserver Heimdall through 2.8.3 ap...	Low / 3.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102138	Kiteworks Core Server-Side Request Forgery (SSRF)	Low / 3.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83813	Twisted: DNS Response Spoofing in twisted.names Due t...	Low / 3.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101057	utcp-mcp before 1.1.3 SSRF via unvalidated MCP server U...	Low / 3.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105682	Ghost: Server-Side Request Forgery in Webhook Trigger	Low / 2.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110805	CVE-2026-110805: Server-side request forgery in PingO...	Low / 2.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110223	Kavita 0.9.0 through 0.9.1.4 SSRF Blocklist Bypass via upl...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115752	Signal K Server 2.28.0-beta.2 before 2.34.0 SSRF via App...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108741	Shepherd through 0.3.1 SSRF via DNS Rebinding in Citatio...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108594	Mealie 3.26.0 through 3.28.0 SSRF via OIDC Picture Claim...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57569	Lychee: Distinct post-fix SSRF variant in Photo::fromUrl d...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108115	Kortix Suna 0.10.7 before 0.13.52 SSRF Guard Bypass via I...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108583	zotero-mcp 0.10.0 through 0.14.1 SSRF via zotero_add_by_...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105214	Zitadel before 4.16.2 SSRF via Organization Domain HTTP ...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115364	OpenBao before 2.6.3 Missing Header Check on Agent/Pr...	Low / 2.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112288	Krayin CRM 2.2.5 before 2.2.7 SSRF Filter Bypass via DNS...	Low / 2.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112358	TiBillet Lespass APIv1 serializers.py get_img_from_url ser...	Low / 2.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-0311	Checkov by Prisma Cloud: Server-Side Request Forgery ...	Low / 1.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69137	[webapps] SuiteCRM 8.10.1 - Authenticated SSRF	Unscored	PUBLIC EXPLOIT/POC	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Uncontrolled Resource Consumption: 260 blocked · avg CVSS 6.9 · 2 CISA KEV				
CVE-2026-101501	CVE-2026-101501: Vulnerability in Oracle Trusted Answer...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-16438	An arbitrary operation vulnerability in GENESIS64, ICONIC...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101980	Junos OS: Malformed Extended Echo requests cause a R...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112779	Grav API Plugin before 1.0.42 Cache Exhaustion and Page...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15176	NGINX ngx_http_core_module vulnerability	Critical / 9.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-93479	NGINX map directive and regex matching vulnerability	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97205	NGINX ngx_http_core_module vulnerability	Critical / 9.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-101634	CVE-2026-101634: Vulnerability in the Oracle Mobile Fiel...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91341	CVE-2026-91341: Vulnerability in the Oracle Outside In Te...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91225	CVE-2026-91225: Vulnerability in the Oracle SOA Suite pr...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91655	CVE-2026-91655: Vulnerability in Oracle Essbase (comp...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91656	CVE-2026-91656: Vulnerability in Oracle Essbase (comp...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88775	Memory overflow vulnerability leading to unpredictable or...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88777	Memory overflow vulnerability leading to unpredictable or...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88776	Memory overflow vulnerability leading to unpredictable or...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-106104	Quasar Framework: Super-linear regex backtracking on U...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105830	league/commonmark 2.0.0 before 2.10.2 Quadratic DoS vi...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88779	Memory overflow vulnerability leading to Denial of Service	High / 8.7	CISA KEV	✓ Blocked
CVE-2026-66858	Apache Thrift, Apache Thrift, Apache Thrift, Apache Thrif...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111901	phpMyFAQ 4.2.0-alpha before 4.2.0-beta Unauthenticate...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Uncontrolled Resource Consumption: 260 blocked · avg CVSS 6.9 · 2 CISA KEV (continued)				
CVE-2026-86535	Apache Thrift: A JSON member name can stall the Node s...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116011	Crow before 1.3.4 Denial of Service via Deeply Nested JS...	High / 8.7	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-91184	NGINX Gateway Fabric vulnerability	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112782	Grav before 1.7.53.5 and 2.2.2 Image Pixel Limit Bypass D...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94197	NGINX Ingress Controller vulnerability	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101895	Angular SSR: Denial of Service (DoS) via Infinite Loop on ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104150	AdonisJS HTTP Server: Uncontrolled Resource Consump...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91137	Apache Thrift: PHP `thrift_protocol` accelerator: zero-byt...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111810	Apache Traffic Server: Unthrottled per-header diagnostic ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102475	CVE-2026-102475: In Eclipse Vert.x versions [5.0.0,5.0.12...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97334	Network messaging layer decompression resource exhau...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108859	mcp-go through 1.2.1 Denial of Service via Unbounded PO...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109398	Gumlet php-image-resize before 3.0.1 Denial of Service vi...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104939	NGINX Ingress Controller vulnerability	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108082	Symfony: ReDoS in HeaderUtils::split() Reachable Throug...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109413	Symfony: Unbounded Recursion in the YAML Inline Lexer ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109449	Symfony: Unbounded Nesting in the Expression Parser L...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103101	CVE-2026-103101: Pexip Infinity 30.0 through 40.x before...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83407	CVE-2026-83407: Vulnerability in the Oracle Access Man...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91534	CVE-2026-91534: Vulnerability in the Oracle Business Int...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Uncontrolled Resource Consumption: 260 blocked · avg CVSS 6.9 · 2 CISA KEV (continued)				
CVE-2026-39453	Red Lion Controls N-Tron 700 Series Reachable Assertion	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91347	CVE-2026-91347: Vulnerability in the iSupport product of...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101648	CVE-2026-101648: Vulnerability in the Oracle Partner Ma...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101459	CVE-2026-101459: Vulnerability in the Siebel CRM Deplo...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97629	NGINX ngx_http_ssl_module vulnerability	High / 8.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-101684	CVE-2026-101684: Vulnerability in the Oracle E-Business...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101019	NGINX ngx_http_js_module vulnerability	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87394	CVE-2026-87394: Vulnerability in the Oracle Outside In T...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94644	Apache Thrift: PHP `TJSONProtocol` string/number reade...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101903	Axios: ReDoS in fromDataURI data: URL parser freezes th...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94653	Apache Thrift: PHP framed/memory/HTTP transports re-s...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96780	figlet is vulnerable to denial of service via unbounded loo...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101896	Angular: Denial of Service via Numeric URL Matrix Param...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96289	Apache Thrift: php `--gen php:inlined` struct readers (and...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94482	Next.js: Denial of Service in App Router using Server Acti...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107810	Nginx UI: Backup restore follows crafted symlinks into the...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101422	CVE-2026-101422: Vulnerability in the PeopleSoft Enterp...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87309	CVE-2026-87309: Vulnerability in the JD Edwards Enterp...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101427	CVE-2026-101427: Vulnerability in the PeopleSoft Enterpr...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101837	CVE-2026-101837: Vulnerability in the Oracle Shipping Ex...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Uncontrolled Resource Consumption: 260 blocked · avg CVSS 6.9 · 2 CISA KEV (continued)				
CVE-2026-101818	CVE-2026-101818: Vulnerability in the Oracle Product Hu...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111805	Apache Traffic Server: HTTP/2 Content-Length truncatio...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101833	CVE-2026-101833: Vulnerability in the Oracle Shipping Ex...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101641	CVE-2026-101641: Vulnerability in the Oracle Report Man...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101387	CVE-2026-101387: Vulnerability in the Oracle Capacity pr...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101398	CVE-2026-101398: Vulnerability in the Oracle Capacity pr...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101815	CVE-2026-101815: Vulnerability in the Assets product of ...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101434	CVE-2026-101434: Vulnerability in the PeopleSoft Enterp...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85642	Formidable Forms 6.5 - 6.35 - Unauthenticated Payment ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100242	DataTransfer depends on phpspreadsheet version vulner...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-68495	jackson-dataformats-binary: CBOR parser does not enfor...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107577	Loop with Unreachable Exit Condition ('Infinite Loop') in h...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15822	IBM DataPower Gateway Denial of Service	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107579	Inefficient Algorithmic Complexity in hMailServer	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91345	CVE-2026-91345: Vulnerability in the Oracle Outside In T...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91349	CVE-2026-91349: Vulnerability in the Oracle Outside In T...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2015-5477	CVE-2015-5477: named in ISC BIND 9.x before 9.9.7-P2 a...	High / 7.5	CISA KEV	✓ Blocked
