

• MONTHLY BULLETIN • SEPTEMBER 2026

Zero-Day Vulnerability Coverage Report

September 2026: 808 zero-day attacks detected across AppTrana-protected traffic. All were autonomously blocked, with no manual intervention and no exposure window.

808

ZERO-DAYS BLOCKED

100%

CATEGORY COVERAGE

27

CISA KEV BLOCKED

9

AGENTIC AI / LLM
BLOCKED

In this Report

This report covers every zero-day vulnerability AppTrana blocked in September 2026. For each one, you will find exploitation status, severity, and the threat-intelligence context behind it.

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, September 2026. Each vulnerability ties to a CVE, a blocking rule, and a scanner check

Zero-Day Exposure Window: 0 Days

AppTrana's default rule set blocked 808 vulnerabilities in September 2026, with 100% coverage and no manual tuning required. The window between disclosure and protection, the window where exposure usually lives, stayed closed.

808

BLOCKED BY DEFAULT

AppTrana blocked 808 vulnerabilities by default, with 100% coverage across Cross-Site Scripting, Command Injection, SQL Injection, Path Traversal, SSRF, Injection, the file-upload pattern of Insecure Design, Uncontrolled Resource Consumption, and XML Injection.

27

CISA KEV CLOSED

CISA confirmed 27 of these vulnerabilities as actively exploited, 22 of them in a Command Injection cluster that includes N-able N-central, JetBrains TeamCity, Gitea, and Langflow.

Day zero

PUBLIC EXPLOIT CLOSED

A public exploit for the Drupal core SQL injection (CVE-2026-9082, CVSS 9.8) was published on Exploit-DB while the CVE sat on CISA's KEV catalog. AppTrana blocked it on default rules, with no signature work and no patch dependency.

9

AGENTIC AI & LLM CLOSED

AppTrana autonomously blocked 9 AI/LLM-related CVEs in September 2026, spanning RAG data exposure, prompt injection, and agent-to-tool trust boundary violations

Coverage by Category

Cross-Site Scripting was the largest category by volume at 271. Command Injection carried the most risk, with 101 Critical-severity CVEs and 22 of the 27 CISA KEV entries, including the N-able N-central and Gitea disclosures covered in Section 07. Coverage stayed at 100% across every category.

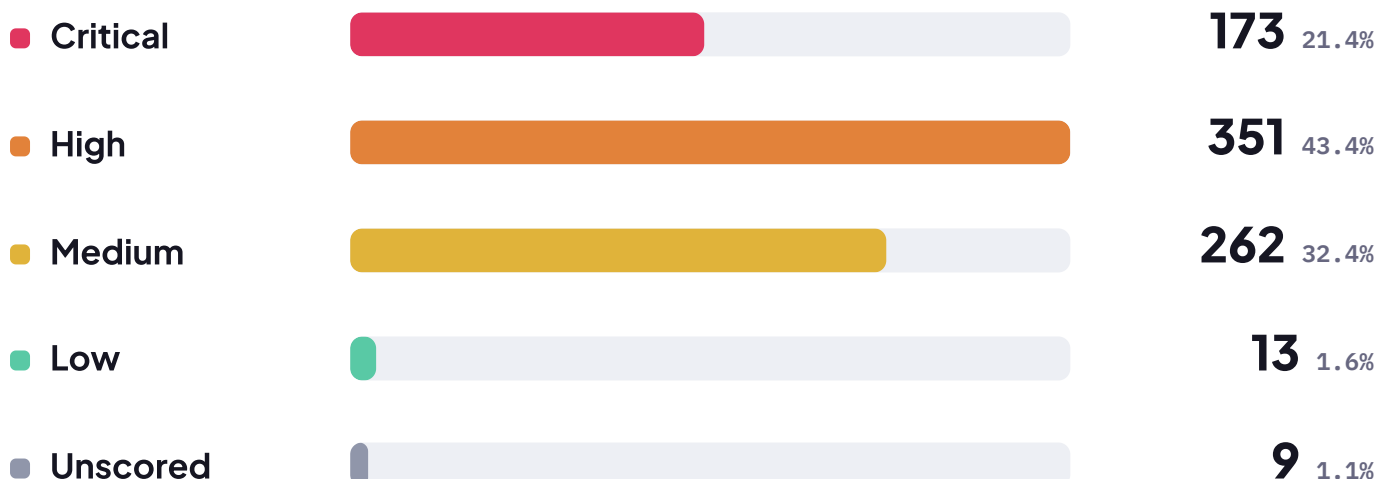
CATEGORY	BLOCKED	CRITICAL	HIGH	AVG CVSS	PEAK
Cross-Site Scripting	271	8	114	6.6	10.0
Command Injection	231	101	106	8.7	10.0
SQL Injection	105	33	46	8.1	10.0
Path Traversal	77	9	37	7.4	10.0
SSRF	63	10	26	7.2	10.0
Injection	25	0	8	6.0	8.8
Insecure Design (File-Upload)	17	10	3	8.7	10.0
Uncontrolled Resource Consumption	13	0	9	7.0	8.7
XML Injection	6	2	2	7.8	9.8

Severity Snapshot

Severity didn't change the outcome. 524 of the 808 blocked vulnerabilities (64.9%) were Critical or High, the tier that usually requires emergency patching. All were blocked at the edge automatically. It worked without needing an emergency patch, an out-of-band change, or any manual fix. A further 9 (1.1%) had no published CVSS score yet and were still blocked, on the same default rules.



BREAKDOWN BY SEVERITY



524

CRITICAL + HIGH SEVERITY

These are the vulnerabilities most organizations rush to patch first. An open exposure window here carries the highest risk. AppTrana had already blocked every one of them at the edge. No emergency patch cycle. No manual configuration needed.

Exploitation & KEV Status

Of the 808 vulnerabilities blocked, 27 were already confirmed by CISA as actively exploited and listed in the Known Exploited Vulnerabilities (KEV) catalog (3.3%).

27

CISA KEV • ACTIVELY EXPLOITED
3.3%

25

PUBLIC EXPLOIT / POC AVAILABLE
3.1%

NOTABLE CISA KEV ENTRIES BLOCKED

CVE	SEVERITY / CVSS	CATEGORY
CVE-2026-86218	Critical / 10.0	Command Injection
CVE-2026-85706	Critical / 10.0	Path Traversal
CVE-2026-83548	Critical / 10.0	SSRF
CVE-2026-9082	Critical / 9.8	SQL Injection
CVE-2026-60004	Critical / 9.8	Command Injection
CVE-2026-9198	Critical / 9.8	Command Injection
CVE-2023-42793	Critical / 9.8	Command Injection
CVE-2026-42271	High / 8.7	Command Injection

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 9 AI/LLM-tagged CVEs in September 2026, most of them in RAGFlow and LiteLLM. Two were Critical, led by a RAGFlow server-side template injection leading to remote code execution (CVE-2026-45312, CVSS 9.9). A LiteLLM command-execution flaw (CVE-2026-42271) is listed on CISA's KEV catalog.



THREAT TAG	CVES	WHAT IT COVERS
RAG Data Exposure	4	RAG pipelines and connected data sources
General LLM Application Risk	3	LLM application code and integrations
Agent-Framework Risk	2	Autonomous-agent frameworks and trust boundaries
Prompt-Injection Vectors	1	Direct or indirect prompt-injection paths
Embedding & Vector Risk	1	Embedding models and vector stores

Vulnerability Trend

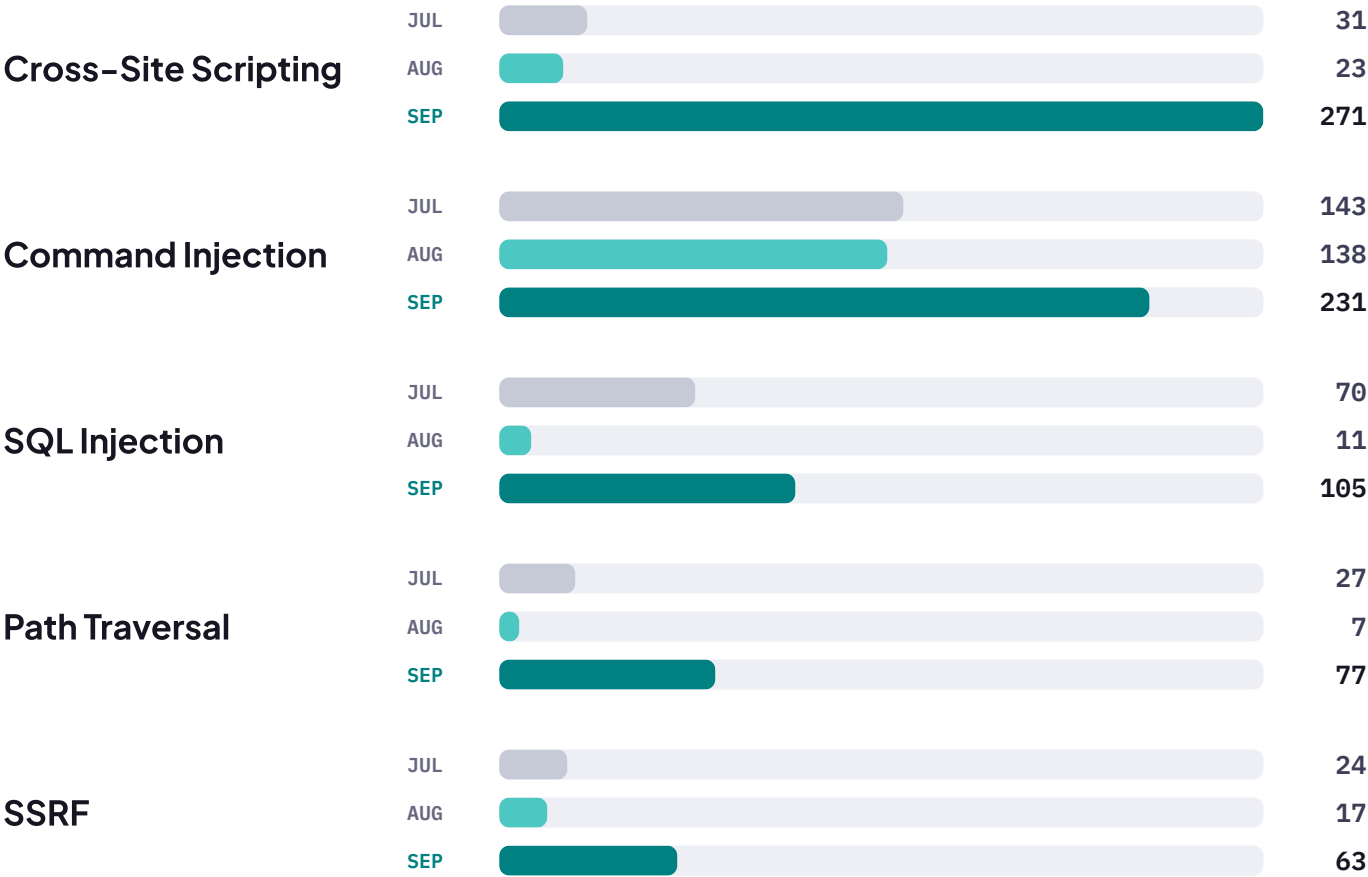
Volume rose sharply in September. Cross-Site Scripting climbed from 23 in August to 271, and Command Injection rose from 138 to 231. SQL Injection, Path Traversal, and SSRF all exceeded their July levels. Across all five categories, AppTrana held 100% coverage every month, with no custom rule work and no emergency patch cycles.

