INDUSFACE™

ZERO-DAY VULNERABILITY REPORT

• MONTHLY BULLETIN · JUNE 2026

Zero-Day Vulnerability Coverage Report

In June 2026, 400 zero-days emerged across the traffic AppTrana protects. Every one was caught and blocked automatically, no manual intervention, no exposure window.

400	100%	26	20
ZERO-DAYS BLOCKED	CATEGORY COVERAGE	CISA KEV CLOSED	AGENTIC AI / LLM CLOSED

CONTENTS

In this Report

Coverage data for every zero-day vulnerabilities AppTrana blocked in June 2026, plus the exploitation, severity, and threat-intelligence context behind the numbers.

RESEARCH BASIS

Coverage reflects real enforcement across AppTrana-protected traffic in June 2026. Every vulnerability listed traces back to a specific CVE, blocking rule, and scanner check.

Zero-Day Exposure Window: 0 Days

In June 2026, AppTrana's default rule set automatically blocked 400 zero-day vulnerabilities, achieving 100% coverage with zero manual intervention. The gap between disclosure and protection, usually where exposure lives, never opened.

400

BLOCKED BY DEFAULT

Command Injection, SQL Injection, Path Traversal, and Cross-Site Scripting all covered at 100% out of the box, zero manual tuning required.

26

CISA KEV ENTRIES

Including CVE-2026-12569 and CVE-2026-20230, both cited under Binding Operational Directive 26-04, blocked before any patch obligation existed.

Pre-patch

EXTORTION CAMPAIGN CLOSED

The Oracle PeopleSoft zero-day exploited by UNC6240 (ShinyHunters) was blocked by default before the vendor's own advisory shipped, eliminating that exposure window entirely.

20

AGENTIC AI & LLM ZERO-DAYS

Blocked automatically across prompt injection, RAG data exposure, and agent-to-tool trust boundaries. AI threats didn't get a free pass.

Coverage by Category

Command Injection accounted for 180 of 400 vulnerabilities and the most Critical findings of any category, the largest share of risk this report tracks. All identified vulnerabilities were covered at 100%, with no exceptions.

CATEGORY	BLOCKED	CRITICAL	HIGH	AVG CVSS	PEAK
Command Injection	180	79	82	8.8	10.0
SQL Injection	93	15	71	8.2	9.8
Path Traversal	40	5	17	7.4	10.0
Cross-Site Scripting	33	3	18	6.7	9.6
SSRF	24	3	12	7.3	9.9
Injection	11	4	5	8.2	9.1
Insecure Design (File-Upload)	11	6	1	9.5	10.0
Uncontrolled Resource Consumption	7	0	3	6.8	7.5
XML Injection	1	1	0	9.4	9.4

Severity Snapshot

81% of the 400 vulnerabilities blocked, 325 in total, were Critical or High severity, normally the fastest-tracked tier for patching. Here, there was no fast-track needed: all were already blocked by default.

BREAKDOWN BY SEVERITY

Critical	116	29.0%
High	209	52.3%
Medium	48	12.0%
Low	2	0.5%
Unscored	25	6.3%

325

CRITICAL + HIGH SEVERITY

These sit in the tier most organizations rush to patch first, where an open exposure window carries the highest risk. Every one was already blocked at the edge, with no emergency patch cycle, out-of-band change, or manual rule work required.

Exploitation & KEV Status

Of the 400 blocked, 26 were already confirmed by CISA as actively exploited and listed in the Known Exploited Vulnerabilities catalog. Another 161 had a public exploit or proof-of-concept in circulation. The usual gap between exploit and patch simply didn't apply, coverage was already there.

26
CISA KEV · ACTIVELY EXPLOITED
6.5%

161
PUBLIC EXPLOIT / POC AVAILABLE
40.3%

213
NO KNOWN EXPLOIT
53.2%

NOTABLE CISA KEV ENTRIES BLOCKED

CVE	SEVERITY / CVSS	CATEGORY
CVE-2026-35273	Critical / 9.8	SSRF
CVE-2026-10520	Critical / 10.0	Command Injection
CVE-2026-10523	Critical / 9.9	Command Injection
CVE-2026-8037	Critical / 9.8	Command Injection

05 • EMERGING RISK

Agentic AI & LLM Risk Coverage

Agentic AI and LLM components introduce a distinct set of exposures: prompt injection, insecure agent-to-tool trust boundaries, and exposed RAG data sources. In June 2026, 20 vulnerabilities across this attack surface were blocked automatically.