CVE-2026-91828	OMGF < 6.3.11 - Unauthenticated DoS via do_optimize	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114136	Django REST framework: JSONParser applies an attacker...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114138	Django REST framework: Accept header with many large ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Uncontrolled Resource Consumption: 260 blocked · avg CVSS 6.9 · 2 CISA KEV (continued)				
CVE-2026-76290	Cisco: Denial of Service (DoS) through Unauthenticated P...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107574	Inefficient Algorithmic Complexity in hMailServer	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87395	CVE-2026-87395: Vulnerability in the Oracle Outside In T...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87369	CVE-2026-87369: Vulnerability in the Oracle Service Bus ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87398	CVE-2026-87398: Vulnerability in the Oracle Outside In T...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91344	CVE-2026-91344: Vulnerability in the Oracle Outside In T...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91350	CVE-2026-91350: Vulnerability in the Oracle Outside In T...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75996	ColdFusion | Uncontrolled Resource Consumption (CWE-...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101508	CVE-2026-101508: Vulnerability in the Siebel CRM Integr...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96580	Gitea Actions memory exhaustion through large static mat...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102281	Nest: Remote process termination via a deeply nested mi...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103471	restbed through 5.0.0 Denial of Service via Unbounded H...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107805	Nginx UI: Unauthenticated signed-request body staging c...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103499	IBM WebSphere Application Server and WebSphere Appli...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101160	WP Ultimate Review < 2.4.4 - Unauthenticated DoS via N...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104712	Apache Struts: Disproportionate response size when ren...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101161	WP Ultimate Review < 2.4.4 - Unauthenticated DoS via U...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110354	CVE-2026-110354: HAProxy 3 before 3.4.6 allows a remo...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113711	ApostropheCMS: Unauthenticated resource exhaustion vi...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-50787	CVE-2026-50787: e-SIC Livre (esiclivre) v0.2.2 and earlie...	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Uncontrolled Resource Consumption: 260 blocked · avg CVSS 6.9 · 2 CISA KEV (continued)				
CVE-2026-75507	GraphQL-core: Denial of service via quadratic complexity ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75508	GraphQL-core: Denial of service via comment tokens byp...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-68498	jackson-core: Delayed maxNameLength enforcement for ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115887	graphql-scalars PhoneNumber scalar is vulnerable to reg...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76491	Cisco Expressway Series Software Hardening Release: O...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111181	body-parser vulnerable to Denial of Service via trailing byt...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101520	CVE-2026-101520: Vulnerability in the Oracle Global Lifec...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97076	WordPress WP Rocket plugin < 3.23.5 - Denial of Service ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100354	kin-openapi: Uncontrolled Recursion on Circular allOf/any...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101572	CVE-2026-101572: Vulnerability in the Helidon product of...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109527	Model Context Protocol Python SDK HTTP and OAuth en...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108395	Model Context Protocol Java SDK HTTP server transport...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113872	multer vulnerable to Denial of Service via a pending async...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105900	ColdFusion | Improper Input Validation (CWE-20)	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14854	WooCommerce Bookings < 3.11.0 - Unauthenticated Deni...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100352	kin-openapi: YAML NaN/Inf Values Bypass Built-in Guard...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110353	CVE-2026-110353: HAProxy 3.2 before 3.4.6 allows a re...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91502	CVE-2026-91502: Vulnerability in the Oracle WebLogic S...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91642	CVE-2026-91642: Vulnerability in Oracle Essbase (comp...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101822	CVE-2026-101822: Vulnerability in the Oracle Bills of Mat...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked

INDUSFACE™ ©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Uncontrolled Resource Consumption: 260 blocked · avg CVSS 6.9 · 2 CISA KEV (continued)				
CVE-2026-87307	CVE-2026-87307: Vulnerability in the JD Edwards Enterp...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87671	CVE-2026-87671: An out-of-bounds memory read vulner...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101040	Ricoh SP 330DN/SP 221/SP C252SF/Aficio SP 3500SF H...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18105	Fireware OS Uncontrolled Resource Consumption in Diag...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109310	SiYuan v3.1.12 before v3.8.6 Denial of Service via getDyna...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87358	CVE-2026-87358: Vulnerability in the Oracle General Led...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91238	CVE-2026-91238: Vulnerability in the Oracle SOA Suite pr...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101388	CVE-2026-101388: Vulnerability in the PeopleSoft Enterp...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101085	Nezha before 2.3.8 Denial of Service via Alert Rule	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111383	Nezha 2.0.13 before 2.3.15 Denial of Service via /api/v1/ws...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101649	CVE-2026-101649: Vulnerability in the Oracle Partner Ma...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109324	Grav before 2.1.7 Memory Exhaustion via Oversized Imag...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96615	NGINX Gateway Fabric vulnerability	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101650	CVE-2026-101650: Vulnerability in the Oracle Partner Ma...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101827	CVE-2026-101827: Vulnerability in the Oracle HCM Com...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101642	CVE-2026-101642: Vulnerability in the Oracle Report Man...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111384	Nezha 1.0.0 before 2.3.15 Memory Exhaustion via File Man...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101583	CVE-2026-101583: Vulnerability in the Helidon product of...	High / 7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-17545	PHP on Windows: Reserved Device Names Are Not Rejec...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115971	Travisun Opptrix preParsing handler webhook Buffer.con...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Uncontrolled Resource Consumption: 260 blocked · avg CVSS 6.9 · 2 CISA KEV (continued)				
CVE-2026-100572	OpenClaw before 2026.8.1 Denial of Service via Rate Limit	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77468	Lychee: Missing Authentication for Critical Function and A...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108755	Hatchet through 0.110.5 Unauthenticated Memory Exhaus...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97212	Monta monta.app Insufficient Session Expiration	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84429	Potential denial-of-service vulnerability in HTTP header p...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77050	Potential denial-of-service vulnerability in get_supported...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101025	NGINX ngx_http_js_module vulnerability	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95101	NGINX ngx_http_v3_module vulnerability	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108121	Koozali - SME Server Improper Input Validation in domain ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55835	Lookyloo: Potential sub-system DoS due to parameter mi...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100647	vLLM before 0.29.0 CPU Exhaustion via unbounded cach...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111817	Apache Traffic Server: Dropping chunked trailers stalls a ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103261	Tornado before 6.5.9 Denial of Service via Query String	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104454	YesWiki before 4.6.7 ReDoS via wakka.php Edit-Preview E...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101695	CVE-2026-101695: Vulnerability in the Oracle One-to-On...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-60869	CVE-2026-60869: Vulnerability in the PeopleSoft Enterpr...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112955	ApostropheCMS: Import archives can exhaust server stor...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105964	Gitea Actions artifact v4 API unbounded request body	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101488	CVE-2026-101488: Vulnerability in the PeopleSoft Enterp...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101584	CVE-2026-101584: Vulnerability in the Helidon product of...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Uncontrolled Resource Consumption: 260 blocked · avg CVSS 6.9 · 2 CISA KEV (continued)				