TOP FIVE CATEGORIES · THREE-MONTH COMPARISON

July

August

September



High-Profile Attacks Blocked

THREAT	SEVERITY / CVSS	EXPLOITATION
N-able N-central Unauthenticated RCE CVE-2026-86218	Critical / 10.0	CISA KEV
GitLab Path Traversal CVE-2026-85706	Critical / 10.0	CISA KEV
SonicWall SMA1000 Pre-Auth SSRF CVE-2026-83548	Critical / 10.0	CISA KEV
Drupal Core SQL Injection CVE-2026-9082	Critical / 9.8	CISA KEV
Gitea Git-Hook RCE CVE-2026-60004	Critical / 9.8	CISA KEV

N-able N-central: fourth hotfix in five weeks

N-able issued its fourth N-central hotfix in five weeks for an unauthenticated remote-code-execution flaw (CVE-2026-86218, Critical, CVSS 10.0). The CVE is on CISA's KEV catalog and a proof-of-concept is public. AppTrana's Command Injection policy blocked it by default.

GitLab: path traversal with 93% EPSS

CVE-2026-85706 (Critical, CVSS 10.0), a path traversal in GitLab, is on CISA's KEV catalog with a 93% EPSS exploitation probability. AppTrana's Local File Inclusion Protection Policy blocked the request pattern.

SonicWall SMA1000: pre-authentication SSRF

A pre-authentication SSRF in the SMA1000 Work Place interface (CVE-2026-83548, Critical, CVSS 10.0) is KEV-listed, with a weaponized proof-of-concept and a public Nuclei template. AppTrana's SSRF rules blocked it by default.

Drupal core: highly critical SQL injection

SA-CORE-2026-004, a SQL injection in Drupal core (CVE-2026-9082, Critical, CVSS 9.8), is on CISA's KEV catalog and has a public exploit on Exploit-DB. The default rule set closed it without a custom signature.

Gitea: RCE through Git hook installation

CVE-2026-60004 (Critical, CVSS 9.8) allows remote code execution through diffpatch Git hook installation in Gitea. It is exploitable by any user with write access to a repository, is KEV-listed, and has a public proof-of-concept and a Nuclei template. AppTrana blocked it on default rules.