6	8	6	7.8	9.8
CRITICAL	HIGH	MEDIUM	AVG CVSS	PEAK CVSS

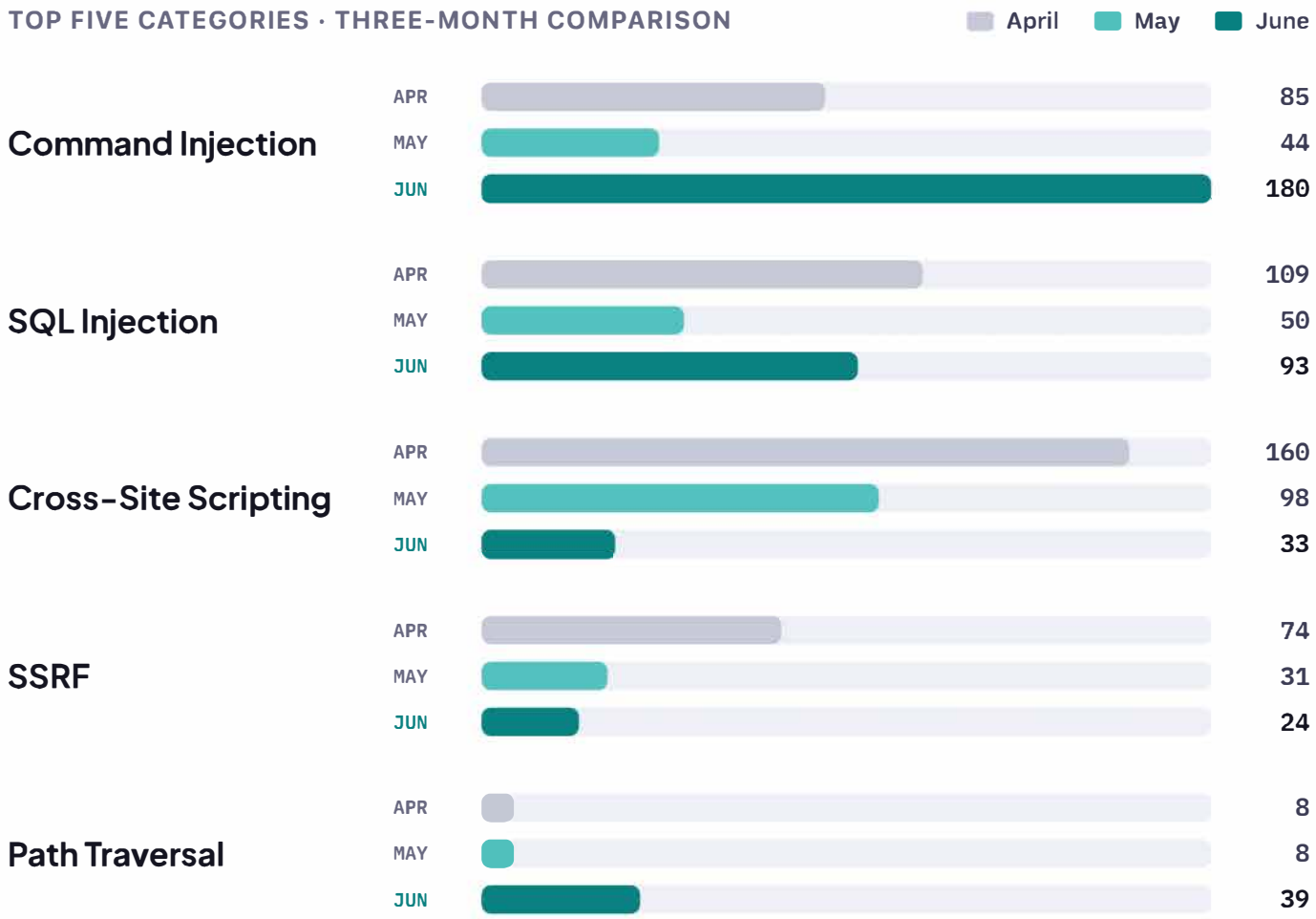
RISK AREA	BLOCKED	WHAT IT COVERS
LLM Application Layer	12	LLM application code and integrations
RAG Data Exposure	4	RAG pipelines and connected data sources
Prompt Injection	3	Direct or indirect prompt-injection vectors
Agent-to-Tool Trust	3	Autonomous-agent frameworks and trust boundaries

NOTABLE AI / LLM ZERO-DAYS BLOCKED

CVE	SEVERITY / CVSS	CATEGORY
CVE-2026-55743	Critical / 9.6	Command Injection
CVE-2024-58351	Critical / 9.8	Command Injection
CVE-2026-55413	Critical / 9.4	Command Injection
CVE-2026-53753	Critical / 9.8	Command Injection
CVE-2026-44020	Critical / 9.4	XML Injection

Vulnerability Trend

Volume this period was heavily back-loaded. Weeks 3 through 5 (9 to 25 June) account for 383 of the 400 vulnerabilities blocked, with week 4 alone outpacing the rest of the month combined. That surge lines up with a run of high-profile disclosures, Ivanti Sentry, Oracle PeopleSoft, and a five-product CISA KEV cluster, all blocked without a single custom rule.



Command Injection rose from 44 in May to 180 in June, and Path Traversal from 8 to 39, the sharpest month-over-month increases here. AppTrana held 100% coverage across both throughout, with no custom rule work or emergency patch cycles. A similar spike next month would need no additional engineering time or change-approval capacity: the existing rule set has already absorbed a 4× jump in volume without a coverage gap.

High-Profile Attacks Blocked

THREAT	SEVERITY / CVSS	EXPLOITATION
Oracle PeopleSoft CVE-2026-35273	Critical / 9.8	CISA KEV
Ivanti Sentry CVE-2026-10520 / CVE-2026-10523	Critical / 10.0 & 9.9	CISA KEV
Cisco Catalyst SD-WAN CVE-2026-20245 / -20182 / -20127	Critical	TARGETED INTRUSION
Command-Injection KEV Cluster 5 products	Critical / 9.1 to 10.0	CISA KEV
Cisco UCM & SD-WAN Manager CVE-2026-20230 / CVE-2026-20262	Unscored / 6.5	CISA KEV

Oracle PeopleSoft: blocked from day zero

Exploited in the wild as a zero-day between 27 May and 9 June, two weeks before Oracle's own advisory and patch. Mandiant attributes the campaign to UNC6240 (ShinyHunters), a financially motivated extortion collective that hit over 100 organizations, 68% of them higher education, stealing data later posted to the group's leak site. AppTrana's SSRF policy blocked the exploitation path from day zero.

Ivanti Sentry: closed same-day, ahead of any patch

A pre-auth path to root-level remote code execution, with a public proof-of-concept released within a day of disclosure. Ivanti Sentry has been a repeat KEV target, cited twice before this incident, and AppTrana's Default Rule Set closed this instance the same day it was disclosed, ahead of any vendor patch.

Cisco Catalyst SD-WAN: upload-based escalation caught

Mandiant documented a threat actor escalating from a compromised admin account to root-level access using a malicious file upload, then executing deliberate anti-forensic cleanup to erase its tracks. The exact upload-based escalation technique is the pattern AppTrana's Malicious File Upload policy is built to catch, and did.

Command-Injection KEV Cluster: five unrelated products, one policy

Kemp LoadMaster, Avada/Fusion Builder, FOSSBilling, and Gogs (twice), five separately disclosed, unrelated products, all added to CISA KEV within the same two-week window, and all closed by the AppTrana security policy.

Every Vulnerability Blocked, by Category

Each of the 400 vulnerabilities blocked in June 2026 traces back to a specific CVE, blocking rule, and scanner check, ready for audit or compliance review.