CVE-2026-101628	CVE-2026-101628: Vulnerability in the MySQL Cluster pro...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101569	CVE-2026-101569: Vulnerability in the Helidon product of...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76289	Cisco: Denial of Service (DoS) through the REST API in Sp...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114508	Laravel relationship inclusion can trigger unauthorized da...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-33374	Unbounded memory allocation in the Prometheus rule co...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104713	Apache Struts: Unbounded request body read in the RES...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76271	Cisco: Denial of Service (DoS) in the Discover Splunk Obs...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107582	Inefficient Algorithmic Complexity in hMailServer	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-1403	Allocation of Resources Without Limits or Throttling in Git...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104633	Gitea migration memory exhaustion from zero page size	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95696	IBM WebSphere Application Server Liberty Denial of Servi...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39767	WordPress WPBase Cache plugin <= 5.5.6 - Denial of Ser...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91435	CVE-2026-91435: Vulnerability in the Siebel CRM Deploy...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91441	CVE-2026-91441: Vulnerability in the Siebel Apps - Custo...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91468	CVE-2026-91468: Vulnerability in the PeopleSoft Enterpri...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91541	CVE-2026-91541: Vulnerability in the PeopleSoft Enterpri...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87365	CVE-2026-87365: Vulnerability in the Oracle WebCenter ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87393	CVE-2026-87393: Vulnerability in the Oracle Outside In T...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107583	Inefficient Algorithmic Complexity in hMailServer	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105754	vLLM: Scale-out disaggregated multimodal transport trus...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Uncontrolled Resource Consumption: 260 blocked · avg CVSS 6.9 · 2 CISA KEV (continued)				
CVE-2026-107294	Pydantic AI: Unbounded memory use when downloading ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101575	CVE-2026-101575: Vulnerability in the Helidon product of...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-60881	CVE-2026-60881: Vulnerability in the PeopleSoft Enterpri...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107381	svg-sanitizer: Mixed-case xlink:HrEf skips the `` nesting-...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91424	CVE-2026-91424: Vulnerability in the Siebel CRM Deploy...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91466	CVE-2026-91466: Vulnerability in the PeopleSoft Enterpri...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106436	Application denial of service and data truncation via unch...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94484	Next.js has cache poisoning in SSG/ISR rendering that lea...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91654	CVE-2026-91654: Vulnerability in Oracle Essbase (comp...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94638	Apache Thrift: PHP `thrift_protocol` C extension ignores t...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102598	Werkzeug safe_join() allows Windows special device nam...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110816	qs.stringify with arrayFormat comma throws TypeError on...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114129	stream-json: FlexAssembler string/RegExp path filters joi...	Medium / 6.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83375	CVE-2026-83375: Vulnerability in the PeopleSoft Enterpri...	Medium / 6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102274	PyJWT: Malformed RSA JWK aborts parsing of an entire J...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101389	CVE-2026-101389: Vulnerability in the PeopleSoft Enterp...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104844	PostCSS: Quadratic complexity in flat selector parsing all...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107833	OWASP Coraza WAF: Unbounded recursion in JSON resp...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91247	CVE-2026-91247: Vulnerability in the Oracle WebCenter ...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91421	CVE-2026-91421: Vulnerability in the Siebel CRM Deploy...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Uncontrolled Resource Consumption: 260 blocked · avg CVSS 6.9 · 2 CISA KEV (continued)				
CVE-2026-94681	WordPress WP Store Locator plugin < 3.0.0 - Denial of Se...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115382	Wasmtime 46.0.0 before 48.0.4 and 49.0.0 before 49.0.2 ...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
GHSA-3C6W-J9XM-8H2H	Coraza: Unbounded recursion in JSON response body pr...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70162	Microsoft Security Advisory CVE-2026-70162 - .NET Den...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101524	CVE-2026-101524: Vulnerability in the Oracle Enterprise ...	Medium / 5.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-60839	CVE-2026-60839: Vulnerability in the PeopleSoft Enterpr...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101407	CVE-2026-101407: Vulnerability in the PeopleSoft Enterpr...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93546	Apache HTTP Server: mod_dav_fs namespace overflow	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87390	CVE-2026-87390: Vulnerability in the Oracle WebCenter ...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85005	Popup Maker WP 1.2.2.1 - 1.4.5 - Subscriber+ Zero-Argum...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104893	Plane: Improper validation allows arbitrary modification of...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107585	Allocation of Resources Without Limits or Throttling in hM...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111985	AUTOMATIC1111 stable-diffusion-webui Metadata Extracti...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114731	CVE-2026-114731: Roundcube Webmail before 1.6.20 and...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100508	WordPress Two Factor plugin <= 0.16.0 - Denial of Servic...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101413	CVE-2026-101413: Vulnerability in the PeopleSoft Enterpr...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113650	ApostropheCMS sanitize-html: unbounded recursion whe...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113656	ApostropheCMS: Unauthenticated unbounded multipart u...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110595	BottleCRM 0.45 through 1.14.5 Memory Exhaustion via Co...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100347	kin-openapi: Unauthenticated panic (DoS) in openapi3filt...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Uncontrolled Resource Consumption: 260 blocked · avg CVSS 6.9 · 2 CISA KEV (continued)				
CVE-2026-101088	Nezha before 2.3.1 Denial of Service via Concurrent Serve...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107834	OWASP Coraza WAF: Resource exhaustion via deferred fi...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100350	kin-openapi deepObject query decoding repeatedly com...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101587	CVE-2026-101587: Vulnerability in the Helidon product of...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107843	Contao: The registration module re-sends activation mails	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108681	zhayujie CowAgent Web Console web_channel.py denial ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108750	OpenDocMan 2.4.0 through 2.10.0 Decompression Bomb ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108682	zhayujie CowAgent Web Console upload read denial of se...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91352	CVE-2026-91352: Vulnerability in the Oracle Outside In T...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110249	Mozilla: Denial-of-service in the Exchange email compon...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92707	MessagePack: Nested arrays can blow past buffer length ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95502	Git Sync memory exhaustion via a malicious Git server	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91536	CVE-2026-91536: Vulnerability in the Oracle SOA Suite pr...	Medium / 5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105645	Ghost: Regular Expression Denial of Service in External M...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105646	Ghost: Regular Expression Denial of Service in Content Im...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76733	Authenticated Denial-of-Service Vulnerability in HPE Net...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91524	CVE-2026-91524: Vulnerability in the Oracle Business Int...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107079	CVE-2026-107079: An issue in Systrome Validation & Cer...	Medium / 4.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-91660	CVE-2026-91660: Vulnerability in Oracle Essbase (comp...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73273	Gitea Maven checksum upload quota bypass and memory...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Uncontrolled Resource Consumption: 260 blocked · avg CVSS 6.9 · 2 CISA KEV (continued)				
CVE-2026-42528	Apache HTTP Server: mod_dav shared lock overflow	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73130	Gitea repository initialization resource exhaustion	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101497	CVE-2026-101497: Vulnerability in the Oracle Identity Ma...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107586	Allocation of Resources Without Limits or Throttling in hM...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107312	Examples for Developers - Less critical - Allocation of res...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83390	CVE-2026-83390: Vulnerability in the Oracle Application...	Medium / 4.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-60874	CVE-2026-60874: Vulnerability in the PeopleSoft Enterpri...	Medium / 4.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101333	Keycloak-services: keycloak-services: unbounded metric...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101402	CVE-2026-101402: Vulnerability in the Siebel Apps - Mar...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114723	CVE-2026-114723: Roundcube Webmail before 1.6.20 an...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102414	pbkdf2 rehashes long passwords on every iteration, enabl...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-48005	Apache HTTP Server: mod_auth_digest reauthentication a...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101570	CVE-2026-101570: Vulnerability in the Helidon product of...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107727	Strawberry legacy graphql-ws retains naturally complete...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91582	CVE-2026-91582: Vulnerability in the Oracle Business Int...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101805	CVE-2026-101805: Vulnerability in the Oracle Application...	Low / 3.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101415	CVE-2026-101415: Vulnerability in the PeopleSoft Enterpr...	Low / 3.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55467	CUPS fax option values bypass the CVE-2026-34980 co...	Low / 2.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112157	MemTensor memmy-agent Memory Service http.ts requir...	Low / 2.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-0317	PAN-OS: Denial of Service Vulnerability	Low / 1.2	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 248 blocked · avg CVSS 8.5 · 4 CISA KEV				