Blocked Vulnerabilities by Category

Each of the 808 vulnerabilities blocked in September 2026 traces back to a published advisory (CVE, GHSA, JVN or CERT-EU) and a specific blocking rule, ready for audit or compliance review.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 271 blocked · avg CVSS 6.6 · 0 CISA KEV				
CVE-2026-19471	Rockwell Automation ArmorStart LT	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85061	MapLibre GL JS: XSS Sanitizer Bypass in DOM.sanitize() ...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84648	CVE-2026-84648: In Jenkins 2.579 and earlier, LTS 2.56...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84665	CVE-2026-84665: Jenkins SonarQube Scanner Plugin 2....	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84673	CVE-2026-84673: Jenkins Customizable Header Plugin ...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69356	Microsoft Exchange Server Spoofing Vulnerability	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84189	LibreNMS before 26.7.0 Stored XSS via Oxidized API	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76178	Multiple vulnerabilities in Ocsreports for OCS Inventory NG	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14334	Booking calendar, Appointment Booking System <= 3.2.3...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-16617	Simple File List <= 6.3.11 - Unauthenticated Stored XSS v...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78333	12 Step Meeting List 3.17 - 3.19.16 - Unauthenticated Sto...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 271 blocked · avg CVSS 6.6 · 0 CISA KEV (continued)				
CVE-2026-76789	Slider Hero < 9.1.3 - Unauthenticated Stored XSS via Slid...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83605	xmldom: Attribute name injection via setAttribute() bypas...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-47759	TinyMCE Cross-Site Scripting (XSS) vulnerability using t...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-47761	TinyMCE Cross-Site Scripting (XSS) vulnerability using ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-47762	TinyMCE Cross-Site Scripting (XSS) vulnerability throug...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9585	Unauthenticated Reflected Cross-Site Scripting (XSS) in ...	High / 8.6	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-2026-73781	Authenticated Stored Cross-Site Scripting Vulnerability (...)	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85613	OpenPanel before 2.3.0 Unauthenticated XSS via SVG Fa...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84370	SVGO: removeScripts allows executable links through na...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83946	Azure Portal Spoofing Vulnerability	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83607	xmldom: Element name injection via createElement() byp...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57440	Mediawiki EmbedVideo Extension has stored XSS via mal...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-53610	GLPI: Reflected XSS in dashboards	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18983	One User Avatar User Profile Picture <= 2.5.4 - Authenti...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73546	envoy: envoy: stored XSS through dynamically generated...	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-91775	LimeSurvey Community Edition 7.0.14 - Reflected XSS th...	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69402	Microsoft Office SharePoint Spoofing Vulnerability	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69417	Microsoft Office SharePoint Spoofing Vulnerability	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 271 blocked · avg CVSS 6.6 · 0 CISA KEV (continued)				
CVE-2026-66077	RabbitMQ: Stored XSS via TLS peer-certificate DN in ma...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15780	WP Statistics <= 14.16.8 - Unauthenticated Stored Cross...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75981	TranslatePress – Translate Multilingual sites with AI Trans...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18409	WPForms Pro <= 2.0.0.2 - Unauthenticated Stored Cross...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18109	W3 Total Cache <= 2.10.3 - Unauthenticated Stored Cros...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-19760	WP Fastest Cache <= 1.5.0 - Unauthenticated Stored Cro...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18146	Fluent Forms <= 6.2.11 - Unauthenticated Stored Cross-...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18978	LiteSpeed Cache <= 7.8.1 - Unauthenticated Stored Cros...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84773	WordPress EWWW Image Optimizer plugin <= 8.7.6 - Cro...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18331	Formidable Forms <= 6.33.1 - Unauthenticated Stored Cr...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-6286	Booking for Appointments and Events Calendar <= 2.2 - ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-6176	Customer Reviews for WooCommerce <= 5.106.0 - Unaut...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18328	Forminator Forms <= 1.57.0 - Unauthenticated DOM-Bas...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18324	Forminator Forms <= 1.57.0.1 - Unauthenticated Stored C...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18323	Forminator Forms <= 1.57.0.2 - Unauthenticated Stored C...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77365	Optimole <= 4.2.10 - Unauthenticated Stored Cross-Site ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76053	TranslatePress <= 3.3.3 - Unauthenticated Stored Cross-...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-5934	WP Rocket <= 3.21.0.1 - Unauthenticated Stored Cross-S...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66582	WordPress TranslatePress plugin <= 3.3.2 - Cross Site Sc...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66584	WordPress 12 Step Meeting List plugin <= 3.19.16 - Cross...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 271 blocked · avg CVSS 6.6 · 0 CISA KEV (continued)				
CVE-2026-66607	WordPress Advance Product Search plugin <= 1.4.8 - Cro...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73358	WordPress Affiliates Manager plugin <= 2.9.53 - Cross Si...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66612	WordPress Aora theme <= 1.3.19 - Cross Site Scripting (X...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73338	WordPress Autopay plugin <= 5.0.0 - Cross Site Scripting...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66598	WordPress B2BKing Premium plugin <= 5.6.07 - Cross Sit...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73182	WordPress BBQ Pro plugin <= 3.9 - Cross Site Scripting (...)	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32547	WordPress BP Better Messages plugin <= 2.15.22 - Cros...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73378	WordPress Contact Form by Supsysic plugin < 1.10.0 - C...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-61986	WordPress Contest Gallery plugin <= 30.0.5 - Cross Site ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-68567	WordPress Convert Pro plugin <= 1.0.1 - Cross Site Script...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-28162	WordPress Events Made Easy plugin <= 3.2.5 - Cross Sit...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66673	WordPress Flatastic theme <= 2.0 - Reflected Cross Site ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66633	WordPress Fluent Forms Pro Add On Pack plugin < 6.2.12...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66616	WordPress Form Maker by 10Web plugin <= 1.15.48 - Cro...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66614	WordPress SEO Plugin by Squirrly SEO plugin <= 14.2.2 - ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66604	WordPress GeoDirectory plugin <= 2.8.173 - Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73184	WordPress Global Gallery plugin <= 11.1.2 - Cross Site Sc...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66581	WordPress JetEngine plugin <= 3.8.14.1 - Cross Site Scri...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66629	WordPress Kirki plugin <= 6.2.3 - Cross Site Scripting (X...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73351	WordPress WordPress Social Login and Register plugin <...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 271 blocked · avg CVSS 6.6 · 0 CISA KEV (continued)				
CVE-2026-66596	WordPress Newsletter plugin <= 9.3.3 - Cross Site Script...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-68564	WordPress NotificationX Pro plugin <= 3.1.4 - Cross Site ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66611	WordPress Paymob for WooCommerce plugin <= 4.1.10 - ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66615	WordPress Podlove Podcast Publisher plugin <= 4.5.4 - C...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73190	WordPress WPDM – Premium Packages plugin <= 7.0.5 - ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73361	WordPress Recipe Card Blocks for Gutenberg & Element...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73354	WordPress SimplyRETS Real Estate IDX plugin <= 3.2.8 - ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66606	WordPress SmartSMTP plugin <= 1.2.0 - Cross Site Scrip...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66623	WordPress Social Media & Share Icons plugin <= 2.9.9 - ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66605	WordPress Swatchly – WooCommerce Variation Swatche...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66590	WordPress Tagembed plugin <= 7.4 - Cross Site Scriptin...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66621	WordPress Ultimate Dashboard Pro plugin <= 3.11.2 - Cro...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73375	WordPress Ultimate Maps by Supsysytic plugin < 1.5.0 - C...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73362	WordPress URL Shortify plugin <= 2.5.0 - Cross Site Scri...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66610	WordPress Urna theme <= 2.6.2 - Cross Site Scripting (X...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73342	WordPress WP Multilang plugin <= 2.4.31 - Cross Site Sc...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66599	WordPress WPComplete plugin <= 2.9.5.6 - Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66597	WordPress wpDataTables plugin <= 6.5.1.4 - Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32333	WordPress Mayosis Core plugin <= 5.4.7 - Reflected Cro...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-28569	WordPress SSL Zen plugin <= 4.7.43 - Reflected Cross Si...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 271 blocked · avg CVSS 6.6 · 0 CISA KEV (continued)				
CVE-2026-16570	NextScripts: Social Networks Auto-Poster < 4.4.8 - Refle...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-19056	ProSolution WP Client < 2.0.11 - Reflected XSS via 'page' ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-19055	ProSolution WP Client < 2.0.11 - Reflected XSS via Multipl...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-28177	WordPress Popup Maker plugin <= 1.23.0 - Cross Site Sc...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82883	WordPress Login With Ajax plugin <= 4.5.1 - Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81775	WordPress Estatik plugin <= 4.3.4 - Cross Site Scripting (...)	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81292	WordPress Simple Payment plugin <= 2.5.1 - Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81295	WordPress Under Construction plugin <= 5.82 - Cross Si...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81300	WordPress Calculation For Contact Form 7 plugin <= 1.0 ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81773	WordPress Ninja Forms File Uploads Extension plugin <= ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81776	WordPress WP QuickLaTeX plugin <= 3.8.8 - Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84763	WordPress RTMKit plugin <= 2.1.5 - Cross Site Scripting (...)	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84765	WordPress Breadcrumb NavXT plugin <= 7.5.1 - Cross Sit...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84812	WordPress BP Better Messages plugin <= 2.15.27 - Cross...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84848	WordPress Quick Event Manager plugin <= 9.17 - Cross S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82224	WordPress SliceWP plugin <= 1.2.10 - Cross Site Scriptin...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78289	WordPress CozyStay theme <= 1.10.0 - Cross Site Scripti...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78281	WordPress CP Media Player plugin <= 1.3.0 - Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81764	WordPress Email Essentials plugin <= 6.0.6 - Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81290	WordPress Email Subscribers & Newsletters plugin <= 5....	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 271 blocked · avg CVSS 6.6 · 0 CISA KEV (continued)				
CVE-2026-81760	WordPress JetEngine plugin <= 3.8.14.2 - Cross Site Scri...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81298	WordPress LeadConnector plugin <= 4.0.5 - Cross Site S...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78283	WordPress Music Player for WooCommerce plugin <= 1.8...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78261	WordPress Realtyna Organic IDX plugin plugin <= 5.4.1 - ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82229	WordPress WordPress Social Login and Register plugin <...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81768	WordPress Super Store Finder plugin <= 7.10 - Cross Site...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81765	WordPress Tailored Tools plugin <= 3.0.2 - Cross Site Scr...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81291	WordPress Uncode theme <= 2.12.7 - Cross Site Scriptin...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78293	WordPress WP w3all phpBB plugin <= 3.0.6 - Cross Site ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14307	Geotargeting WP < 3.5.6.2 - Reflected XSS	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9588	Authenticated Stored Cross-Site Scripting (XSS) in Switc...	High / 7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96875	Reflected XSS in Cargo Drilldown hierarchy filters	Medium / 6.9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-96876	Anonymous reflected XSS in CargoExport invalid-alias er...	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-2026-96878	Cargo Exhibit field alias allows stored XSS	Medium / 6.9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-15253	Easy Media Replace <= 0.2.0 - Author+ Stored XSS via At...	Medium / 6.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-19615	Admin and Site Enhancements < 9.0.1 - Author+ Stored X...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-19697	GutenKit < 2.5.0 - Author+ Stored XSS via SVG Upload	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18202	JetEngine < 3.8.14 - Author+ Stored XSS via SVG Upload	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-16260	Post Grid, Slider & Carousel Ultimate < 1.8.1 - Contributor...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 271 blocked · avg CVSS 6.6 · 0 CISA KEV (continued)				