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 180 blocked · avg CVSS 8.8 · 16 CISA KEV				
CVE-2026-10520	More Evidence That Words Don't Mean What We Though...	Critical / 10	CISA KEV	✓ Blocked
CVE-2026-10523	CVE-2026-10520, CVE-2026-10523 - Multiple critical v...	Critical / 10	CISA KEV	✓ Blocked
CVE-2023-38035	CVE-2026-10520, CVE-2026-10523 - Multiple critical v...	Critical / 10	CISA KEV	✓ Blocked
CVE-2020-15505	CVE-2026-10520, CVE-2026-10523 - Multiple critical v...	Critical / 10	CISA KEV	✓ Blocked
CVE-2026-52704	Improper Control of Generation of Code ('Code Injection'...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-25470	Improper Control of Generation of Code ('Code Injection'...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-10561	IBM Langflow OSS 1.0.0 through 1.9.3 has an vulnerability...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-52813	Gogs is an open source self-hosted Git service.	Critical / 10	CISA KEV	✓ Blocked
CVE-2025-71338	Flowise contains a path traversal vulnerability in the /api/...	Critical / 10	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-46850	Vulnerability in the MySQL Shell product of Oracle MySQ...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-5366	Prefect version 3.6.23 is vulnerable to remote code exec...	Critical / 9.9	PUBLIC EXPLOIT/POC	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 180 blocked · avg CVSS 8.8 · 16 CISA KEV (continued)				
CVE-2026-56274	Flowise before 3.1.2 contains multiple OS command injec...	Critical / 9.9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-44789	n8n is an open source workflow automation platform.	Critical / 9.9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-52806	Gogs is an open source self-hosted Git service.	Critical / 9.9	CISA KEV	✓ Blocked
CVE-2026-54158	SiYuan is an open-source personal knowledge managem...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-8037	ZDI-26-340: Progress Software Kemp LoadMaster dodel...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2013-3821	Active Exploitation of Oracle PeopleSoft Zero-Day (CVE-...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2017-3548	Active Exploitation of Oracle PeopleSoft Zero-Day (CVE-...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2018-25436	WordPress Plugin Baggage Freight Shipping Australia 0.1...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-38329	Bludit CMS before version 3.18.4 allows Remote Code Ex...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39006	An issue in SNMP4J-Agent 3.8.3 allows a remote attacker...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-27053	Unauthenticated PHP Object Injection in Broadcast Live ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49085	Unauthenticated PHP Object Injection in WP Insightly for ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49104	Unauthenticated PHP Object Injection in Integration for K...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49105	Unauthenticated PHP Object Injection in WP Zendesk for ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49106	Unauthenticated PHP Object Injection in Integration for C...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49109	Unauthenticated PHP Object Injection in Integration for S...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49763	Unauthenticated PHP Object Injection in Integration for C...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49765	Unauthenticated PHP Object Injection in Integration for ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49768	Unauthenticated PHP Object Injection in Happyforms <= ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49769	Unauthenticated PHP Object Injection in wpForo Forum <...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 180 blocked · avg CVSS 8.8 · 16 CISA KEV (continued)				
CVE-2026-49770	Unauthenticated PHP Object Injection in WP Travel Engin...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49781	Unauthenticated PHP Object Injection in OttoKit <= 1.1.2...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9691	Unauthenticated PHP Object Injection in Integration for A...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-35380	Vulnerability in the WebLogic Server product of Oracle Fu...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-60205	Unauthenticated PHP Object Injection in ThemeREX Add...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-69108	Unauthenticated PHP Object Injection in Hot Coffee <= 1....	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-69122	Unauthenticated PHP Object Injection in SeaFood Compa...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-27429	Unauthenticated PHP Object Injection in Nifty <= 1.4.1 ve...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39529	Unauthenticated PHP Object Injection in Elementra <= 1....	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40725	Unauthenticated PHP Object Injection in WooCommerce ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42380	Unauthenticated PHP Object Injection in AI Lab < 5.4.2 ve...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49075	Contributor PHP Object Injection in JetEngine <= 3.8.9.1 ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49107	Unauthenticated PHP Object Injection in Thrive Apprenti...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-52706	Unauthenticated PHP Object Injection in JetEngine <= 3....	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54194	Contributor PHP Object Injection in Fusion Builder <= 3.1...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54806	Unauthenticated PHP Object Injection in WP Activity Log ...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2025-69111	Unauthenticated PHP Object Injection in Reisen <= 1.4.1 ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-69127	Unauthenticated PHP Object Injection in Plumbing <= 1.6 ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49108	Unauthenticated PHP Object Injection in Moderno < 1.43 ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12569	A critical remote code execution (RCE) vulnerability has b...	Critical / 9.8	CISA KEV	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 180 blocked · avg CVSS 8.8 · 16 CISA KEV (continued)				
CVE-2026-54414	FileRise before 3.16.0 is vulnerable to path traversal in th...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2022-50972	WooCommerce 7.1.0 contains a remote code execution v...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2024-58351	Flowise before 2.1.4 allows configuration to be injected in...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-67038	An issue was discovered in Lantronix EDS5000 2.1.0.0R3.	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2026-53753	Crawl4AI is an open-source LLM friendly web crawler & s...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-56121	Feast before 0.63.0 contains an unsafe deserialization vul...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-39938	Cacti is an open source performance and fault managem...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-40079	Cacti is an open source performance and fault managem...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-71333	Flowise through 2.2.4 contains an unauthenticated arbitr...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2025-71334	Flowise before 3.0.6 (affected versions 2.2.8 and earlier) ...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2025-71336	Flowise before 3.0.6 (affected versions 2.2.7-patch.1 and...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-55743	The shell tool command allowlist in the SecurityPolicy of ...	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55742	Cotonti 1.0.0 (master branch, commit f43f1fc3) is vulnera...	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56395	SiYuan before v3.6.1 fails to sanitize package metadata a...	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56397	SiYuan before v3.6.1 fails to sanitize package metadata a...	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-48519	Langflow is a tool for building and deploying AI-powered ...	Critical / 9.6	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-48909	SP LMS (com_splms) < 4.1.4 by JoomShaper deserializes...	Critical / 9.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-28496	FOSSBilling is a free, open-source billing and client mana...	Critical / 9.4	CISA KEV	✓ Blocked