CVE-2026-100382	Unauthenticated remote code execution through wikitext ...	Critical / 10	VULNCHECK KEV	✓ Blocked
CVE-2026-101076	Netcore NR289-GE CGI set_ntp_server_ip.cgi system os ...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101001	Netcore NBR200V2 Web Management network_tools eval...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101072	Netcore NR289-GE CGI ap_ip.cgi system os command inj...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101075	Netcore NR289-GE Location Time location_time.cgi syste...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102240	Netcore NAP930 Network Tools CGI network_tools eval o...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105134	Ahsay AhsayCBS Replication Receiver UpdateReceivers....	Critical / 10	CISA KEV	✓ Blocked
CVE-2026-108576	TOZED X300 IPPingDiagnostics process_ping os comma...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108804	TRENDnet TEW-751DR/TEW-752DRU/TEW733GR Web M...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105484	TOTOLINK X6000R UploadFirmwareFile cstecgi.cgi firm...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110536	D-Link DIR-868L HNAP CGI cgibin system os command i...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110957	Wavlink WL-WN530BE2-A Login Processing api.cgi sub_1...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109110	Wavlink WL-WN592AX6 wmapd system os command inje...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108917	Edimax BR-6208AC formAutoFWupgrade command injec...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108918	Edimax BR-6208AC formWlanMP command injection	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114575	TOTOLINK A950RG product.so UploadCustomModule co...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79846	HPE: Unauthenticated Command Injection Vulnerabilities i...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57155	OPNsense: Root RCE via Arbitrary File Write in GeoIP Alia...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105697	Langflow: OS command injection (RCE) via arbitrary com...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102911	zosmaai pi-llm-wiki wiki_capture_source MCP tool index.t...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 248 blocked · avg CVSS 8.5 · 4 CISA KEV (continued)				
CVE-2026-93698	CVE-2026-93698: Insufficient validation allows arbitrary ...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105691	Penpot: Authenticated OS Command Injection in Penpot S...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105740	Langflow: Authenticated RCE via MCP Stdio transport allo...	Critical / 9.9	VULNCHECK KEV	✓ Blocked
CVE-2026-103848	Adobe Experience Manager | Improper Neutralization of S...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104584	CVE-2026-104584: reNgine up to v2.2.0 and current mas...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-108983	GV-ASManager Web Server Command Injection Vulnerabi...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110392	Samsung QA-Board — Unauthenticated OS command inje...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104585	CVE-2026-104585: Mobile Security Framework (MobSF) ...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-104586	CVE-2026-104586: AUTOM8N (WHM/cPanel plugin) thro...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-16741	OS Command in TR7 Cyber Defense's TR7 ASP	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79861	HPE: Unauthenticated Command Injection Vulnerability in ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79857	HPE: Unauthenticated Command Injection Vulnerability in ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91140	OS command injection in Progress Software Autonomous...	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79864	HPE: Unauthenticated Adjacent Command Injection Vulne...	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76724	Unauthenticated Adjacent Command Injection Vulnerabili...	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110243	Kiloview E3 NDI Encoder OS Command Injection	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107861	Kiloview E3 NDI Encoder OS Command Injection	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113506	aaPanel File Manager common.py ExecShell os command...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113390	DrayTek Vigor2960 CGI mainfunction.cgi sub_182B0 os c...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108894	Linksys E1700 Static Route addStaticRoute os command i...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 248 blocked · avg CVSS 8.5 · 4 CISA KEV (continued)				
CVE-2026-75937	OS Command Injection in Digi Accelerated Linux (DAL OS)	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108540	OpenSpug File Transfer transfer os command injection	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106126	Command Injection	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100896	TOTOLINK N150RT Web Management formWISiteSurvey ...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100714	Froxlor before 2.3.12 Command Injection via letsencryptc...	Critical / 9.4	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-112370	H3C Magic NX15 usrlist sub_416874 os command injection	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113389	DrayTek Vigor2960 CGI Process mainfunction.cgi set_tab...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109122	Kiloview E3 NDI Encoder OS Command Injection	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113788	Lagoon core ssh service vulnerable to remote code exec...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101008	aaPanel BaoTa File Merge files.py merge_split_file comma...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101002	Netcore NBR200V2 Tools Ping network_tools system os ...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101264	Ziroom ZHOME A0101 set_passwd command injection	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101261	Ziroom ZHOME A0101 firstSetup_wifi command injection	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102792	Ziroom ZHOME A0101 set_syslog command injection	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102793	Ziroom ZHOME A0101 set_time_zone command injection	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113391	DrayTek Vigor2960 Upload Endpoint mainfunction.cgi upl...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108896	Linksys E1700 setLinksysIpv6 os command injection	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109108	Wavlink WL-WN530BE1-A uploadVpn.cgi popen os com...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108895	Linksys E1700 setDMZ os command injection	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115995	Unitree Robotics Unitree Go2 chat_go gpt_thread.py set_v...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 248 blocked · avg CVSS 8.5 · 4 CISA KEV (continued)				
CVE-2025-71429	GPT-SoVITS through 20250606v2pro OS Command Injec...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104019	OS command injection in the Studio Space startup validati...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107459	Openfind | SecuShare Pro - OS Command Injection	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86102	WatchGuard AP Command Injection in Internal Managem...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101007	aaPanel BaoTa Database Backup database.py InputSql os ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101009	aaPanel BaoTa Unzip panelTask.py panelTask.bt_task._un...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107780	Dromara Skyeye Unauthenticated OS Command Injection ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107703	@enmaso/node-convert through 1.0.0 OS Command Inje...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107704	image_optimizer 1.3.0 through 1.9.0 OS Command Injectio...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107699	ppt2png through 0.0.6 OS Command Injection via input a...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110634	git-diff before 2.0.7 OS Command Injection via gitDiff Inpu...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-113802	Wavlink WL-WN530BE1-A Unauthenticated OS Command...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109432	Camunda Expression Injection via orQueries RCE	Critical / 9.3	VULNCHECK KEV	✓ Blocked
CVE-2020-37282	office-converter through 1.0.2 OS Command Injection via ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110635	webp-converter before 3.0.0 OS Command Injection via F...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-110636	pypdftk through 0.5 OS Command Injection via PDF and O...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110638	doc-recog through 1.1.6 OS Command Injection via DocDa...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-110639	@mborne/extract before 0.2.1 OS Command Injection via ...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-110640	Whisper-node through 1.1.1 OS Command Injection via file...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-102031	Junos OS Evolved: A low-privileged TACACS+ user caus...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 248 blocked · avg CVSS 8.5 · 4 CISA KEV (continued)				
CVE-2026-110650	Thumbnail through 1.5 OS Command Injection via generat...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101967	Junos OS Evolved: PTX Series: An attacker controlled DH...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-47786	Pre-Authentication Command Injection	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110643	transcribe2texts through 1.0.6 OS Command Injection via ...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-110644	nodejs-whisper allows OS command injection through cr...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-110645	Video-stitch before 2.0.0-beta.1 OS Command Injection vi...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-110649	Stills before 25.24.2 OS Command Injection via Media File...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-105110	Iskratel Innbox Unauthenticated Remote Code Execution ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102829	simple-git: `VISUAL` editor environment variable is omitte...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103473	Deno 2.7.0 through 2.9.7 Command Injection via node:chil...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102828	simple-git unsafe-operation guard does not block trailer c...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2020-37279	easy-pdf-merge 0.1.0 through 0.2.6 OS Command Injectio...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110646	Beganovich snappdf 1.1.0 before 6.1.0 OS Command Inject...	Critical / 9.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-110858	GitPython 3.1.30 before 3.2.0 Command Injection via Rem...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112900	Pillow: Argument Injection in Ghostscript call, potentially l...	Critical / 9.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-96620	Claude Agent SDK: Argument Injection via resume Option...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110447	CVE-2026-110447: Collabora Online Built-in CODE Server...	Critical / 9.2	CISA KEV	✓ Blocked