CVE-2026-82884	All in One SEO < 5.0.0.1 - Contributor+ Stored XSS via ai-...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-19226	Royal Elementor Addons < 1.7.1066 - Contributor+ Stored...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14835	SOGO Add Script to Individual Pages Header Footer <= 3...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76546	Profile Builder < 4.0.1 - Contributor+ Stored XSS via Form...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-74992	Kirki < 6.2.3 - Editor+ Stored XSS via Font Zip Upload	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66603	WordPress Draft List plugin <= 2.6.4 - Cross Site Scriptin...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66637	WordPress Featured Video Plus plugin <= 2.3.3 - Cross S...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66638	WordPress Frontend Admin by DynamiApps plugin <= 3.2...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-68565	WordPress GeoDirectory plugin <= 2.8.172 - Cross Site S...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66640	WordPress Login With Ajax plugin <= 4.5.1 - Cross Site S...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66591	WordPress Media Library Assistant plugin <= 3.39 - Cros...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66601	WordPress Media Library Assistant plugin <= 3.39 - Cros...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66645	WordPress Table Of Contents Block plugin <= 1.5.0 - Cro...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66644	WordPress Typing Effect plugin <= 1.3.7 - Cross Site Scri...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66641	WordPress Video Conferencing with Zoom plugin <= 4.6....	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66636	WordPress Wise Chat plugin <= 3.4 - Cross Site Scriptin...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73402	WordPress WP BASE Booking plugin <= 6.3.2 - Cross Sit...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66646	WordPress WP Tab Widget plugin <= 1.2.11 - Cross Site S...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73359	WordPress WP Cookie Notice for GDPR, CCPA & ePrivac...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66639	WordPress WPZOOM Forms – Contact Form plugin for G...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 271 blocked · avg CVSS 6.6 · 0 CISA KEV (continued)				
CVE-2026-66643	WordPress Wufoo Shortcode plugin <= 1.55 - Cross Site ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84781	WordPress Gallery PhotoBlocks plugin <= 1.3.4 - Cross Si...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81281	WordPress Graphene theme <= 2.9.4 - Cross Site Scripti...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81282	WordPress Product Variations Swatches for WooCommer...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85302	WordPress WPKoi Templates for Elementor plugin <= 3.7...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85303	WordPress Booking and Rental Manager plugin <= 2.7.7 - ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78273	WordPress Fluent Boards Pro plugin <= 2.0.11 - Cross Sit...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78290	WordPress Magazine Blocks plugin <= 1.8.6 - Cross Site ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-27086	WordPress WoodMart theme < 8.3.8 - Cross Site Scriptin...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69642	Skype for Business Spoofing Vulnerability	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63523	Skype for Business Spoofing Vulnerability	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-4559	Image Photo Gallery Final Tiles Grid <= 3.6.12 - Authentic...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15446	EWWW Image Optimizer <= 8.7.3 - Authenticated (Contri...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-4561	MC4WP: Mailchimp for WordPress <= 4.12.0 - Authentica...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15421	Speed Optimizer <= 7.8.0 - Authenticated (Contributor+) ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-3129	LiteSpeed Cache <= 7.7 - Authenticated (Author+) Store...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15798	Smart Slider 3 <= 3.5.1.38 - Authenticated (Contributor+)...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15066	Loco Translate <= 2.8.7 - Authenticated (Translator+) Sto...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-3851	Divi <= 4.27.6 - Authenticated (Contributor+) Stored Cro...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-3850	Divi <= 4.27.6 - Authenticated (Contributor+) Stored Cro...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 271 blocked · avg CVSS 6.6 · 0 CISA KEV (continued)				
CVE-2025-7963	Easy Waveform Player <= 1.2.2 - Authenticated (Contribu...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-2573	GutenKit <= 2.4.4 - Authenticated (Contributor+) Stored ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-3852	Divi <= 4.27.6 - Authenticated (Contributor+) Stored Cro...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18547	Ultimate Member <= 2.12.1 - Authenticated (Subscriber+)...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-6128	All-in-One WP Migration Unlimited Extension <= 2.84 - A...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-16654	Avada (Fusion) Builder <= 3.15.6 - Authenticated (Contri...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-6178	Betheme <= 28.4 - Authenticated (Contributor+) Stored ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75019	Cozy Blocks <= 2.2.16 - Authenticated (Contributor+) Sto...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76128	eCommerce Product Catalog <= 3.5.10 - Authenticated (...)	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-3423	Envira Gallery <= 1.12.4 - Authenticated (Author+) Stored...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76063	FundEngine <= 1.8.1 - Authenticated (Subscriber+) Store...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-5510	GiveWP <= 4.14.4 - Authenticated (Contributor+) Stored ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-5092	Greenshift <= 12.8.9 - Authenticated (Contributor+) Stor...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-19943	Gutenverse <= 4.0.2 - Authenticated (Contributor+) Stor...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-3002	Gutenverse <= 4.0.2 - Authenticated (Contributor+) Stor...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18100	MetForm <= 4.1.8 - Authenticated (Contributor+) Stored ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-9878	Password Protect WordPress Lite <= 1.9.21 - Authentica...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-2388	Reviews and Rating – Google Reviews <= 5.10 - Authenti...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12561	tagDiv Composer <= 5.4.5 - Authenticated (Contributor+...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18512	TranslatePress <= 3.2.6 - Authenticated (Subscriber+) St...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 271 blocked · avg CVSS 6.6 · 0 CISA KEV (continued)				
CVE-2026-84463	Zammad: Stored HTML injection in Knowledge Base vide...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93460	CVE-2026-93460: A stored cross-site scripting vulnera...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93463	CVE-2026-93463: Cross-Site Scripting via Script Valid...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93464	CVE-2026-93464: A stored cross-site scripting vulnera...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-19712	Masteriyo LMS < 2.3.3 - Instructor+ Stored XSS via Quiz ...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85227	Reflected Cross-Site Scripting in MISP Event Filtering via...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84774	WordPress WP Statistics plugin <= 14.16.11 - Cross Site S...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-4246	ElementsKit Pro <= 4.10.1 - Unauthenticated Stored Cros...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-17089	Events Manager <= 7.4.0.1 - Reflected Cross-Site Scripti...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-80180	Apache Allura: Stored XSS via markdown HTML processing	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85229	Apache SkyWalking: CWE-79 stored XSS in Booster UI d...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-80190	Apache Allura: Stored XSS via code repositories	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-72925	SWC HTML minifier may allow script element breakout w...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84369	SVGO: removeScripts incompletely sanitizes executable ...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77490	Microsoft Edge (Chromium-based) Spoofing Vulnerability	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82773	Multiple vulnerabilities in Contec CONPROSYS series (C...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82776	Multiple vulnerabilities in Contec CONPROSYS series (C...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82788	Multiple vulnerabilities in Contec CONPROSYS series (C...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-58504	draw.io: Stored XSS on file open via editable=0 sibling cel...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93405	Mailspring: Stored XSS in attachment quick preview (uns...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 271 blocked · avg CVSS 6.6 · 0 CISA KEV (continued)				
CVE-2026-88996	WPForms <= 2.0.2 - Reflected Cross-Site Scripting via 'p...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-27365	WordPress PublishPress Series plugin <= 2.17.0 - Cross S...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84815	WordPress Enfold theme <= 8.0 - Cross Site Scripting (X...	Medium / 5.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96873	Reflected XSS in CirrusSearch debug explain output	Medium / 5.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-84232	pulpcore: python-pulpcore: Stored cross-site scripting vi...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84371	sanitize-html: stored XSS via SVG SMIL URI-list scheme-...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56128	pfSense Plus < 26.07 / CE < 2.9.0 Stored XSS via firewall...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81635	Multiple vulnerabilities in SHIRASAGI (CVE-2026-81635)	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82582	Multiple vulnerabilities in SHIRASAGI (CVE-2026-82582)	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82763	Multiple vulnerabilities in Contec FLEXLAN series (CVE-2...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82769	Multiple vulnerabilities in Contec FLEXLAN series (CVE-2...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82771	Multiple vulnerabilities in Contec FLEXLAN series (CVE-2...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82781	Multiple vulnerabilities in Contec CONPROSYS series (C...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-48541	Krayin CRM 2.2.6 Stored Template Injection XSS via Cont...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-48542	Krayin CRM 2.2.6 Stored Template Injection XSS via Prod...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82451	Formwork < 2.3.11 Stored XSS via Referer Header	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85158	AVideo Reflected XSS via videoEmbedded.php link param...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85159	AVideo Reflected XSS via cancelUri in userLogin.php	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78000	Joomla Extension - j2commerce.com - Open redirect in c...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85230	MISP Dashboard Button Widget Allows Persistent JavaSc...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 271 blocked · avg CVSS 6.6 · 0 CISA KEV (continued)				
CVE-2026-85453	MOOS core-moos through 10.4.0 MOOSDB HTTP Pages ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82535	Chamilo LMS Stored XSS via Survey Answer Submission i...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-90443	Cross-site Scripting in Malcolm	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63216	Zammad: Stored XSS via unescaped option labels in the ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85021	langgenius dify Splash Layout splash.tsx router.replace c...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85382	light0011 cms Chapter Content Output oneChapter.tpl ht...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82767	Multiple vulnerabilities in Contec FLEXLAN series (CVE-2...	Medium / 5.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81887	Livewire DOM-based cross-site scripting during client-si...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73524	Cypht < 2.12.2 XSS via FROM Email Header in Contacts M...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75134	SEOWriting WordPress Plugin 1.12.5 Stored XSS via ifram...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56126	pfSense Plus < 26.07 / CE < 2.9.0 Stored XSS via status_...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56127	pfSense Plus < 26.07 / CE < 2.9.0 Stored XSS via firewall...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82024	LearnPress WordPress Plugin < 4.4.6 Stored XSS via Qui...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73319	XenForo < 2.3.13 XSS via Dynamic Redirect Handler	Medium / 5.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-93339	Ditty < 3.1.70 Stored XSS via Layout Tag Wrapper Attribute	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-45381	Tautulli: Reflected XSS in `/search` endpoint	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97062	Aureus ERP 1.6.0 Stored XSS via SVG File Upload	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84437	OpenCart Autocomplete Workflow address.php cross sit...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85022	langgenius dify WebApp Sign-In mail-and-password-aut...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85207	itsourcecode Online Medicine Delivery System index.php...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 271 blocked · avg CVSS 6.6 · 0 CISA KEV (continued)				