CVE-2026-55413	ToolJet is the open-source foundation an AI-native platf...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-5482	Responsive FileManager's allows an unauthenticated atta...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 180 blocked · avg CVSS 8.8 · 16 CISA KEV (continued)				
CVE-2026-54088	File Browser is a file managing interface for uploading, de...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-48853	Deserialization of Untrusted Data and Allocation of Reso...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-45034	PhpSpreadsheet is a pure PHP library for reading and writ...	Critical / 9.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-22313	The device has a webserver that exposes a REST API aut...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-36418	JimuReport versions 2.3.4 and below are vulnerable to re...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-8713	The Avada (Fusion) Builder plugin for WordPress is vulne...	Critical / 9.1	CISA KEV	✓ Blocked
CVE-2026-12045	Read-only transaction bypass in the pgAdmin 4 AI Assist...	Critical / 9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12046	Two state-mutating endpoints in pgAdmin 4's SQL Editor...	Critical / 9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42850	Kitty is a cross-platform GPU based terminal.	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2016-20075	WordPress Ultimate Product Catalog 3.8.6 contains an ar...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-39474	Contributor PHP Object Injection in Post Duplicator <= 3....	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39478	Contributor PHP Object Injection in Anti-Malware Securit...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39532	Contributor PHP Object Injection in Events Calendar for ...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-48017	DbGate is cross-platform database manager.	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-6933	The Premmerce Dev Tools plugin for WordPress is vulner...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12256	Contributor PHP Object Injection in Avada <= 3.15.3 versi...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-69130	Subscriber PHP Object Injection in Entrepreneur - Bookin...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9860	The Offload, AI & Optimize with Cloudflare Images plugin...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2019-25758	Joomla! Component vBizz 1.0.7 contains an unrestricted ...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-49241	The Angular Language Service VS Code Extension provid...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 180 blocked · avg CVSS 8.8 · 16 CISA KEV (continued)				
CVE-2026-54232	vLLM is an inference and serving engine for large langua...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-34916	A missing validation of user input when saving delivery li...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-44959	A missing validation of user input exists when saving deli...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9772	Unraid Web Server FileUpload Command Injection Remot...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-9773	Unraid Web Server ToggleState Command Injection Rem...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-12242	The AdRotate Banner Manager plugin for WordPress is vu...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57296	Jenkins External Workspace Manager Plugin 1.3.2 and ea...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57301	Jenkins OWASP ZAP Plugin 1.0.7 and earlier performs bui...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-48732	Warp is an agentic development environment.	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-56053	Subscriber PHP Object Injection in EventPrime <= 4.3.4.1 ...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57281	Jenkins Script Security Plugin 1402.v94c9ce464861 and...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-44017	Docling simplifies document processing by parsing diver...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-44016	Docling simplifies document processing by parsing diver...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42687	Unauthenticated PHP Object Injection in EventPrime <= ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-8442	The WP Review Slider Pro plugin for WordPress is vulner...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-46851	Vulnerability in the PeopleSoft Enterprise CS Campus Co...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39443	Unauthenticated PHP Object Injection in EmallShop <= 2....	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39446	Unauthenticated PHP Object Injection in Kapee < 1.7.0 ve...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39539	Unauthenticated PHP Object Injection in Alloggio - Hotel ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39545	Unauthenticated PHP Object Injection in Zermatt <= 1.6.1...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 180 blocked · avg CVSS 8.8 · 16 CISA KEV (continued)				
CVE-2026-39554	Unauthenticated PHP Object Injection in Fidalgo <= 1.2.2 ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39557	Unauthenticated PHP Object Injection in NeoBeat <= 1.7 ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39567	Unauthenticated PHP Object Injection in Santé <= 1.5.1 v...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39573	Unauthenticated PHP Object Injection in Mildhill <= 1.5 v...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39580	Unauthenticated PHP Object Injection in Micdrop <= 1.3.1...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40735	Unauthenticated PHP Object Injection in Reina <= 2.1 ver...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40736	Unauthenticated PHP Object Injection in Laurits <= 1.5.1 ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40739	Unauthenticated PHP Object Injection in LuxeDrive <= 1....	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40751	Unauthenticated PHP Object Injection in Ashtanga <= 1.2 ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40753	Unauthenticated PHP Object Injection in EasyMeals <= 1....	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40754	Unauthenticated PHP Object Injection in Roisin <= 1.4 ver...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40755	Unauthenticated PHP Object Injection in TechLink <= 1.3 ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40758	Unauthenticated PHP Object Injection in Léonie <= 1.2.1 v...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40759	Unauthenticated PHP Object Injection in Esmée <= 1.4 ve...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40760	Unauthenticated PHP Object Injection in Behold <= 1.5 ve...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40761	Unauthenticated PHP Object Injection in Valeska <= 1.2.2...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39442	Unauthenticated PHP Object Injection in PressMart <= 1....	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39445	Unauthenticated PHP Object Injection in Alukas < 3.0.0 v...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39556	Unauthenticated PHP Object Injection in Konsept <= 1.9 ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39560	Unauthenticated PHP Object Injection in Hiroshi <= 1.5.1 ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 180 blocked · avg CVSS 8.8 · 16 CISA KEV (continued)				