CVE-2026-10135	CVE-2026-10135: A OS command injection vulnerability e...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-35499	CVE-2026-35499: An os command injection vulnerability...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-10131	CVE-2026-10131: An OS command injection vulnerability ...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 248 blocked · avg CVSS 8.5 · 4 CISA KEV (continued)				
CVE-2026-9814	CVE-2026-9814: An OS command injection vulnerability ...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-33568	CVE-2026-33568: A OS command injection vulnerability ...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40627	CVE-2026-40627: An os command injection vulnerability ...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2024-4457	Remote Code Execution via JDBC User Store Configurati...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-10138	CVE-2026-10138: A OS command injection vulnerability e...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105014	Azure Pipelines Remote Code Execution Vulnerability	Critical / 9.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-101263	Ziroom ZHOME A0101 set_online_client command injection	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101187	Ziroom ZHOME A0101 USB Device Management API zrUs...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102794	Ziroom ZHOME A0101 ping command injection	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84436	IBM Guardium Data Protection is affected by multiple vuln...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105793	Microsoft UFO: Authenticated Android shell command inj...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79898	Fortra BoKS Manager crlserver command injection vulner...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107202	A command injection vulnerability exists in the h-ui (versi...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101260	Ziroom ZHOME A0101 firstLogin command injection	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101262	Ziroom ZHOME A0101 set_online_client command injection	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102667	Joyland AI WebView command injection	Critical / 9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103056	AiSOC 7.2.0 before 12.0.0 Command Injection via CrowdS...	Critical / 9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102608	ZoneMinder: Authenticated OS Command Injection via un...	Critical / 9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100292	Improper neutralization of special elements used in an OS...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2022-51019	Akaunting before 2.1.31 OS Command Injection via app alias	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 248 blocked · avg CVSS 8.5 · 4 CISA KEV (continued)				
CVE-2026-52356	CVE-2026-52356: An OS command injection vulnerabilit...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111853	CVE-2026-111853: An issue was discovered on Tektronix ...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-30971	ZoneMinder: Authenticated RCE via command injection in...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57117	PraisonAI: Compute-bridged file tools allow shell comma...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108743	Apache Kylin: spark job OS command injection	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102607	ZoneMinder: Authenticated OS Command Injection (RCE) ...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96951	Windows Shell Security Feature Bypass Vulnerability	High / 8.8	CISA KEV	✓ Blocked
CVE-2026-82096	DataStage on Cloud Pak for Data Command Injection	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110005	Moghtech Komodo contains an OS command injection vul...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105106	Koha authenticated OS command injection in tools/sched...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55376	heym Python Tool Sandbox Escape	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110908	CVE-2026-110908: Netgate pfSense FRR package (pfSen...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92115	WP Photo Album Plus <= 9.3.02.002 - Authenticated (Cus...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101207	CVE-2026-101207: Dell OpenManage Integration with Mic...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105407	OS Command Injection vulnerability affecting Tuleap Ente...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12268	Authenticated PowerShell Injection leads to RCE	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78424	OS Command Injection in Packet-Capture (Sniffer) Filter I...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105797	SimpleChat: Command injection via authorization-gate or...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79803	HPE: Authenticated Command Injection Leading to Privile...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12405	Rubygem-foreman_remote_execution: command injectio...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 248 blocked · avg CVSS 8.5 · 4 CISA KEV (continued)				
CVE-2026-100254	CVE-2026-100254: In JetBrains TeamCity before 2026.2,...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82804	Apache DolphinScheduler: Command Injection in the Aler...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87741	ConvertPlus <= 3.6.3 - Authenticated (Subscriber+) PHP ...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85523	OS Command Injection in Felisify Informatics' SambaBox	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105788	Microsoft UFO: Authenticated Android shell command inj...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104085	odt2spip < 4.4.0 OS Command Injection via Document Fil...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100599	OpenClaw 2026.5.1 before 2026.7.1 Remote Code Executi...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110641	@runnerty/executor-decompress through 3.1.1 OS Comm...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77931	MoviePilot 3.1.5 Command Injection via ExecuteComman...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109318	Grav Git Sync 1.0.2 through 3.4.12 Command Injection via ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18529	IBM Maximo Application Suite - Location Service for Esri ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106059	GitAhead through 2.7.1 on macOS Command Injection via ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93858	CVE-2026-93858: In OpenStack Mistral through 23.0.0, t...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100852	AzuraCast before 0.23.8 Command Injection via Streamer...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-41545	WebSocket timelapse path traversal and command injection	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111214	Netgate pfSense CE 2.7.0 through 2.9.0 OS Command Inj...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111217	Netgate pfSense CE through 2.9.0 OS Command Injection...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75779	CVE-2026-75779: Improper Neutralization of Special Ele...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111223	Netgate pfSense CE 2.7.0 through 2.9.0 Command Injecti...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111216	Netgate pfSense CE through 2.9.0 OS Command Injection...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 248 blocked · avg CVSS 8.5 · 4 CISA KEV (continued)				
CVE-2026-111218	Netgate pfSense CE 2.7.0 through 2.9.0 OS Command Inj...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87666	CVE-2026-87666: An OS command injection vulnerability...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102160	Security Advisory 0190	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54674	Authenticated Command Injection in FreePBX UCP Interfa...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87969	WatchGuard AP Authenticated Command Injection in Dia...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100559	OpenClaw before 2026.8.1 Command Injection via Escape...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75600	FreePBX: Authenticated API generatedocs Host Comman...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111226	Netgate pfSense CE 2.4.5 through 2.9.0 OS Command Inj...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111215	Netgate pfSense CE through 2.9.0 OS Command Injection...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-43850	CVE-2026-43850: A command injection vulnerability cou...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111229	Netgate pfSense CE 2.7.0 through 2.9.0 Command Injecti...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94581	CVE-2026-94581: An OS command injection vulnerability...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87680	CVE-2026-87680: A command injection vulnerability in th...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86035	Weblate: Mercurial argument injection via repository filen...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94586	CVE-2026-94586: A command injection vulnerability exis...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106931	CVE-2026-106931: SiteGuard Server Edition contains an ...	High / 8.5	CISA KEV	✓ Blocked
CVE-2026-55786	Flyto2 Core: Unauthenticated Command Execution via HT...	High / 8.4	VULNCHECK KEV	✓ Blocked
CVE-2026-45449	Unitronics - CWE-78: Improper Neutralization of Special E...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79890	HPE: Unauthenticated Command Injection Vulnerabilities i...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84057	IBM Guardium Data Protection is affected by multiple vuln...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 248 blocked · avg CVSS 8.5 · 4 CISA KEV (continued)				