CVE-2026-85405	Eleveo Call Recording Software roleAddAction.do cross s...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85406	Eleveo Quality Management Conversation Review cross s...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85541	Interinfo DreamMaker - Reflected Cross-site Scripting	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14287	TenWeb Speed Optimizer < 2.33.5 - Unauthenticated Sto...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15452	Smash Balloon Social Photo Feed <= 6.11.3 - Reflected C...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76579	LiteSpeed Cache <= 7.9 - Reflected Cross-Site Scripting ...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69690	Microsoft Office SharePoint Spoofing Vulnerability	Medium / 4.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-46650	Joplin: Stored XSS in public share viewer via javascript: U...	Medium / 4.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97322	YunaiV/zhijiantianya ruoyi-vue-pro File Upload FileContro...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13416	CMP - Coming Soon & Maintenance < 4.1.18 - Editor+ Sto...	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14325	Drag and Drop Multiple File Upload for Contact Form 7 < ...	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78364	MW WP Form < 5.1.6 - Editor+ Stored XSS via Inquiry Dat...	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69615	Microsoft Office SharePoint Spoofing Vulnerability	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97897	Krayin laravel-crm TinyMCE Media Upload Sanitizer.php ...	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96874	Stored XSS in Cargo Drilldown tab names	Low / 2.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-84911	AI (Artificial Intelligence) - Moderately critical - Cross sit...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87949	SAML SSO - Service Provider - Moderately critical - Cros...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87948	SAML SSO - Service Provider - Moderately critical - Cros...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96382	Diba carousel slider - Moderately critical - Cross Site Scri...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96361	Webform - Moderately critical - Cross-site scripting - SA...	Unscored	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 231 blocked · avg CVSS 8.7 · 22 CISA KEV				
CVE-2024-3400	PAN-OS: Arbitrary File Creation Leads to OS Command In...	Critical / 10	CISA KEV	✓ Blocked
CVE-2026-73343	WordPress WP Compress plugin < 7.20.01 - Remote Cod...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82222	Unauthenticated PHP Object Injection to Remote Code E...	Critical / 10	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-12663	Rockwell Automation ControlFLASH	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86218	N-able Issues Fourth N-central Hotfix in Five Weeks for U...	Critical / 10	CISA KEV	✓ Blocked
CVE-2026-84650	CVE-2026-84650: In Jenkins 2.579 and earlier, LTS 2.56...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84670	CVE-2026-84670: Jenkins Performance Plugin 1015.v09...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84671	CVE-2026-84671: Jenkins File Parameter Plugin 425.v3f...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82004	Adobe Campaign Classic (ACC) Improper Neutralization ...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75595	Netty: SNI Routing Bypass via Fragmented TLS ClientHell...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97359	HFS2 2.4.0 RCE via Multipart Upload Filename Template I...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73992	WordPress Query Wrangler plugin <= 1.5.57 - Remote Co...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32444	WordPress Cwicyly plugin <= 1.4.4 - Remote Code Executi...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-45312	RAGFlow: Server-Side Template Injection in Prompt Gene...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73294	Semaphore U: OS Command Injection	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85885	Microsoft 365 Copilot Elevation of Privilege Vulnerability	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77602	OpenC3 COSMOS: Authenticated remote code execution...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2023-42793	CVE-2023-42793: In JetBrains TeamCity before 2023.05...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2024-47575	CVE-2024-47575: A missing authentication for critical fu...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2026-80428	ILIAS PHP Object Injection via Shibboleth Logout	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 231 blocked · avg CVSS 8.7 · 22 CISA KEV (continued)				
CVE-2026-47884	org.springframework/spring-webmvc: Spring Framework...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66613	WordPress JetEngine plugin <= 3.8.14 - Remote Code Ex...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-4703	WS Form LITE <= 1.10.80 - Unauthenticated PHP Object I...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66672	WordPress Flatastic theme <= 2.0 - PHP Object Injection ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66583	WordPress Forminator plugin <= 1.57.0 - PHP Object Inje...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66650	WordPress FreightCo theme <= 1.1.15 - PHP Object Inject...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73993	WordPress FundEngine plugin <= 1.7.9 - PHP Object Injec...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73389	WordPress Kalles Addons plugin <= 1.0.6 - PHP Object Inj...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73364	WordPress Flexible Subscriptions plugin <= 1.8.1 - PHP O...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15748	Forminator Forms <= 1.56.1 - Unauthenticated Arbitrary F...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73341	WordPress RegistrationMagic plugin <= 6.0.9.7 - PHP Obj...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73380	WordPress Popup by Supsysytic plugin <= 1.13.0 - PHP Ob...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73376	WordPress Ultimate Maps by Supsysytic plugin < 1.5.0 - P...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73397	WordPress Youzify plugin <= 1.3.7 - Deserialization of unt...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78032	Multiple vulnerabilities in SOY series (CVE-2026-78032)	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73827	Multiple vulnerabilities in SOY series (CVE-2026-73827)	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77838	Multiple vulnerabilities in SOY series (CVE-2026-77838)	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78238	Multiple vulnerabilities in SOY series (CVE-2026-78238)	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2023-27350	CVE-2023-27350: This vulnerability allows remote attac...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2026-9198	[webapps] Langflow 1.10.0 - RCE	Critical / 9.8	CISA KEV	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 231 blocked · avg CVSS 8.7 · 22 CISA KEV (continued)				
CVE-2026-55559	Yamcs: Remote Code Execution via instance-template ar...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-20212	Cisco Nexus 3000 and 9000 Series Switches Silicon One...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-24770	RAGFlow Affected by Zip Slip Remote Code Execution (R...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2023-46747	Overview of F5 vulnerabilities (October 26, 2023) (CVE-...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2026-84753	WordPress Mail Mint plugin <= 1.31.0 - PHP Object Injecti...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-84834	WordPress JobSearch plugin <= 3.2.0 - PHP Object Injec...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18080	ERP: Complete HR, Accounting & CRM Suite Built for Wo...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14494	Sigma Forms Pro <= 1.4.5 - Unauthenticated Unauthentic...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78286	WordPress Geo Controller plugin <= 8.9.8 - PHP Object I...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78292	WordPress Hash Form plugin <= 1.4.1 - PHP Object Inject...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82226	WordPress Tickera plugin <= 3.6.0.2 - PHP Object Injecti...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-85504	CVE-2026-85504: FreeIPMI before 1.6.19 has a stack-ba...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62928	CVE-2026-62928: XING CPTrans-ME-X contains an OS ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66840	CVE-2026-66840: XING CPTrans-ME-X contains an Exp...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69657	CVE-2026-69657: XING CPTrans-ME-X contains a Use o...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70403	CVE-2026-70403: XING CPTrans-ME-X contains a Use o...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82923	AI Website Builder (GitHub build) 1.0.0 - Unauthenticated...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66302	Skype for Business Remote Code Execution Vulnerability	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2022-24086	Adobe Commerce checkout improper input validation lea...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2026-60004	Gitea: Remote Code Execution via diffpatch Git Hook Inst...	Critical / 9.8	CISA KEV	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 231 blocked · avg CVSS 8.7 · 22 CISA KEV (continued)				
CVE-2026-84372	Predis: Redis command injection and denial of service via...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85102	Improper Certificate Validation in Quantum Security Gate...	Critical / 9.8	CISA KEV	✓ Blocked
CERTEU:2026-012	2026-012: Critical Vulnerabilities in Check Point Products	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
JVN:JVND-2026-032927	Vulnerability in Cosminexus	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
JVN:JVND-2026-032929	Vulnerability in Cosminexus	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96754	orval @orval/hono before 8.29.0 Code Injection via Open...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96759	orval before 8.29.0 Code Injection via operationId	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-53649	Joro: Unauthenticated Cross-Origin Plugin Upload Leads...	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
GHSA-2XP9-VWFH-VXW4	Next.js: Unauthenticated Remote Code Execution in Imag...	Critical / 9.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-19681	Command Injection	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-19478	Improper Control of Generation of Code ('Code Injection'...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76174	Multiple vulnerabilities in Ocsreports for OCS Inventory NG	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85222	D-Link DNS-340L Add-On Center addon_center.cgi os c...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85223	D-Link DNS-340L CGI dropbox.cgi os command injection	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85224	D-Link DNS-320 ShareCenter File Sharing file_sharing.c...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-8876	Command Injection Vulnerability	Critical / 9.4	CISA KEV	✓ Blocked
CVE-2025-8875	Insecure Deserialization Vulnerability	Critical / 9.4	CISA KEV	✓ Blocked
CVE-2026-57909	WatchGuard Agent path traversal allows unauthenticated...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93985	OpenPanel js-runtime through 2.3.0 JavaScript Template...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81698	openssl_encrypt before 1.4.9 Shell Injection via info com...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 231 blocked · avg CVSS 8.7 · 22 CISA KEV (continued)				
CVE-2026-81701	openssl_encrypt before 1.4.9 Arbitrary Code Execution vi...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81719	openssl_encrypt before 1.4.9 Remote Code Execution via...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85425	MOOS-IvP through 24.8.1 iSay Command Injection via SA...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85426	MOOS-IvP through 24.8.1 uMemWatch Command Injecti...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-44402	Voltronic Power SNMP Web Pro 1.1 Unauthenticated RCE ...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-57910	WatchGuard Agent improper authentication allows unaut...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18667	Sensor Proxy Version 1.4.2 Fixes One Vulnerability	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-72710	SPIP < 4.4.18 RCE via editor_objet.php Job Queue Injection	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-95675	D-Link DAP-1360 6.14 Unauthenticated RCE via Web Ma...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-43641	Softaculous Virtualizor OS Command Injection via Billing ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66047	ProfilePress WordPress Plugin < 4.17.2 Unauthenticated ...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85427	MOOS essential-moos through 10.0.1 pAntler Remote Co...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-43642	Softaculous Virtualizor PHP Object Injection via Billing M...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66786	Submariner: submariner: ipsec.conf stanza injection via r...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-58400	GeoNetwork vulnerable to Remote Code Execution via un...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79766	Termix: OS command injection in ACME/Let's Encrypt cer...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-58072	CVE-2026-58072: A vulnerability in Veeam Service Provi...	Critical / 9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18937	Broken Link Checker < 2.4.12 - Unauthenticated RCE via ...	Critical / 9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-75604	Next.js: Unauthenticated Remote Code Execution on win...	Critical / 9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-67394	CVE-2026-67394: A critical local privilege escalation via ...	Critical / 9	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 231 blocked · avg CVSS 8.7 · 22 CISA KEV (continued)				
CVE-2026-67378	Microsoft SQL Server Remote Code Execution Vulnerability	Critical / 9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-65646	Plesk: Plesk: Remote Privilege Escalation and File Disclos...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2019-1068	CVE-2019-1068: A remote code execution vulnerability e...	High / 8.8	CISA KEV	✓ Blocked