CVE-2026-39576	Unauthenticated PHP Object Injection in SingleMalt <= 1....	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40733	Unauthenticated PHP Object Injection in ShiftUp <= 1.3 v...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40738	Unauthenticated PHP Object Injection in Eldon <= 1.4.1 v...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40752	Unauthenticated PHP Object Injection in Manufaktur Solu...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40756	Unauthenticated PHP Object Injection in Zoya <= 1.4 vers...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40757	Unauthenticated PHP Object Injection in Château <= 1.2.1...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49286	PhpWeasyPrint is a PHP library allowing PDF generation f...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9843	The Database for Contact Form 7, WPforms, Elementor fo...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-71348	picklescan before 0.0.28 fails to detect malicious pickle fi...	High / 8.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2025-71357	picklescan before 0.0.30 fails to detect malicious pickle fi...	High / 8.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2025-71378	picklescan before 0.0.30 fails to detect cProfile.runctx fu...	High / 8.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-9072	IBM WebSphere Application Server and IBM WebSphere ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55388	piscina is a node.js worker pool implementation.	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-45135	Caddy is an extensible server platform that uses TLS by d...	High / 8.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-49402	Deno is a JavaScript, TypeScript, and WebAssembly runti...	High / 8.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-39253	An issue in Pivotal CRM v.6.6.04.08 allows a remote attac...	High / 8.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-54512	jackson-databind contains the general-purpose data-bin...	High / 8.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-49290	Slopsmith is a self-contained web application for browsin...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-11911	The Simple File List plugin for WordPress is vulnerable to ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-41523	vLLM is an inference and serving engine for large langua...	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 180 blocked · avg CVSS 8.8 · 16 CISA KEV (continued)				
CVE-2026-55697	pnpm is a package manager.	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-39434	Shop manager PHP Object Injection in CTX Feed <= 6.6.2...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39471	Author PHP Object Injection in ShortPixel Image Optimiz...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39472	Shop manager PHP Object Injection in WooCommerce P...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39481	Author PHP Object Injection in Modula Image Gallery <= ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39498	Shop manager PHP Object Injection in YayMail <= 4.3.3 v...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39499	Shop manager PHP Object Injection in Advanced Product...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-11407	Pimcore CMS/DXP version 12.3.8 contains a sandbox byp...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56382	Craft CMS (composer package craftcms/cms) versions >...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56446	MISP allowed a site administrator to configure an arbitrar...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12115	The Counter Box – Add Countdowns, Timers & Dynamic ...	Medium / 6.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9815	The MagicForm WordPress plugin through 0.1.3 does not...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56304	picklescan before 1.0.1 contains an unsafe pickle deserial...	Medium / 6.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-55249	@rtk-ai/rtk-rewrite transparently rewrites shell command...	Medium / 6.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2016-20082	WordPress Plugin Abtest contains a local file inclusion vu...	Medium / 6.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-39577	Unauthenticated PHP Object Injection in Playroom <= 1.4...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39578	Unauthenticated PHP Object Injection in Valiance <= 1.2 ...	Medium / 5.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12565	The unarchive internal module's archive extraction comm...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49345	Mercator is an open source web application that enables ...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54686	Warp is an agentic development environment.	Medium / 4.3	PUBLIC EXPLOIT/POC	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 180 blocked · avg CVSS 8.8 · 16 CISA KEV (continued)				
ZD-6957A6DC88860 1F6	[webapps] Grav CMS 2.0.0-beta.2 - Remote Code Execut...	Unknown	PUBLIC EXPLOIT/POC	✓ Blocked
ZD-9809053C15578 C74	[webapps] scramble - Remote Code Execution	Unknown	PUBLIC EXPLOIT/POC	✓ Blocked
ZD-3024774F1462B 7E7	[webapps] Quick Playground for WordPress 1.3.1 - Unaut...	Unknown	PUBLIC EXPLOIT/POC	✓ Blocked
ZD-56D26310F8A1F 98D	[webapps] Langflow 1.3.0 - Remote Code Execution	Unknown	PUBLIC EXPLOIT/POC	✓ Blocked
ZD-90B1F1500448D A45	[webapps] MixPHP Framework 2.2.17 - Unsafe Deserializ...	Unknown	PUBLIC EXPLOIT/POC	✓ Blocked
ZD-3741748785035 2B1	[remote] Notepad++ 8.9.6 - Arbitrary Code Execution	Unknown	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-20253	CVE-2026-20253 | Splunk Enterprise PostgreSQL Sidec...	Unknown	CISA KEV	✓ Blocked
CVE-2026-28318	A Crash, Not a Shell: SolarWinds Serv-U CVE-2026-28318	Unknown	CISA KEV	✓ Blocked
CVE-2025-54068	CVE-2025-54068 Laravel Livewire Credential Theft Cam...	Unknown	CISA KEV	✓ Blocked
SQL Injection: 93 blocked · avg CVSS 8.2				
CVE-2026-44172	MariaDB server is a community developed fork of MySQL...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-38812	RuoYi v4.8.2 is vulnerable to SQL Injection via the /tool/g...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-48114	Metacat is data repository software that helps researcher...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55740	Nur-Alam39 bus-ticket (no released versions; latest com...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54419	claudiopizzillo PIAF-HMS (PBX-In-A-Flash Hotel Manage...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39948	Cacti is an open source performance and fault managem...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39955	Cacti is an open source performance and fault managem...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-39441	Unauthenticated SQL Injection in Feed KuantoKusta for ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42386	Unauthenticated SQL Injection in Order Delivery Date for ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 93 blocked · avg CVSS 8.2 (continued)				
CVE-2026-49776	Unauthenticated SQL Injection in GPTranslate – Multiling...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49772	Improper Neutralization of Special Elements used in an S...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-52715	Unauthenticated SQL Injection in GEO my WordPress <= ...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54815	Improper Neutralization of Special Elements used in an S...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54849	Unauthenticated SQL Injection in Premmerce Wishlist for...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-44792	n8n is an open source workflow automation platform.	Critical / 9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-36670	A Time-Based Blind SQL Injection vulnerability in the alia...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-8443	The WP Review Slider Pro plugin for WordPress is vulner...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-8444	The WP Review Slider Pro plugin for WordPress is vulner...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12044	SQL injection in pgAdmin 4 across every dialog template ...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-8163	The Infility Global WordPress plugin before 2.15.19 does ...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-48964	Subscriber SQL Injection in ELEX WordPress HelpDesk & ...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-69135	Subscriber SQL Injection in Events Schedule - WordPres...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-22335	Subscriber SQL Injection in WooCommerce Frontend Ma...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34914	A missing sanitisation of user input in the zone-include.p...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2016-20068	WordPress Booking Calendar Contact Form version 1.0.2...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2016-20069	WordPress Booking Calendar Contact Form 1.0.23 contai...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2016-20071	The 404 Redirection Manager plugin version 1.0 for Word...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2016-20072	BBS e-Franchise 1.1.1 plugin for WordPress contains an S...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2016-20073	Answer My Question 1.3 plugin for WordPress contains a...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 93 blocked · avg CVSS 8.2 (continued)				