CVE-2026-102826	simple-git allows command execution through unblocked ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102827	simple-git: unsafe-operations plugin bypass via git long-o...	High / 8.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-102422	shell-quote: `quote()` command injection via a line termin...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110455	CVE-2026-110455: A malicious actor with access to the n...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87864	IMAP APPEND plus CRLF conversion command injection	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101045	Fleet Homebrew Cask OS Command Injection via Metadata	High / 8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111451	CVE-2026-111451: Wheels CLI 4.0.0 through 4.1.1 insuffici...	High / 7.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-45562	FreePBX: Authenticated Remote Code Execution in FreeP...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108161	FusionPBX through 5.6.5 OS Command Injection via Calle...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106056	Rundeck before 6.2.0 OS Command Injection via Window...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108546	Spotweb through 1.5.8 OS Command Injection via Spot Tit...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105841	lrzsz before 0.13.0 OS Command Injection via lrz Pipe Mode	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106058	GitAhead through 2.7.1 OS Command Injection via Git Filte...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106556	Backstage: Configuration bypass in TechDocs mkdocs.y...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106510	Backstage: Remote code execution via crafted markdown...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
GHSA-W2VW-W76X-QR89	Nx: OS command injection via git revisions and remote refs	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112942	launch-editor: `fs.existsSync()` existence check can be b...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84440	IBM Guardium Data Protection is affected by multiple vuln...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92531	Improper Neutralization of Special Elements used in an O...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102243	MODSetter SurfSense MCP Connector Integration test co...	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 248 blocked · avg CVSS 8.5 · 4 CISA KEV (continued)				
CVE-2026-87675	CVE-2026-87675: An OS command injection vulnerability...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102874	HKUDS AnyTool Execute Endpoint main.py subprocess.ru...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104859	@nx/docker: OS command injection in the @nx/docker re...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86330	Noobaa-core: noobaa-core: os command injection in clus...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12267	Authenticated PowerShell Injection in DNS Query Resoluti...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79956	HPE: Improper Sanitization leads to Command Injection in...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95709	HPE: Authenticated Command Injection Vulnerabilities in ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39902	Cacti: Authenticated RCE on Data Input	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100232	CVE-2026-100232: Post-authentication Improper Neutral...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95708	HPE: Authenticated File Write leads to Command Injection...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84278	IBM Guardium Data Protection Command Injection	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76727	Authenticated Command Injection Vulnerabilities in HPE ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102114	Kiteworks Core OS Command Injection	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102096	Kiteworks Core OS command injection	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84422	IBM Guardium Data Protection is affected by multiple vuln...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76740	HPE Compute Scale-up Server 3200 and 3250 platforms,...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95705	HPE: Authenticated Command Injection Vulnerabilities in ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92263	SparkyFitness: Authenticated OS command injection (hos...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95706	HPE: Authenticated Command Injection Vulnerabilities in ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114646	NoSQL command injection via mismatched raw BSON len...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 248 blocked · avg CVSS 8.5 · 4 CISA KEV (continued)				
CVE-2026-112301	orbitale imagemagick-php Command.php font os comma...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115969	Travisun Opptrix Schedule API setup command injection	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108916	Edimax BR-6208AC formAccept command injection	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34007	**RCE** Unsanitized `X-Forwarded-For` header passed t...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101216	CVE-2026-101216: Dell Unisphere for PowerMax vApp, ve...	Medium / 6.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101215	CVE-2026-101215: Dell Unisphere for PowerMax vApp, ve...	Medium / 6.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-20321	Cisco Application Policy Infrastructure Controller API Co...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55679	WeGIA: Pre-auth Installer Injection Chain Enables Comma...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79815	HPE: Authenticated Command Injection Vulnerability in th...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112943	launch-editor: escapeCmdArgs() omits % escaping on Wi...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-0313	Cortex XSOAR: OS Command Injection Vulnerability	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-0320	PAN-OS: Authenticated Admin Command Injection Vulner...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89116	SAP: OS Command Injection in Yeoman-UI / Application ...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
GHSA-5GJ4-9GM7-2FX2	Coraza body processor has a JSON key collision that allo...	Medium / 5.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113396	DrayTek Vigor2960 Rename Table mainfunction.cgi rena...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113397	DrayTek Vigor2960 IPsec mainfunction.cgi ruequest_cert...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105487	yogeshojha reNgine listTargets Endpoint tasks.py subdo...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102906	0xshariq github-mcp-server Git Remove MCP Tool github...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101859	RaspAP raspap-webgui OpenVPN Configuration del_ovpn...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108817	agno-agi agno CodingTools coding.py agno.CodingTools....	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 248 blocked · avg CVSS 8.5 · 4 CISA KEV (continued)				
CVE-2026-112159	JumpServer Template Rendering os command injection	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112195	FusionPBX Dialplan Editor dialplan.php os command injec...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34498	L4L	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76437	Cisco Smart Software Manager On-Prem Command Inject...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101858	RaspAP raspap-webgui SSID Processing WiFiManager.ph...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55453	CUPS ipp backend status-line injection can update queue...	Low / 3.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105767	Chainguard Academy (edu) integrate-platform-docs com...	Low / 2.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114523	Ffmpeg Image Toolkit - Highly critical - Remote Code Exe...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
Injection: 101 blocked · avg CVSS 6.9 · 0 CISA KEV				
CVE-2026-100717	froxlor before 2.3.12 CRLF Injection via validateUrl userinfo	Critical / 9.9	PUBLIC EXPLOIT/POC	✓ Blocked
GHSA-CXF3-9H37-7RR8	Echo: Rejected WebSocket upgrades can bypass Echo ro...	Critical / 9.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82973	GitLab: Improper Neutralization of CRLF Sequences ('CRL...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88092	Microsoft Security Advisory CVE-2026-88092 - ASP.NE...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88773	HTTP Request Smuggling	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-105844	Payload: Prototype pollution in Payload Import Export plu...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-109758	CVE-2026-109758: Perforce Helix Authentication Service...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111816	Apache Traffic Server: A malformed 302 response bypas...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-118264	Echo: Rejected WebSocket upgrades can bypass Echo ro...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115823	Starman versions before 0.4019 for Perl send response b...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Injection: 101 blocked · avg CVSS 6.9 · 0 CISA KEV (continued)				
CVE-2026-70188	Microsoft Security Advisory CVE-2026-70188 - ASP.NET ...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-31699	Apache Traffic Server: Origin connection still owed a requ...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106448	StableLib: Prototype poisoning via `__proto__` map keys in...	High / 8.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2021-48012	fast-toml through 0.5.4 Prototype Pollution via __proto__ ...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114142	toml-node: Prototype pollution: parsing a TOML documen...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107701	dot-access through 1.0.0 Prototype Pollution via set() pat...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102479	CVE-2026-102479: In Eclipse Vert.x versions [5.0.0,5.0.1...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94646	Apache Thrift: Node.js `server.js` ends the process on an...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100631	Parse Server 9.0.0 Unauthenticated Installation Deletion v...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112309	@rvf/set-get before 7.0.4 Prototype Pollution via setPath I...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111220	Netgate pfSense CE through 2.9.0 Crontab Injection via P...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73975	djehuty: Authenticated SPARQL injection in session editin...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101909	Axios: Prototype Pollution Gadget in axios toFormData Op...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104852	GraphQL Tools has prototype pollution in well-establishe...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-61642	Squid Request Smuggling in HTTP Transfer-Encoding	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110842	n8n before 2.41.4 and 2.42.1 Prototype Pollution via MCP ...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110111	Xen Orchestra before 6.9.0 Privilege Escalation via Protot...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101905	Axios: Node HTTP adapter prototype-pollution gadget all...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102600	Socket.IO: Prototype Pollution via Unsafe Client Session L...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111222	Netgate pfSense CE through 2.9.0 php.ini Injection via Ti...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Injection: 101 blocked · avg CVSS 6.9 · 0 CISA KEV (continued)				