CVE-2026-0551	PPWP – Password Protect Pages <= 1.9.18 - Authenticate...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-74012	WordPress TaxoPress plugin <= 3.51.0 - PHP Object Inje...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12894	Quarkus-qute: io.quarkus.qute.reflectionvalueresolver: q...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84202	modelscope: ModelScope: Arbitrary code execution via u...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73751	Authenticated Remote Command Injection in AOS-CX We...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73753	Authenticated Remote Command Injection Vulnerabilities...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84637	thunderbird: Thunderbird: Arbitrary code execution via m...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14357	DevKit Pro <= 2.3.0 - Missing Authorization to Authentica...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81772	WordPress Ninja Forms - Layout & Styles plugin <= 3.0.3...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84645	CVE-2026-84645: In Jenkins 2.579 and earlier, LTS 2.56...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2023-46748	Overview of F5 vulnerabilities (October 26, 2023) (CVE-...	High / 8.8	CISA KEV	✓ Blocked
CVE-2026-84752	WordPress RTMKit plugin <= 2.1.5 - PHP Object Injection ...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-16601	CM Map Locations <= 2.1.8 - Authenticated (Subscriber+...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78257	WordPress Booking and Rental Manager plugin <= 2.7.5 - ...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77018	Workeera Remote Tech Job Board < 1.0.6 - Subscriber+ A...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-3910	CVE-2026-3910: Inappropriate implementation in V8 in ...	High / 8.8	CISA KEV	✓ Blocked
CVE-2026-69268	Microsoft Office SharePoint Remote Code Execution Vul...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 231 blocked · avg CVSS 8.7 · 22 CISA KEV (continued)				
CVE-2026-69273	Microsoft Office SharePoint Remote Code Execution Vul...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69282	Microsoft Office SharePoint Remote Code Execution Vul...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69724	Microsoft Office SharePoint Remote Code Execution Vul...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69355	Microsoft Exchange Server Remote Code Execution Vuln...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77484	Microsoft SQL Server Remote Code Execution Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69465	Microsoft Office SharePoint Remote Code Execution Vul...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-65772	Microsoft Dynamics 365 On-Premises Remote Code Exe...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77908	Microsoft Dynamics 365 On-Premises Remote Code Exe...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69485	Remote Desktop Client Remote Code Execution Vulnerab...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69676	Windows Kerberos Remote Code Execution Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-71336	Windows Work Folder Service Remote Code Execution V...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69742	Microsoft Office Publisher Remote Code Execution Vulne...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78463	Remote Desktop Client Remote Code Execution Vulnerab...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69266	Windows DHCP Server Remote Code Execution Vulnerab...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-71352	Windows Remote Access Connection Manager Remote C...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69499	Windows Imaging Component Remote Code Execution V...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78519	Microsoft Office Outlook Remote Code Execution Vulner...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81385	Microsoft Office Publisher Remote Code Execution Vulne...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69598	Windows iSCSI Remote Code Execution Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82794	Multiple vulnerabilities in SolarView Compact (CVE-2026...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 231 blocked · avg CVSS 8.7 · 22 CISA KEV (continued)				
CVE-2026-82795	Multiple vulnerabilities in SolarView Compact (CVE-2026...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82796	Multiple vulnerabilities in SolarView Compact (CVE-2026...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82762	Multiple vulnerabilities in Contec FLEXLAN series (CVE-2...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82766	Multiple vulnerabilities in Contec FLEXLAN series (CVE-2...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82774	Multiple vulnerabilities in Contec CONPROSYS series (C...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82777	Multiple vulnerabilities in Contec CONPROSYS series (C...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82779	Multiple vulnerabilities in Contec CONPROSYS series (C...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77853	Multiple vulnerabilities in Lite-On O-RU "FF-RFI079I4" an...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-80217	Multiple vulnerabilities in Lite-On O-RU "FF-RFI079I4" an...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42271	LiteLLM: Authenticated command execution via MCP stdi...	High / 8.7	CISA KEV	✓ Blocked
CVE-2026-79756	Nuclio: Unauthenticated OS command injection via name...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-28797	RAGFlow: Server-Side Template Injection (SSTI) leading t...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85169	n8n before 1.123.73 Remote Code Execution via \$fromAI ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85610	OpenPanel before 2.3.0 Remote Code Execution via chart...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73693	FileRun < 2026.3.0 OS Command Injection via PhotoProo...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-90444	OS Command Injection in Malcolm	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89036	Appwrite < 2.0.0 Argument Injection via providerRootDire...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77929	ClipBucket < 5.5.3-#182 Remote Code Execution via Pho...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-64328	FreePBX Administration GUI is Vulnerable to Authenticat...	High / 8.6	CISA KEV	✓ Blocked
CVE-2026-84194	LibreNMS 23.10.0 before 26.4.0 OS Command Injection v...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 231 blocked · avg CVSS 8.7 · 22 CISA KEV (continued)				
CVE-2026-71963	Hermes Agent 0.18.2 - 0.21.0 RCE via git core.fsmonitor ...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84452	Windows ML CLI: CORS misconfig enables localhost RCE	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82524	UnoPim File Upload RCE via TinyMCE Image Upload Endp...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-68700	RAGFlow Remote Code Execution Vulnerability	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84832	Unsafe deserialization in the REST interface	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84830	OS command injection in privileged configuration handling	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-26212	Rara One Click Demo Import < 1.3.5 Arbitrary File Upload ...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73694	FileRun < 2026.3.0 OS Command Injection via escapeshe...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73699	FileRun < 2026.3.0 PHP Object Injection via Perms::getP...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-92980	HortusFox-Web < 6.1 Remote Code Execution via Import/...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85012	OS command injection in the Amazon CodeCatalyst blue...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2020-5741	CVE-2020-5741: Deserialization of Untrusted Data in Ple...	High / 8.5	CISA KEV	✓ Blocked
CVE-2026-19843	389-ds-base: 389-ds-base: Command injection via unes...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63376	toml-node: Prototype Pollution Leads to `Object.prototy...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-44728	Security Bulletin - September 15 2026 — RCE (Remote C...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-47864	org.springframework.integration/spring-integration-http...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2021-23758	Deserialization of Untrusted Data	High / 8.1	CISA KEV	✓ Blocked
CVE-2026-19942	Atarim <= 5.1.1 - Authenticated (Author+) Arbitrary File D...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73712	Unauthenticated Remote Code Execution in HPE Networ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14982	WP File Download <= 6.3.4 - Authenticated (Subscriber+...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 231 blocked · avg CVSS 8.7 · 22 CISA KEV (continued)				
CVE-2019-18935	CVE-2019-18935: Progress Telerik UI for ASP.NET AJAX ...	High / 8.1	CISA KEV	✓ Blocked
CVE-2026-47297	Microsoft SQL Server Remote Code Execution Vulnerability	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69438	Microsoft JScript Remote Code Execution Vulnerability	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78444	Microsoft Failover Cluster Remote Code Execution Vulne...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100389	GestSup before 3.2.62 Remote Code Execution via IMAP ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79755	Nuclio: Unauthenticated OS command injection via functi...	High / 8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-52831	Nuclio: Unsanitized cron trigger event headers/body inje...	High / 8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83948	Microsoft Azure CLI Remote Code Execution Vulnerability	High / 8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83549	CVE-2026-83549: Post-authentication Improper Neutral...	High / 7.8	CISA KEV	✓ Blocked
CVE-2026-84361	Composer arbitrary command execution via a malicious p...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85168	n8n before 1.123.73 Remote Code Execution via Git Node	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84374	Laravel Excel writes exports outside the configured filesy...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69804	Microsoft Office SharePoint Remote Code Execution Vul...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-100208	Microsoft Office Outlook Remote Code Execution Vulner...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78501	Microsoft 365 Copilot Business Chat Information Disclos...	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-61788	@bytebase/dbhub's read-only mode does not prevent da...	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2024-8190	CVE-2024-8190: An OS command injection vulnerability ...	High / 7.2	CISA KEV	✓ Blocked
CVE-2026-66620	WordPress OptionTree plugin <= 2.7.3 - PHP Object Injec...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15049	Depicter < 4.8.0 - Editor+ Arbitrary File Upload via ZIP Im...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73765	Authenticated Path Traversal Vulnerabilities Lead to Rem...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 231 blocked · avg CVSS 8.7 · 22 CISA KEV (continued)				
CVE-2026-73766	Authenticated Command Injection Vulnerabilities in the A...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73767	Authenticated Remote Command Injection Vulnerabilities...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81757	WordPress Rank Math SEO plugin <= 1.0.276 - Remote C...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78276	WordPress Fluent Boards Pro plugin <= 2.0.11 - PHP Obje...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76561	Pki-core: dogtag/pki: certprofile-import allows code exe...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81349	Azure HDInsight Ambari Elevation of Privilege Vulnerability	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69358	Remote Desktop Client Remote Code Execution Vulnerab...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85137	SeaCMS Locoy Collector seacms_locoy_news.php parsel...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-90843	SabyasachiRana WebMap New Nmap Scan functions_nm...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76547	Profile Builder < 4.0.1 - Admin+ PHP Object Injection via I...	Medium / 6.6	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-16759	Tutor LMS <= 4.0.5 - Unauthenticated Remote Code Exec...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55946	Microsoft Copilot Information Disclosure Vulnerability	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66323	Microsoft Edge (Chromium-based) Remote Code Executi...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82790	Multiple vulnerabilities in Contec PC-HELPER series (CV...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82791	Multiple vulnerabilities in Contec PC-HELPER series (CV...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82792	Multiple vulnerabilities in Contec PC-HELPER series (CV...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82793	Multiple vulnerabilities in Contec PC-HELPER series (CV...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-3424	kk Star Ratings <= 5.4.10.3 - Unauthenticated Arbitrary S...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-19032	com.fasterxml.jackson.core/jackson-databind: tools.jack...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75036	Fleet: DNS exfiltration via Sprig getHostByName in fleet....	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 231 blocked · avg CVSS 8.7 · 22 CISA KEV (continued)				
CVE-2026-81380	GitHub Copilot and Visual Studio Code Information Discl...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85040	ZhongBangKeJi CRMEB Custom Scheduled Task Feature...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84967	Arbitrary command execution via shell-expanded connec...	Medium / 5.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-35160	CVE-2026-35160: Dell SmartFabric OS10 Software, versi...	Medium / 5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63694	CVE-2026-63694: Dell SmartFabric OS10 Software, vers...	Medium / 5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82853	nodemailer: Nodemailer: SMTP Command Injection allow...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84646	jenkins: Jenkins: Unauthorized creation of user objects vi...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78593	Improper Control of Generation of Code in Kibana Leadin...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63630	BentoPDF: Workflow Import Allows Unvalidated TSA URL...	Low / 3.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96376	Cloud - Critical - Remote code execution - SA-CONTRIB-...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96375	Cloud - Critical - Remote code execution - SA-CONTRIB-...	Unscored	NO KNOWN EXPLOIT	✓ Blocked