CVE-2017-20252	Joomla NextGen Editor 2.1.0 contains an SQL injection vu...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20253	Joomla! Component My Projects 2.0 contains an SQL inje...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20254	Joomla! Component User Bench 1.0 contains an SQL inje...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20255	Joomla! Component JB Visa 1.0 contains an SQL injectio...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20256	Joomla Survey Force Deluxe 3.2.4 contains an SQL inject...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20257	Joomla! Component Quiz Deluxe 3.7.4 contains an SQL in...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20258	Joomla! Component RPC Responsive Portfolio 1.6.1 cont...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20259	Joomla OSDownloads 1.7.4 contains an SQL injection vul...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20260	Joomla! Component Price Alert 3.0.2 contains an SQL inj...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20261	Joomla! Component Bargain Product VM3 1.0 contains a...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20262	Joomla! Component Ajax Quiz 1.8 contains an SQL injecti...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20263	Joomla! Component FocalPoint Pro/Free 1.2.3 contains a...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20266	Joomla SP Movie Database 1.3 contains an SQL injection ...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20267	Joomla! Component Calendar Planner 1.0.1 contains an S...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20268	Joomla! Component Zap Calendar Lite 4.3.4 contains an ...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20269	Joomla! Component KissGallery 1.0.0 contains an SQL inj...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20270	Joomla! Component Twitch Tv 1.1 contains an SQL injecti...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20271	Joomla StreetGuessr Game 1.1.8 contains an SQL injectio...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20272	Joomla Ultimate Property Listing 1.0.2 contains an SQL in...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20273	Joomla Event Registration Pro Calendar 4.1.3 contains an...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 93 blocked · avg CVSS 8.2 (continued)				
CVE-2017-20274	Joomla LMS King Professional 3.2.4.0 contains an SQL inj...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20275	Joomla! Component PHP-Bridge 1.2.3 contains an SQL in...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20276	Joomla! Component SIMGenealogy 2.1.5 contains an SQL...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20277	Joomla JoomRecipe 1.0.4 component contains a blind SQ...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20278	Joomla Component JoomRecipe 1.0.3 contains an SQL in...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20279	Joomla Payage 2.05 contains an SQL injection vulnerabili...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20280	Joomla Component Myportfolio 3.0.2 contains an SQL inj...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20281	Joomla! Component Extra Search 2.2.8 contains an SQL i...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20282	Joomla! Component jCart for OpenCart 2.0 contains an S...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2019-25748	Joomla JHotelReservation 6.0.7 contains an SQL injectio...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2019-25750	Joomla Component J-MultipleHotelReservation 6.0.7 co...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2019-25751	Joomla Component J-ClassifiedsManager 3.0.5 contains ...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2019-25752	Joomla! Component J-BusinessDirectory 4.9.7 contains ...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2019-25753	Joomla! Component VMap 1.9.6 contains an SQL injectio...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2019-25754	Joomla Component vRestaurant 1.9.4 contains an SQL inj...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2019-25755	Joomla Component vReview 1.9.11 contains an SQL inject...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2019-25756	Joomla! Component vAccount 2.0.2 contains an SQL inje...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-56351	n8n before version 2.4.0 contains a sql injection vulnerab...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-66336	Apache Doris MCP Server contains a SQL injection vulner...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54313	n8n is an open source workflow automation platform.	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 93 blocked · avg CVSS 8.2 (continued)				
CVE-2026-37149	GROCERY-STORE-MANAGEMENT-SYSTEM-USING-PHP...	High / 7.7	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-6428	SQL Injection in reports/catalogue_out.pl in Koha Commu...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9848	The WP Ticket plugin for WordPress is vulnerable to SQL ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12360	The JetEngine plugin for WordPress is vulnerable to SQL ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-8705	The ClearSale Total plugin for WordPress is vulnerable to ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9179	The WP Forms Connector plugin for WordPress is vulner...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12077	The Dokan Pro plugin for WordPress is vulnerable to time...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12937	The Tourfic – AI Powered Travel Booking, Hotel Booking ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12775	A vulnerability was detected in Montodel House-Rental-...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40083	Cacti is an open source performance and fault managem...	High / 7.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2019-25746	WordPress Sliced Invoices 3.8.2 contains an authenticate...	High / 7.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20264	Joomla! Component Sponsor Wall 8.0 contains an SQL inj...	High / 7.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2017-20265	Joomla! Component Flip Wall 8.0 contains an SQL injecti...	High / 7.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2019-25749	Joomla J-CruisePortal 6.0.4 contains an SQL injection vu...	High / 7.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2019-25757	Joomla vWishlist 1.0.1 contains an SQL injection vulnerab...	High / 7.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2019-25759	Joomla! Component vBizz 1.0.7 contains an SQL injection...	High / 7.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2019-25761	Joomla! Component JoomCRM 1.1.1 contains an SQL inje...	High / 7.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2025-71332	Flowise through 2.2.7 contains a SQL injection vulnerabili...	Medium / 6.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-11776	The Form Maker by 10Web – Mobile-Friendly Drag & Dro...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-11777	The Form Maker by 10Web – Mobile-Friendly Drag & Dro...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 93 blocked · avg CVSS 8.2 (continued)				
ZD-C7C78CB0F7D9083E	[webapps] OpenCATS 0.9.7.4 - SQL Injection	Unknown	PUBLIC EXPLOIT/POC	✓ Blocked
ZD-B86FA9BEEE0BF887	[webapps] MikroORM 7.0.13 - SQL Injection	Unknown	PUBLIC EXPLOIT/POC	✓ Blocked
ZD-1C5AA772CD4F17A5	[webapps] Drupal Core 10.5.5 - Error-Based SQL Injection	Unknown	PUBLIC EXPLOIT/POC	✓ Blocked
ZD-68C1C3A71C86732D	[webapps] WordPress Contest Gallery 28.1.4 - Unauthen...	Unknown	PUBLIC EXPLOIT/POC	✓ Blocked
Path Traversal: 40 blocked · avg CVSS 7.4 · 3 CISA KEV				