CVE-2026-86146	Apache bRPC: HTTP Request Smuggling and Header Inje...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112212	Inconsistent Interpretation of HTTP Requests ('HTTP Req...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106550	Mozilla's Node-convict (version 6.2.2 and later) is vulnera...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105675	Ghost: Invite Token Disclosure in Ghost Admin API	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63718	Apache HTTP Server: mod_proxy_uwsgi Transfer-Encodi...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100666	Netty 4.2.0 through 4.2.16 Response Desynchronization v...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114648	NoSQL injection via dot and dollar characters in LINQ filte...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88829	Busybox: busybox: http request smuggling via pipelined r...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113666	ApostropheCMS: Authenticated projection-exclusion prot...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114652	Update operator injection via single-element list rewriting ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114396	Trudesk through 1.2.11 MongoDB $where Injection via tick...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57488	pupnp: Integer truncation in HTTP Content-Length parsin...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103289	Ghost 5.9.0 before 6.44.1 Authorization Bypass via Comm...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73976	djehuty: Unauthenticated SPARQL injection in the search ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114510	Flexible GraphRAG: Cypher/Graph Injection via broken stri...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103250	n8n before 1.123.80, 2.39.6, and 2.40.1 NoSQL Injection vi...	High / 7	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2025-55702	Apache Traffic Server: An unread Expect: 100-continue re...	High / 7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93003	NetX Duo Web HTTP server interprets request body cont...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101904	Axios: Header Injection via Inherited headers After Minim...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114401	Trudesk through 1.2.11 Username Enumeration via Regex I...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Injection: 101 blocked · avg CVSS 6.9 · 0 CISA KEV (continued)				
CVE-2026-111809	Apache Traffic Server: HEAD requests carrying Content-L...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101902	Axios: Prototype-Pollution Gadget in the Default Instance ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101908	Axios: Prototype pollution gadget in fetch adapter can alte...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101900	Axios: Fetch Adapter Header Injection via Inherited Form...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103258	n8n before 2.39.6 and 2.40.x before 2.40.1 Filter Bypass v...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100659	Netty 4.2.0 through 4.2.17 HTTP/3 Request Routing Bypass	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106513	MISP: Site-Admin Can Repoint Redis Workers to Attacker-...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87678	CVE-2026-87678: An input validation and output encodin...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87661	CVE-2026-87661: Brocade Fabric OS versions before 9.2...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-107301	msgpack5: Partial options disable prototype protection	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59962	Tandoor Recipes: ORM ORDER BY Injection via FK Traver...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94439	HTTP/1 server connection desynchronization after 2xx C...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103036	@orpc/json-schema: Prototype injection in smart coercion	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83395	CVE-2026-83395: Vulnerability in the Oracle Java SE, Or...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105681	Ghost: Authorization Bypass in Comments Feature	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103918	@orpc/zod: Prototype injection in smart coercion	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56866	HTTP/1 client connection desynchronization after CONNE...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100724	http4k before 6.49.0.0 Host Header Routing Bypass via re...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91860	Prototype Pollution in Vaadin Charts and Component Bas...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94194	Mint HTTP/1 client applies chunked framing when chunke...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Injection: 101 blocked · avg CVSS 6.9 · 0 CISA KEV (continued)				
CVE-2026-110835	FreeRDP 3.0.0 before 3.32.0 HTTP Header Injection via Pr...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111750	AIOHTTP: Pure-Python parser request smuggling	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77802	HTTP Request Smuggling Vulnerability in Progress® Teler...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86536	Apache Thrift, Apache Thrift, Apache Thrift: A map key fr...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111172	@casl/ability 6.7.5 before 7.0.2 Prototype Pollution via rule...	Medium / 6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114655	KMS request injection via unsanitized key vault and provi...	Medium / 6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106119	LangChain: MongoDBChatMessageHistory query injectio...	Medium / 6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110848	n8n before 1.123.83, 2.41.4, and 2.42.1 Prototype Pollution...	Medium / 6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-41504	Coraza: Native audit-log format allows CRLF injection and...	Medium / 5.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85976	HTTP response splitting in Progress MarkLogic Server Qu...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115877	Twisted: HTTP Request Smuggling in twisted.web via a B...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113662	ApostropheCMS import-export: NoSQL injection via upda...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106160	Prototype Pollution via Model.accept and kendo.setter in ...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103399	Libsoup: soupserver: http/1 request smuggling via undrai...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104956	Plane: Unauthenticated ORM field-name injection via `gro...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114647	NoSQL operator injection via unvalidated replacement do...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91453	CVE-2026-91453: Vulnerability in the Oracle Java SE, Ora...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91452	CVE-2026-91452: Vulnerability in the Oracle Java SE, Ora...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110757	Text::CSV_XS versions before 1.65 for Perl allow record s...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91332	CVE-2026-91332: Vulnerability in Oracle Java SE (compo...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Injection: 101 blocked · avg CVSS 6.9 · 0 CISA KEV (continued)				
CVE-2026-91451	CVE-2026-91451: Vulnerability in Oracle Java SE (compo...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102988	Plane: ORM Field Injection via Unvalidated `order_by` Para...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104183	stream-json has a prototype pollution issue: Assembler w...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111228	Netgate pfSense CE 2.7.1 through 2.9.0 CRLF Injection via...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111227	Netgate pfSense CE through 2.9.0 CRLF Injection via serv...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81914	Apache Airflow Google provider: Google Drive query inje...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76295	Cisco: SPL Injection through the REST API in Splunk Secu...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87292	CVE-2026-87292: Vulnerability in the Oracle Java SE, Or...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77803	Front-end Desynchronization Vulnerability in Progress® T...	Low / 3.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105652	Ghost: Password Hash Ordering Disclosure in Ghost Admi...	Low / 3.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113715	virtualenv: Venv configuration readback can reinterpret p...	Low / 2	NO KNOWN EXPLOIT	✓ Blocked
Insecure Design (File-Upload, LDAP): 65 blocked · avg CVSS 7.3 · 2 CISA KEV				
CVE-2026-39770	WordPress Doctreat theme <= 1.7.0 - Arbitrary File Upload...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32579	WordPress Kognetiks Chatbot for WordPress plugin <= 2....	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94503	WordPress Zombify plugin <= 1.7.7 - Arbitrary File Upload ...	Critical / 10	VULNCHECK KEV	✓ Blocked
CVE-2026-111832	WordPress WP Mailster plugin <= 1.9.1.0 - Arbitrary File U...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111834	WordPress Mang Board WP plugin <= 2.4.4 - Arbitrary Fil...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39755	WordPress WP Duplicate plugin <= 1.1.11 - Arbitrary File U...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62024	WordPress CodeBard Help Desk plugin <= 1.1.2 - Arbitrar...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Insecure Design (File-Upload, LDAP): 65 blocked · avg CVSS 7.3 · 2 CISA KEV (continued)				
CVE-2026-39759	WordPress Workreap Core plugin <= 3.4.5 - Arbitrary File ...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39757	WordPress Taskbot plugin <= 6.6 - Arbitrary File Upload v...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62129	WordPress Creator LMS plugin <= 1.2.21 - Arbitrary File U...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111406	WordPress MapSVG plugin <= 8.16.1 - Arbitrary File Uploa...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18143	Request a Quote for WooCommerce <= 2.9.2 - Unauthent...	Critical / 9.8	VULNCHECK KEV	✓ Blocked
CVE-2026-85097	Bricksforge <= 3.1.8.9 - Unauthenticated Arbitrary File Upl...	Critical / 9.8	VULNCHECK KEV	✓ Blocked
CVE-2026-96431	Flowring Agentflow 4.0 - Unrestricted Upload of File with ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-21589	CVE-2026-21589: This is a vulnerability in Bitbucket Data ...	Critical / 9.3	CISA KEV	✓ Blocked
CVE-2026-111497	Out-of-Bounds Write in Google Brotli Decoder	Critical / 9.2	CISA KEV	✓ Blocked