SQL Injection: 105 blocked · avg CVSS 8.1 · 1 CISA KEV

CVE-2026-19949	5 Million WordPress Sites Affected by SQL Injection Vuln...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9082	Drupal core - Highly critical - SQL injection - SA-CORE-2...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2026-77635	CakePHP: FunctionsBuilder::jsonValue() vulnerable to SQL...	Critical / 9.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-6881	Authenticated SQL Injection Enables Unauthorized Acces...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-58048	CVE-2026-58048: Improper preservation of SQL mode ...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73391	WordPress Total Donations plugin <= 2.0.5 - SQL Injectio...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-68566	WordPress BookingPress Appointment Booking Pro plugi...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 105 blocked · avg CVSS 8.1 · 1 CISA KEV (continued)				
CVE-2026-66649	WordPress Directory Pro plugin <= 2.5.8 - SQL Injection ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66680	WordPress Locatoraid Store Locator plugin <= 3.9.72 - S...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73183	WordPress Maps Marker Pro plugin <= 4.32 - SQL Injecti...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73185	WordPress NGG Smart Image Search plugin < 4.0.0 - SQ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73388	WordPress Nikstore Core plugin <= 1.5 - SQL Injection vu...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66592	WordPress rtMedia for WordPress, BuddyPress and bbPr...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66593	WordPress Security & Malware scan by CleanTalk plugin ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66609	WordPress TheGem (Elementor) theme <= 5.12.3 - SQL I...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73355	WordPress Affiliates Manager plugin <= 2.9.53 - SQL Inje...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-15688	WordPress Capella theme <= 2.5.5 - SQL Injection vulner...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73365	WordPress JetAppointment plugin <= 2.5.2 - SQL Injecti...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73339	WordPress Modern Events Calendar plugin < 7.35.0 - SQ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-74015	WordPress Readabler plugin < 2.0.18 - SQL Injection vuln...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73187	WordPress Sticky Chat Widget plugin <= 1.4.2 - SQL Inje...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81286	WordPress WCFM Marketplace plugin <= 3.8.1 - SQL Inje...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78080	Joomla Extension - feenders.de - Unauthenticated SQL i...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84768	WordPress VikAppointments Services Booking Calendar ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84813	WordPress GeoDirectory plugin <= 2.8.174 - SQL Injectio...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82526	R2R 3.6.6 SQL Injection via Vector Index Creation Endpoint	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78288	WordPress Beautiful Taxonomy Filters plugin <= 2.4.6 - S...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 105 blocked · avg CVSS 8.1 · 1 CISA KEV (continued)				
CVE-2026-78260	WordPress Epayco plugin <= 8.4.6 - SQL Injection vulner...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81756	WordPress Smart Marketing SMS and Newsletters Forms...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81763	WordPress Throws SPAM Away plugin <= 3.8.2 - SQL Inje...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32479	WordPress Visitor Traffic Real Time Statistics Pro plugin ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81293	WordPress WP Data Access plugin <= 5.5.81 - SQL Injecti...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62262	Piwigo: Unauthenticated SQL injection in `pwg.images.fil...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14828	CVE-2026-14828: Zohocorp ManageEngine Password M...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82538	ILIAS Arbitrary SQL Injection via Repository Trash Table S...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66819	Microsoft SQL Server Elevation of Privilege Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-67370	Microsoft SQL Server Elevation of Privilege Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69716	Microsoft Office SharePoint Elevation of Privilege Vulner...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62895	Azure Arc SQL Server Extension Elevation of Privilege Vul...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66820	SQL Server Elevation of Privilege Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85155	WWBN AVideo SQL Injection via get.json.php APIName c...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82527	R2R 3.6.6 SQL Injection via Retrieval Search Filter Key	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85540	Interinfo DreamMaker - SQL Injection	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-72708	SPIP < 4.4.18 Unauthenticated Blind SQL Injection via sit...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12983	Dinatur <= 1.18 - Unauthenticated SQL Injection via Colu...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-16950	Product Shortlist <= 1.0.4 - Unauthenticated SQL Injectio...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76175	Multiple vulnerabilities in Ocsreports for OCS Inventory NG	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 105 blocked · avg CVSS 8.1 · 1 CISA KEV (continued)				
CVE-2026-76176	Multiple vulnerabilities in Ocsreports for OCS Inventory NG	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85388	Worklenz through 3.0.0 SQL Injection via the sort-field Q...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73698	FileRun < 2026.3.0 Authenticated SQL Injection via Grou...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66668	WordPress Community by PeepSo plugin <= 9.0.5.2 - SQ...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-74013	WordPress eShipper Commerce plugin <= 2.16.13 - SQL I...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66594	WordPress WordPress Persistent Login plugin <= 3.1.0 - ...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73998	WordPress WP w3all phpBB plugin <= 3.0.5 - SQL Injecti...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32552	WordPress YITH WooCommerce Membership Premium pl...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32466	WordPress Gravity Forms Bookings premium plugin <= 2....	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32564	WordPress ACPT (Pro) - Custom Post Types Plugin for W...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32550	WordPress Kadence Shop Kit plugin <= 3.0.6 - SQL Inject...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78285	WordPress Like Button Rating plugin <= 2.6.61 - SQL Inje...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81277	WordPress Suggestion Engine for WooCommerce plugin ...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82227	WordPress WPBulky plugin <= 1.2.2 - SQL Injection vulne...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88890	OpenPanel through 2.3.0 SQL Injection via unvalidated pr...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-17543	SQL injection in ext-pgsql via E'...' backslash breakout	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-74011	WordPress InfiniteWP Client plugin <= 1.13.9 - SQL Inject...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78270	WordPress FluentCRM Pro plugin <= 3.1.12 - SQL Injectio...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57777	WordPress WooCommerce plugin < 11.0 - SQL Injection v...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2023-34133	CVE-2023-34133: Improper Neutralization of Special Ele...	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 105 blocked · avg CVSS 8.1 · 1 CISA KEY (continued)				
CVE-2026-66622	WordPress Depicter Slider plugin <= 4.8.0 - SQL Injectio...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18884	WooCommerce Lottery <= 2.2.9 - Unauthenticated Time...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-5097	wpForo Forum <= 2.4.17 - Unauthenticated SQL Injection...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40018	dovecot: Dovecot: MySQL multi-byte escaping wrong	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96602	Abdurrab5 online-makeup-store Customer Login custom...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97882	mathurvishal CloudClassroom-PHP-Project Faculty Auth...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18653	WP Directory Kit < 1.5.7 - Admin+ SQL Injection via sectio...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-33639	InvoicePlane permits DDL injection through tax_rate_dec...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73345	WordPress License Manager for WooCommerce plugin <...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75132	WAPT Server SQL Injection via /api/v3/hosts Endpoint	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77927	ClipBucket < 5.5.3-#182 Blind SQL Injection via Photo De...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77928	ClipBucket < 5.5.3-#182 Blind SQL Injection via Private M...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85138	SeaCMS WeChat index.php addslashes sql injection	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85187	itsourcecode Online Medicine Delivery System Order Sta...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85225	code-projects Doctor Appointment System patient_login...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85397	code-projects Hospital Information System addReq.php f...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85398	code-projects Hospital Information System viewReq.php ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85399	code-projects Hospital Information System PrespControl...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85402	code-projects Doctor Appointment System booking.php ...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85403	code-projects Doctor Appointment System contactus.ph...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 105 blocked · avg CVSS 8.1 · 1 CISA KEV (continued)				
CVE-2026-93462	CVE-2026-93462: A missing authentication for critical f...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-16959	Media Library Assistant < 3.40 - Author+ SQL Injection vi...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14601	Link Whisper < 0.9.7 - Editor+ SQL Injection via domain P...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78470	WP Project Manager Pro <= 4.0.1 - Authenticated (Subsc...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15023	Events Manager <= 7.4.0 - Authenticated (Contributor+) ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69636	Microsoft Office SharePoint Information Disclosure Vulne...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96777	Forma LMS Multi-User-Selector AJAX Endpoint getData ...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62956	Multiple vulnerabilities in baserCMS (CVE-2026-62956)	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97886	mathurvishal CloudClassroom-PHP-Project managevide...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77790	RegistrationMagic < 6.0.9.4 - Admin+ SQLi via 'rm_sortb...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-19094	Tutor LMS < 4.0.6 - Unauthenticated SQLi via 'offset' and...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85205	itsourcecode Online Medicine Delivery System Wishlist c...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85383	itsourcecode Sales and Inventory System inv_del.php sql...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93983	OpenPanel through 2.3.0 SQL Injection via ClickHouse Pr...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77824	Media Sweep <= 1.1.3 - Authenticated (Administrator+) S...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-80488	WP Ultimate CSV Importer < 9.0 - Admin+ SQLi via AIOSE...	Medium / 4.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82186	WPLP Cookie Consent < 4.4.2 - Admin+ SQLi via 'offset' ...	Medium / 4.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87936	amazee.ai Private AI Provider - Critical - SQL injection - S...	Unscored	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 77 blocked · avg CVSS 7.4 · 2 CISA KEV				
CVE-2026-18051	W3 Total Cache < 2.10.5 - Unauthenticated Arbitrary Dire...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84669	CVE-2026-84669: A path traversal vulnerability in Jenki...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85706	Improper Limitation of a Pathname to a Restricted Direct...	Critical / 10	CISA KEV	✓ Blocked
CVE-2026-70200	Azure Logic Apps Elevation of Privilege Vulnerability	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66587	WordPress WP Cafe Pro plugin < 3.0.15 - Local File Inlus...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-11613	Divi Ajax Filter <= 5.1.2 - Unauthenticated Local File Inclu...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-78069	Joomla Extension - j2commerce.com - Missing authoriza...	Critical / 9.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2024-8963	CVE-2024-8963: Path Traversal in the Ivanti CSA before ...	Critical / 9.4	CISA KEV	✓ Blocked
CVE-2026-70009	Azure Arc Elevation of Privilege Vulnerability	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85199	CVE-2026-85199: Eclipse aeriOS Self-orchestrator versi...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81690	verify-usb before 1.4.9 Symlink Directory Traversal Code ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81716	openssl_encrypt before 1.4.9 Plugin Sandbox Path Traver...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81726	nlTK: NLTK: Unauthorized file access via path traversal in ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85396	rubyzip before 3.4.0 Path Traversal in Zip::Entry#extract ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-67281	Unauthenticated file read in Mikrotik RouterOS	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-16616	Simple File List <= 6.3.11 - Unauthenticated Arbitrary File ...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-74239	XenForo < 2.3.13 Path Traversal via Style Archive Importe...	High / 8.6	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-67397	CVE-2026-67397: Path traversal in Plesk 18.0.79.9 and e...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-14727	NGINX Ingress Controller vulnerability CVE-2025-14727	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-28150	WordPress Golo Framework plugin < 1.7.5 - Local File Incl...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 77 blocked · avg CVSS 7.4 · 2 CISA KEV (continued)				
CVE-2026-78478	Måne <= 1.7 - Unauthenticated Local File Inclusion	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73387	WordPress Resido theme <= 1.5 - Local File Inclusion vul...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-28151	WordPress Tonda theme < 2.6 - Local File Inclusion vulne...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-28152	WordPress Tonda Core plugin < 2.6 - Local File Inclusion ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66671	WordPress Verdure Core plugin <= 1.2 - Local File Inclusi...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73400	WordPress Restaurant Menu by MotoPress plugin <= 2.4...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-15637	WordPress Shuffle theme <= 1.8 - Local File Inclusion vul...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78254	org.apache.ant/ant: Apache Ant: Arbitrary file write via pa...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82765	Multiple vulnerabilities in Contec FLEXLAN series (CVE-2...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82768	Multiple vulnerabilities in Contec FLEXLAN series (CVE-2...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-90959	Pulpcore: pulpcore: file:// scheme allowlist bypass in cont...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69807	PowerShell Elevation of Privilege Vulnerability	High / 8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75963	Events Made Easy <= 3.2.5 - Authenticated (Contributor+...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82393	pnpm: pnpm: Arbitrary file write and code execution via p...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85124	@fastify/http-proxy vulnerable to prefix escape via backs...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15990	Formidable Charts <= 2.0.1 - Unauthenticated Arbitrary Fi...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-6377	CSM: Next4Biz CSM: Information disclosure via path trav...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75887	Openshift/console: openshift/console: unauthenticated p...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78461	Visual Studio Code Security Feature Bypass Vulnerability	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85160	AVideo through c91b5975d CSRF and Path Traversal via ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 77 blocked · avg CVSS 7.4 · 2 CISA KEV (continued)				
CVE-2026-100372	ClipBucket v5 before 5.5.3-#197 Path Traversal via templ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40526	Volmarg Personal Management System Path Traversal via...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9587	Authenticated Local File Inclusion (LFI) in Switchvox SMB...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
GHSA-2Q42-4Q24-7 RGV	OpenAPI3 version value escapes `emitterOutputDir` and...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-90445	Path Traversal in Malcolm	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82392	pnpm: pnpm: Arbitrary Code Execution via Path Traversal	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73102	RustDesk Path Traversal via macOS Clipboard File-Paste	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84478	WWBN AVideo Unauthenticated Arbitrary Log File Deletion	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84441	Piwigo Image Derivative i.php path traversal	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-89021	MikroTik RouterOS Path Traversal via Container OCI/tar I...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78275	WordPress Fluent Boards Pro plugin <= 2.0.11 - Arbitrary ...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12513	Shared Files < 1.7.68 - Unauthenticated Arbitrary File Del...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66586	WordPress WP Cafe Pro plugin < 3.0.15 - Local File Inlus...	Medium / 6.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14280	Events Manager <= 7.3.7.4 - Authenticated (Administrator...	Medium / 6.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18027	WebToffee WooCommerce PDF Invoices, Packing Slips, ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82877	ILIAS Arbitrary File Read via SOAP addFile	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84365	Hono: Incomplete fix for CVE-2026-39408: `toSSG()` st...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75602	OpenList: Authenticated arbitrary file write via Content-D...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62801	Microsoft PowerShell Security Feature Bypass Vulnerability	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81377	Visual Studio Code Tampering Vulnerability	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 77 blocked · avg CVSS 7.4 · 2 CISA KEV (continued)				
CVE-2026-87727	a-blog cms vulnerable to path traversal (CVE-2026-87727)	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82521	parsedmarc 9.0.6 < 11.0.1 Path Traversal via Forensic Rep...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-96678	weiqingwen spring-boot-forum Avatar Upload NewUserF...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-97365	chonkie-inc litt.rs lib.rs mount path traversal	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84373	Vitest: Path Traversal / Arbitrary File Read via @vitest/mo...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81347	Frontend Admin by DynamiApps < 3.29.13 - Unauthentic...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87910	tarfile hardlink fallback ignores custom extraction filter re...	Medium / 5.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-83557	com.fasterxml.jackson.core/jackson-databind: tools.jack...	Medium / 5.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82193	WPvivid Backup & Migration < 0.9.134 - Admin+ File Writ...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82194	WPvivid Backup & Migration < 0.9.134 - Admin+ Arbitrary...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73551	envoy: envoy: path normalization bypass via dot/dot-dot ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79706	Breeze Cache < 2.5.13 - Unauthenticated File Creation vi...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85409	Eleveo Quality Management Questionnaire Service Quest...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63006	Zammad: HTML sanitizer API path allowlist bypass via int...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2024-7634	NGINX Agent vulnerability CVE-2024-7634	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-79705	Podman: buildah: buildah/copier: directory escape via cra...	Medium / 4.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49830	DSpace: ORE resource URI does not validate scheme for ...	Medium / 4.4	NO KNOWN EXPLOIT	✓ Blocked

SSRF: 63 blocked · avg CVSS 7.2 · 1 CISA KEV

CVE-2026-54745	kubeflow/pipelines: pipelines: Kubeflow Pipelines: Unaut...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
----------------	---	---------------	------------------	-----------