CVE-2026-54917	SeaweedFS is a distributed storage system for object sto...	Critical / 10	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-50869	An issue in the api/plugin.php component of Bludit v3.19....	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-7515	The BetterDocs Pro plugin for WordPress is vulnerable to...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2026-50203	A path traversal in the SFTP provider (`SFTPHook.retriev...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-20181	A vulnerability in Cisco ISE and ISE-PIC could allow an aut...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-11769	We have released version 5.24.0 of the Grafana Operator.	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-50016	pnpm is a package manager.	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-48716	nanobot is a personal AI assistant.	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-69115	Unauthenticated Local File Inclusion in LuxMed	Medicin...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54814	Improper Control of Filename for Include/Require Statem...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-45233	HTMLy CMS through 3.1.1 contains a path traversal vulne...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-60223	Subscriber Arbitrary File Deletion in WPBot Pro Wordpres...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55488	motionEye (mEye) is an online interface for a piece of sof...	High / 7.7	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2016-20076	WordPress Simple-Backup 2.7.11 contains multiple vulner...	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 40 blocked · avg CVSS 7.4 · 3 CISA KEV (continued)				
CVE-2016-20081	WordPress Plugin HB Audio Gallery Lite 1.0.0 contains a p...	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2025-69131	Unauthenticated Arbitrary File Download in WordPress & ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54293	NLTK (Natural Language Toolkit) is a suite of open source...	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-53571	Vite is a frontend tooling framework for JavaScript.	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-52844	Caddy is an extensible server platform that uses TLS by d...	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2025-71324	Flowise before 3.0.6 contains an arbitrary file read vulner...	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-50015	pnpm is a package manager.	High / 7.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-55700	pnpm is a package manager.	High / 7.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-39468	Contributor Arbitrary File Deletion in Meta Box – WordPre...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-20262	A vulnerability in the web UI of Cisco Catalyst SD-WAN M...	Medium / 6.5	CISA KEV	✓ Blocked
CVE-2026-42867	Langflow is a tool for building and deploying AI-powered ...	Medium / 6.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-31978	motionEye (mEye) is an online interface for motion softw...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55699	pnpm is a package manager.	Medium / 6.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-40084	Cacti is an open source performance and fault managem...	Medium / 6.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2016-20077	WordPress Plugin Photocart Link 1.6 contains a local file i...	Medium / 6.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2016-20078	WordPress IMDb Profile Widget 1.0.8 contains a local file ...	Medium / 6.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2016-20079	WordPress Dharma Booking 2.28.3 and earlier contains a ...	Medium / 6.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2016-20080	WordPress Brandfolder plugin version 3.0 and earlier con...	Medium / 6.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2019-25760	Joomla! Component Easy Shop 1.2.3 contains a local file i...	Medium / 6.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-12089	The LWS Optimize – All-in-One Speed Booster & Cache T...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 40 blocked · avg CVSS 7.4 · 3 CISA KEV (continued)				
CVE-2026-7547	The Woosa – Marktplaats for WooCommerce plugin for W...	Medium / 4.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54014	Open WebUI is a self-hosted artificial intelligence platfor...	Medium / 4.3	PUBLIC EXPLOIT/POC	✓ Blocked
ZD-880BE8E03FA5C C0B	[webapps] Casdoor 3.54.1 - Arbitrary File Write via Path T...	Unknown	PUBLIC EXPLOIT/POC	✓ Blocked
ZD-A09075F561214 62B	[webapps] Prodigy Commerce 3.3.0 - Local File Inclusion	Unknown	PUBLIC EXPLOIT/POC	✓ Blocked
ZD-154AE34C26562 E54	[webapps] WordPress OrderConvo 14 - Path Traversal	Unknown	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2025-8088	STOCKSTAY Another Day: The Latest Addition to Turla's I...	Unknown	CISA KEV	✓ Blocked
Cross-Site Scripting: 33 blocked · avg CVSS 6.7				
CVE-2026-53662	immich is a high performance self-hosted photo and vide...	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-44990	ApostropheCMS is an open-source Node.js content man...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12048	Stored cross-site scripting in pgAdmin 4's error-renderin...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-5305	The Email Address Encoder WordPress plugin before 1.0....	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54011	Open WebUI is a self-hosted artificial intelligence platfor...	High / 8.7	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-54013	Open WebUI is a self-hosted artificial intelligence platfor...	High / 7.6	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-9109	The GPTranslate – Multilingual AI Translation for WordPre...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-5513	The Online Scheduling and Appointment Booking System...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2016-20066	WordPress CP Polls 1.0.8 contains a persistent cross-site...	High / 7.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2016-20084	WordPress appointment-booking-calendar 1.1.24 contain...	High / 7.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-3652	The ARForms plugin for WordPress is vulnerable to Store...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-10091	The Email JavaScript Cloak plugin for WordPress is vulne...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 33 blocked · avg CVSS 6.7 (continued)				
CVE-2026-10092	The Cincopa video and media plug-in plugin for WordPre...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9643	The WP Meta SEO plugin for WordPress is vulnerable to ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49055	Unauthenticated Cross Site Scripting (XSS) in Drag and ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-8089	The weMail: Email Marketing, Email Automation, Newslett...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9570	The Taskbuilder WordPress plugin before 5.0.8 does not ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-4259	The ultimate-woocommerce-auction-pro WordPress plu...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-6858	The Transbank Webpay WordPress plugin before 1.14.0 d...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-50146	Astro is a web framework.	High / 7.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-8172	The Simple Basic Contact Form WordPress plugin throug...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-3297	The Page Builder: Pagelayer – Drag and Drop website buil...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2016-20070	WordPress Booking Calendar Contact Form 1.0.23 contai...	Medium / 6.4	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2025-71331	Flowise before 3.0.8 contains a cross-site scripting (XSS...	Medium / 6.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-10850	Plane CE 1.3.1 allows a low-privileged project member to ...	Medium / 5.4	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-44311	Fabric.js is a Javascript HTML5 canvas library.	Medium / 5.4	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-54025	LibreChat is an enhanced ChatGPT clone that supports m...	Medium / 5.4	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-44587	CarrierWave is a framework to upload files from Ruby app...	Medium / 4.7	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-54298	Astro is a web framework.	Medium / 4.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-52846	Caddy is an extensible server platform that uses TLS by d...	Medium / 4.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-4983	Open VSX Registry does not sanitize SVG files uploaded ...	Medium / 4.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-44960	A stored XSS can be exploited by leveraging the usernam...	Low / 0	PUBLIC EXPLOIT/POC	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 33 blocked · avg CVSS 6.7 (continued)				