CVE-2026-17609	Super Forms <= 6.3.316 - Unauthenticated Arbitrary Direc...	Critical / 9.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-105032	EnergizeLab Eilik AI Skill Upload Unauthenticated Path Tra...	Critical / 9.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-70356	Toptech TMS7 and TopHAT Unrestricted Upload of File wi...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62025	WordPress Tailored Tools plugin <= 3.0.3 - Arbitrary File ...	Critical / 9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-109205	LogicalDOC Community Edition through 9.3 Unauthentica...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105862	Payload: Bypassed sanitization of user uploaded SVGs	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104471	YesWiki before 4.6.7 Unrestricted File Upload via Bazar C...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105868	Payload: Uploaded XML files could execute same-origin J...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115481	baserCMS: BcCustomContent file fields can be configure...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15723	Improper Neutralization of Special Elements used in an LD...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-108101	HortusFox through 6.3 Unrestricted File Upload via Plant ...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Insecure Design (File-Upload, LDAP): 65 blocked · avg CVSS 7.3 · 2 CISA KEV (continued)				
CVE-2026-89071	MOVEit Transfer LDAP injection in certificate-based authe...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-90979	Apache Karaf: LDAP filter injection in JAAS LDAP login m...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105679	Ghost: Stored XSS via File Uploads on Local Storage	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105649	Ghost: Stored XSS via SVG Uploads Bypassing Sanitization	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105651	Ghost: Stored XSS via Bookmark Card Images	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104637	onetwothreeneth HospitalManagementSystem controller....	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-112149	vraj404 Criminal-Management-System home.php move_...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108975	SourceCodester Library Management System add_admin....	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114262	file-management-system FileController.php store unrestri...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114259	oretnom23 file-management-system-php admin_class.p...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110025	slackero phpwcms Extension Check cnt23.article.inc.php...	Medium / 6.9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-108974	SourceCodester E-Learning System Users.php save_user...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108973	SourceCodester Contact Tracing System Users.php mov...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87800	IBM Cyber Fraud includes components with multiple kno...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105644	Ghost : Stored XSS via SVG Files in Content Imports	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102842	gedelumbung HospitalManagement KCFinder File Manag...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-110256	Dockhand before 1.0.19 Username Enumeration via LDAP I...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-71431	Frappe before 15.86.0 LDAP Injection via Unsanitized End...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-10759	BUG-000171040 Portal for ArcGIS has a security vulnerab...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59188	Part-DB: SVG Sanitization Bypass via Extension Spoofing ...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Insecure Design (File-Upload, LDAP): 65 blocked · avg CVSS 7.3 · 2 CISA KEV (continued)				
CVE-2026-101145	Eleveo Call Recording Software User Management userA...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-101071	Acrel Electric Unet Web Service Upload Endpoint upload ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116057	KodCloud KodExplorer Online Editor Save Endpoint editor...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93635	Zimbra Collaboration Suite LDAP Filter Injection via Unesc...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113382	arizu-id fast-tunnel Plugin Installer api_plugins.php extrac...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-3717	CV Builder – Professional Resume Builder SaaS <= 1.3.1 - ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-103541	formtools.org Form Tools Ajax actions.php uploadFile unr...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105389	feelec-yishu feelcrm-os UploadTicketFile Endpoint Uploa...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108922	KusalkaSilva Learning-Management-System upload_save...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-108801	prasathmani TinyFileManager tinyfilemanager.php move_...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-116044	prasathmani TinyFileManager Remote URL File Upload tin...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113393	DrayTek Vigor2960 commonupload mainfunction.cgi unr...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-114398	Trudesk through 1.2.11 Unrestricted File Upload via /settin...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102263	mwasikz robo-cafe-rms manage-food.php unrestricted u...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102366	mall4j through 4.0 Unrestricted File Upload in Admin File ...	Medium / 4.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93550	Veeqo for WooCommerce <= 2.2.8 - Subscriber+ Arbitrar...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93636	Zimbra Collaboration Suite LDAP Filter Injection via Calen...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76144	Genians, Inc Genian SSL PNS Unrestricted File Upload	Low / 1.8	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
XML Injection: 25 blocked · avg CVSS 7.6 · 0 CISA KEV				
CVE-2026-90531	Adobe Experience Manager | Improper Restriction of XM...	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-113582	Apache Abdera: XML external entity expansion in Atom d...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-115506	libexpat through 2.9.0 Denial of Service via Billion Laughs ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77090	CVFS Information Disclosure	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-106616	ColdFusion | Improper Restriction of XML External Entity ...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88789	Apache Camel Quarkus: Camel Quarkus: Forced Xalan Tr...	High / 8.6	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-92877	CVE-2026-92877: The JAXB factory methods historically...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88901	Apache Camel: Camel-Smooks XML External Entity Proce...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-14905	IBM DataPower Gateway XXE	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88794	XML External Entity injection in Sparx Enterprise Architect	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82386	Apache Roller: XML external entity processing in OPML b...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82376	Apache Roller: XML external entity processing in trackbac...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93891	Security Vulnerability identified in IBM TRIRIGA - XXE	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85250	Apache Camel: Camel-XPath XML External Entity Process...	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-85957	Improper XML external entity restriction in Progress Mark...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102155	Security Advisory 0190	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85970	Improper XML external entity restriction in Progress Mark...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-102127	Kiteworks Email Protection Gateway Improper Restriction ...	High / 7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-74030	Wazuh 3.9.0 before 4.14.8 Memory Exhaustion via SCA Y...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-104679	CVE-2026-104679: VOCALOID6 Editor provided by Yama...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
XML Injection: 25 blocked · avg CVSS 7.6 · 0 CISA KEV (continued)				
CVE-2026-97400	jdmpview / DTFJ reads arbitrary local files and makes arbi...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-111252	OpenNMS denial of service via XML entity expansion	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91858	Apache Camel: Camel-FOP Resolves External DTDs and E...	Medium / 6.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-83387	CVE-2026-83387: Vulnerability in the Oracle Java SE, Or...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83400	CVE-2026-83400: Vulnerability in the Oracle Java SE, Or...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
Identification & Authentication Failures: 3 blocked · avg CVSS 9.0 · 0 CISA KEV				
CVE-2026-109357	LibreNMS before 26.9.0 LDAP Filter Injection Authenticati...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94053	Apache MINA SSHD: LDAP injection in sshd-ldap	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-105630	Plane: Stored XSS via SVG attachment served inline on th...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
Security Logging & Monitoring Failures: 1 blocked · avg CVSS 5.3 · 0 CISA KEV				
CVE-2026-83380	CVE-2026-83380: Vulnerability in the Oracle Java SE, Or...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked

©2026 Indusface. All rights reserved.

ABOUT INDUSFACE

Autonomous Application Security for the AI Era

Indusface protects thousands of business-critical web, API and AI applications across 45+ countries. Backed by leading institutional investors, Indusface has been featured in research by Gartner, Forrester and IDC for its application security capabilities. The company maintains globally recognized security and compliance credentials, including ISO 27001, SOC 2 and PCI DSS, and supports GDPR-related requirements. Its globally distributed cloud infrastructure spans Asia, the Middle East, Europe and North America, delivering low-latency protection and regional data residency options for enterprises worldwide.

AppTrana is Indusface's autonomous enterprise application security platform that continuously discovers vulnerabilities, autonomously mitigates exploitable risks through virtual patching, and protects applications against DDoS attacks, malicious bots, API abuse and zero-day threats. Combining AI-powered intelligence, expert oversight and SLA-backed managed protection, AppTrana helps enterprises reduce the time from vulnerability discovery to protection while delivering audit-ready remediation evidence and managed security services focused on eliminating false positives.

Bangalore | Delhi | Mumbai | Vadodara | Dallas

www.indusface.com | sales@indusface.com | support@indusface.com

© 2026 Indusface Pvt. Ltd. All rights reserved.