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 63 blocked · avg CVSS 7.2 · 1 CISA KEV (continued)				
CVE-2026-83548	CVE-2026-83548: A Pre-authentication SSRF vulnerabili...	Critical / 10	CISA KEV	✓ Blocked
CVE-2026-75754	CVE-2026-75754: Missing Authentication for Critical Fu...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42038	Security Bulletin - June 16 2026 — Bitbucket Data Center...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78003	Mailgun for WordPress <= 2.2.0 - Unauthenticated Serve...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77012	Icollect <= 1.0.0 - Unauthenticated Arbitrary File Read, S...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85695	FastChat Unauthenticated Worker Registration SSRF and...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75885	Openshift/console: openshift/console: unauthenticated s...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85614	OpenPanel API before 2.3.0 Unauthenticated SSRF via sit...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-80181	Apache Allura: Server-side request forgery	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85180	Ollama 0.30.0 through 0.33.2 SSRF via Cross-Host Tenso...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85612	OpenPanel before 2.3.0 SSRF via favicon and og endpoints	High / 8.7	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-81889	eFinder: SSRF protection bypass via DNS rebinding in th...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-65818	Power Automate Elevation of Privilege Vulnerability	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76086	Formie: Integration form-settings action allows SSRF and...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85179	Label Studio through 1.23.0 SSRF via Unvalidated Webho...	High / 8.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77348	Wallos incomplete fix for CVE-2026-33407: unauthentic...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81357	Visual Studio Code Security Feature Bypass Vulnerability	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14540	Server-Side Request Forgery via Unrestricted HTTP Redi...	High / 8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-16600	SmartAIPress <= 1.2.0 - Subscriber+ Server-Side Reques...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-71196	openstack-glance: openstack-glance: SSRF via web-dow...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 63 blocked · avg CVSS 7.2 · 1 CISA KEV (continued)				
CVE-2026-71198	openstack-glance: openstack-glance: SSRF via location ...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73315	XenForo < 2.3.13 SSRF via PayPal REST Webhook Handler	High / 7.7	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-75899	fast-uri vulnerable to server-side request forgery via rep...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-75975	fast-uri vulnerable to server-side request forgery via malf...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76172	fast-uri vulnerable to host confusion via percent-encode...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66304	Skype for Business Information Disclosure Vulnerability	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85917	Azure AI Foundry Elevation of Privilege Vulnerability	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32473	WordPress PDF Smart Viewer for Elementor plugin <= 1.0...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84761	WordPress LiteSpeed Cache plugin <= 7.9 - Server Side ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-17565	Animation Addons for Elementor < 2.7.2 - Unauthenticate...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82659	nodemailer: Nodemailer: Arbitrary file read and Server-Si...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76177	Multiple vulnerabilities in Ocsreports for OCS Inventory NG	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85163	AVideo Server-Side Request Forgery via epg_link param...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85164	WWBN AVideo Server-Side Request Forgery via set_api_...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85170	n8n before 1.123.73 Local File Read and SSRF via Gmail a...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85242	Server-Side Request Forgery via Favicon Redirect to Loc...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85380	light0011 cms UEditor controller.php catchimage server-...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85609	Openpanel before 2.3.0 SSRF via Site Checker Endpoint	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81092	github.com/mark3labs/mcp-go: mcp-go: DNS Rebinding ...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55421	Open edX Platform: SSRF in Studio Video Download End...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 63 blocked · avg CVSS 7.2 · 1 CISA KEV (continued)				
CVE-2026-84377	LiteLLM: Authenticated SSRF and provider-credential exf...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69361	Microsoft Exchange Server Spoofing Vulnerability	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69683	Microsoft Office SharePoint Information Disclosure Vulne...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-78269	WordPress Shared Files plugin <= 1.7.69 - Server Side Re...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82556	net: golang: codeberg.org/forgejo/forgejo: Forgejo: Serv...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32467	WordPress [Aotuman] Grab WeChat Articles plugin <= 2...	Medium / 6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55473	HomeBox: Notifier SSRF guard misses NAT64 prefixes (6...	Medium / 6	NO KNOWN EXPLOIT	✓ Blocked
GHSA-8M3C-C648-2 XJJ	Nodemailer: resolveContent() on a MailMessage bypasse...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84772	WordPress Broken Link Checker plugin <= 2.4.14 - Serve...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85305	WordPress SEOPress plugin <= 10.1 - Server Side Reque...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85172	n8n before 2.34.1 SSRF via Request Helper URI Validatio...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85106	NousResearch hermes-agent Link Title Fetch index.tsx f...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-5096	Everest Forms <= 3.4.4 - Unauthenticated Server-Side R...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85528	Snowflake JDBC Driver auto-configuration account valid...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-88892	OpenPanel through 2.3.0 SSRF via Unguarded Importer F...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-90446	Server-Side Request Forgery in Malcolm	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56734	Zammad: Avatar Image URL Server-Side Request Forwar...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-71197	openstack-glance: openstack-glance: SSRF blocklist byp...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-74768	CVE-2026-74768: Dell PowerProtect Data Manager, vers...	Medium / 4.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69904	Microsoft Office SharePoint Information Disclosure Vulne...	Low / 3.5	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 63 blocked · avg CVSS 7.2 · 1 CISA KEV (continued)				
CVE-2026-13176	Eventin < 4.1.21 - Contributor+ Server-Side Request Forg...	Low / 2.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-87953	SAML SSO - Service Provider - Moderately critical - Serv...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
Injection: 25 blocked · avg CVSS 6.0 · 0 CISA KEV				
CVE-2026-55159	luci-app-adblock-fast: Delegated `luci-app-adblock-fast...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73812	OTP: inets: inets: HTTP Request Smuggling allows bypas...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81356	Visual Studio Code Security Feature Bypass Vulnerability	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81525	mongodb: Reject "." and NUL bytes in database and colle...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73548	envoy: envoy: connection poisoning through generic non...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-77634	CakePHP: SmtptTransport vulnerable to CRLF header inje...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2020-7746	Multiple vulnerabilities in Contec CONPROSYS series (C...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62906	Microsoft Discovery Studio Information Disclosure Vulne...	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85063	node-csv: Prototype replacement still reachable via colu...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-93579	io.netty/netty-codec-http2: netty: http/2 header field val...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85167	n8n before 2.36.2 Query Injection via Elasticsearch Firest...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-33604	dovecot: Dovecot: SMTP smuggling vulnerability allows s...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84363	Hono: Query parser reads parameters after the URL frag...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84962	Authenticated KMS request forgery via CRLF injection in ...	Medium / 5.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84380	httpx2: HTTPX2: Request Smuggling and Connection De...	Medium / 5.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-37236	github.com/grpc-ecosystem/grpc-gateway: grpc-gatew...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Injection: 25 blocked · avg CVSS 6.0 · 0 CISA KEV (continued)				
CVE-2026-82661	nodemailer: Nodemailer: Header injection via unsanitized...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84379	httpx2: HTTPX2: Multipart header injection via unvalidate...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-10841	Multiple security vulnerabilities may affect IBM WebSphe...	Medium / 4.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49469	GLPI: LDAP filter injection in user import feature	Medium / 4.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-94216	ST Engineering iDirect Evolution/Velocity WebServer Evo...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84367	joi: object().rename() with a template target can set the v...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84368	joi: Prototype pollution via a `__proto__` language key in ...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85008	undici: undici: Integrity failure due to caching of unsafe H...	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18540	undici: undici: HTTP response splitting via retry interceptor	Low / 3.7	NO KNOWN EXPLOIT	✓ Blocked

Insecure Design (File-Upload): 17 blocked · avg CVSS 8.7 · 0 CISA KEV

CVE-2026-81780	WordPress Hash Form plugin <= 1.4.2 - Arbitrary File Uplo...	Critical / 10	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-74014	WordPress IT Residence theme <= 3.2.1 - Arbitrary File U...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-74016	WordPress Smart Cleaning theme <= 4.8.6 - Arbitrary Fil...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-74018	WordPress Warehouse Cargo theme <= 2.6.9 - Arbitrary ...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66627	WordPress GP Premium plugin <= 2.5.5 - Arbitrary File U...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32463	WordPress Sync Post With Other Site plugin <= 1.9.3 - Ar...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32474	WordPress Templatiq plugin <= 0.2.5 - Arbitrary File Uplo...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73996	WordPress Masteriyo - LMS plugin <= 2.3.2 - Arbitrary Fil...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66600	WordPress Media Library Assistant plugin <= 3.39 - Arbit...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Insecure Design (File-Upload): 17 blocked · avg CVSS 8.7 · 0 CISA KEV (continued)				
CVE-2026-78274	WordPress Fluent Boards Pro plugin <= 2.0.11 - Arbitrary ...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82780	Multiple vulnerabilities in Contec CONPROSYS series (C...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63219	Unauthenticated file upload via missing authorization on ...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84063	CVE-2026-84063: BurgerEditor 3.2.0 through 3.4.0 cont...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85208	itsourcecode Online Medicine Delivery System Order Ma...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84062	CVE-2026-84062: BurgerEditor 3.0.0 through 3.4.0 cont...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85135	ILIAS MediaPool ZipAdapter.php uploadMultipleSubtitleF...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85186	itsourcecode Online Medicine Delivery System Customer...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
Uncontrolled Resource Consumption: 13 blocked · avg CVSS 7.0 · 0 CISA KEV				
CVE-2026-89025	Hirschmann HiOS Switch Platform DoS via Malformed HT...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-76763	io.smallrye/smallrye-graphql: SmallRye GraphQL: Unauth...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69664	otp: inets: Erlang/OTP inets httpd: Denial of Service via m...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84776	WordPress MalCare Security plugin <= 6.69 - Denial of S...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84778	WordPress Migrate Guru – Site Migration & Cloning plugi...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81285	WordPress Smush Image Compression and Optimization ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69378	Microsoft Exchange Server Denial of Service Vulnerability	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82333	multer vulnerable to Denial of Service via oversized array ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-86065	Klever-Go: Unauthenticated WebSocket /subscribe: no re...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84856	rowboatlabs rowboat Composio Webhook Endpoint route...	Medium / 6.9	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Uncontrolled Resource Consumption: 13 blocked · avg CVSS 7.0 · 0 CISA KEV (continued)				
CVE-2026-84775	WordPress Really Simple SSL plugin <= 9.8.0 - Denial of ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-84780	WordPress WP Go Maps plugin <= 10.1.08 - Denial of Ser...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-85407	Eleveo Quality Management Conversation events denial o...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
XML Injection: 6 blocked · avg CVSS 7.8 · 1 CISA KEV				
CVE-2024-34102	XXE can expose crypt key and other secrets granting full ...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2026-61741	http4s-scala-xml has an XML External Entity (XXE) proce...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-17615	Resteasy-core: resteasy sourceprovider remote unauth...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
JVN: JVNDB-2026-032928	Vulnerability in Cosminexus Component Container	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-82525	Exterro FTK Imager < 8.3 XXE via Report.xml XSLT Proce...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-81723	nltk: NLTK: Denial of Service via malformed XML corpus f...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked

• ABOUT INDUSFACE

Autonomous Application Security for the **AI Era**

Indusface secures the web, API, and AI applications of thousands of organizations across 95 countries. Backed by leading institutional investors, Indusface is recognized by Gartner, Forrester, and IDC for its innovation in application security and meets globally accepted security and compliance standards, including ISO 27001, SOC 2, PCI DSS, and GDPR. Its globally distributed cloud infrastructure spans Asia, the Middle East, Europe, and North America, enabling low-latency protection and regional data residency for enterprises worldwide.

AppTrana is Indusface's autonomous enterprise application security platform that continuously discovers vulnerabilities, autonomously remediates exploitable risks through virtual patching, and protects applications against DDoS, bot, API, AI, and zero-day attacks. Combining AI-powered intelligence, expert governance, and SLA-backed protection, AppTrana helps organizations reduce the time from vulnerability discovery to protection while delivering compliance-ready reports with zero false positives.

Bangalore | Delhi | Mumbai | Vadodara | Dallas

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