ZD-8A2407006C834C70	[webapps] CubeCart < 6.7.0 - Reflected Cross-Site Scrip...	Unknown	PUBLIC EXPLOIT/POC	✓ Blocked
SSRF: 24 blocked · avg CVSS 7.4 · 2 CISA KEV				
CVE-2026-55454	Appsmith is a platform to build admin panels, internal tool...	Critical / 9.9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-35273	ZDI-26-387: Oracle PeopleSoft HttpListeningConnector ...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2026-48814	Network-AI is a TypeScript/Node.js multi-agent orchestr...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56266	Crawl4AI before 0.8.7 contains a server-side request forg...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-53755	Crawl4AI is an open-source LLM friendly web crawler & s...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54008	Open WebUI is a self-hosted artificial intelligence platfor...	High / 8.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-46717	Nezha Monitoring is a self-hostable, lightweight, servers ...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54018	Open WebUI is a self-hosted artificial intelligence platfor...	High / 7.7	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-54033	LibreChat is an enhanced ChatGPT clone that supports m...	High / 7.7	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-9006	IBM WebSphere Application Server 9.0, and 8.5 is vulner...	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-11395	The CF7 to Webhook plugin for WordPress is vulnerable t...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12095	The Kargo Takip plugin for WordPress is vulnerable to Se...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12100	The URL Preview plugin for WordPress is vulnerable to S...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-50189	Appsmith is a platform to build admin panels, internal tool...	High / 7.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-56275	Flowise before 3.1.0 contains a server-side request forge...	High / 7.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-48782	Pydantic AI is a Python agent framework for building appl...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-11989	The Bit Integrations – Form Integration, Webhook, Sprea...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 24 blocked · avg CVSS 7.4 · 2 CISA KEV (continued)				
CVE-2026-50221	In OpenStack Swift before 2.37.2, proxy-server does not ...	Medium / 6.4	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-12774	A security vulnerability has been detected in BerriAI litell...	Medium / 6.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-12798	A weakness has been identified in BerriAI litellm up to 1.8...	Medium / 6.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-55599	phpseclib is a PHP secure communications library.	Medium / 5.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-49979	Appsmith is a platform to build admin panels, internal tool...	Low / 2.7	PUBLIC EXPLOIT/POC	✓ Blocked
ZD-5F1CAB80D00956EB	[webapps] EspoCRM 9.3.3 - SSRF	Unknown	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-20230	CVE-2026-20230 | Cisco Unified Communications Mana...	Unknown	CISA KEV	✓ Blocked
Injection (General): 11 blocked · avg CVSS 8.2				
CVE-2026-53609	ApostropheCMS is an open-source Node.js content man...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-48714	i18next-http-middleware is a middleware to be used with ...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-45688	Rocket.Chat is an open-source, secure, fully customizabl...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-45689	Rocket.Chat is an open-source, secure, fully customizabl...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-47835	In Spring AI Vector Stores, special characters could be us...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-52845	Caddy is an extensible server platform that uses TLS by d...	High / 8.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-48979	PHP Standard Library (PSL) is set of APIs covering async,...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55603	http-proxy-middleware is node.js http-proxy middleware.	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-8646	IBM WebSphere Application Server 9.0 and 8.5 and IBM ...	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54019	Open WebUI is a self-hosted artificial intelligence platfor...	Medium / 6.5	PUBLIC EXPLOIT/POC	✓ Blocked
ZD-938E56DC1CA225B3	[webapps] cPanel – CRLF Injection	Unknown	PUBLIC EXPLOIT/POC	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Insecure Design (File-Upload Pattern): 11 blocked · avg CVSS 9.5 · 5 CISA KEV				
CVE-2025-69129	Unauthenticated Arbitrary File Upload in WordPress & W...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57780	Unrestricted Upload of File with Dangerous Type vulnera...	Critical / 10	CISA KEV	✓ Blocked
CVE-2026-27041	Contributor Arbitrary File Upload in Unlimited Elements f...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-48988	A vulnerability in SP Page Builder for Joomla allows unaut...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2026-48939	A vulnerability in the iCagenda extension for Joomla allow...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-49268	A remote attacker can inject LDAP special characters into...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56345	AVideo through 29.0 contains an authorization bypass vu...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
ZD-2E5201C53C6EC296	[webapps] YAMCS yamcs-core 5.12.7 - LDAP Injection	Unknown	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-20127	Zero-Day Exploitation of Vulnerability (CVE-2026-20245...	Unknown	CISA KEV	✓ Blocked
CVE-2026-20182	Zero-Day Exploitation of Vulnerability (CVE-2026-20245...	Unknown	CISA KEV	✓ Blocked
CVE-2026-20245	Zero-Day Exploitation of Vulnerability (CVE-2026-20245...	Unknown	CISA KEV	✓ Blocked
Uncontrolled Resource Consumption: 7 blocked · avg CVSS 6.8				
CVE-2026-9071	IBM WebSphere Application Server 9.0, and 8.5 and IBM ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56248	Cap-go capgo (capgo-backend) before 12.128.12 contain...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55446	Langflow is a tool for building and deploying AI-powered ...	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-54024	LibreChat is an enhanced ChatGPT clone that supports m...	Medium / 6.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-54037	LibreChat is an enhanced ChatGPT clone that supports m...	Medium / 6.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-9320	IBM WebSphere Application Server 9.0, and 8.5 and IBM ...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-10852	IBM WebSphere Application Server and IBM WebSphere ...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
XML Injection: 1 blocked · avg CVSS 9.4				
CVE-2026-44020	Docling simplifies document processing by parsing diver...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked

• ABOUT INDUSFACE

Autonomous Application Security for the AI Era

Indusface secures web, AI, and API applications of thousands of businesses across 95 countries. It is backed by institutional investors and is a category leader in cloud WAAP and API Security, with recognition from Gartner, Forrester, IDC, GigaOm, and G2.

Indusface AppTrana is the industry's only integrated autonomous application security platform that discovers and remediates vulnerabilities, and protects web, API, and AI applications against DDoS, bot, and zero-day attacks, backed by a 100% uptime guarantee. The human-in-the-loop system ensures zero false positives and SLA-backed compliance reports.

Bangalore | Delhi | Mumbai | Vadodara | Dallas

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