INDUSFACE™

ZERO-DAY VULNERABILITY REPORT

• MONTHLY BULLETIN · JULY 2026

Zero-Day Vulnerability Coverage Report

In July 2026, 323 zero-days emerged across the traffic AppTrana protects. AppTrana caught and blocked every one automatically, with no manual intervention and no exposure window.

323	100%	33	47
ZERO-DAYS BLOCKED	CATEGORY COVERAGE	CISA KEV CLOSED	AGENTIC AI / LLM CLOSED

CONTENTS

In this Report

Coverage data for every zero-day AppTrana blocked in July 2026, along with the exploitation, severity, and threat-intelligence context behind the numbers.

RESEARCH BASIS

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

Zero-Day Exposure Window: 0 Days

In July 2026, AppTrana's default rule set blocked 323 vulnerabilities across nine tracked categories, with 100% coverage in each and no manual tuning required. The gap between disclosure and protection, where exposure usually lives, never opened.

323

BLOCKED BY DEFAULT

AppTrana blocked 323 vulnerabilities by default, with 100% coverage across Command Injection, SQL Injection, Path Traversal, Cross-Site Scripting, SSRF, Injection, the file-upload pattern of Insecure Design, Uncontrolled Resource Consumption, and XML Injection.

33

CISA KEV CLOSED

CISA confirmed 33 of these vulnerabilities as actively exploited, most of them in a Command Injection cluster linked to Microsoft SharePoint, Langflow, ColdFusion, and SonicWall SMA1000.

Pre-patch

AI RANSOMWARE CHAIN CLOSED

Attackers used the Langflow AI-agent RCE chain (CVE-2025-3248, CVE-2026-33017) first to install cryptomining software, then to deliver ransomware built to encrypt AI model weights and vector indexes. AppTrana blocked this chain by default before either attack was observed.

47

AGENTIC AI & LLM CLOSED

AppTrana automatically blocked 47 vulnerabilities across prompt injection, RAG data exposure, and agent-to-tool trust boundaries. AI-related threats received the same coverage as any other threat.

Coverage by Category

Command Injection drew the heaviest attacker traffic, and AppTrana blocked all 143 attempts, including the Critical-severity SharePoint, Langflow, ColdFusion, and SonicWall disclosures covered in Section 07. Coverage stayed at 100% across every in-scope category.

CATEGORY	BLOCKED	CRITICAL	HIGH	AVG CVSS	PEAK
Command Injection	143	66	47	8.7	10.0
SQL Injection	70	13	56	7.8	10.0
Path Traversal	27	2	18	7.5	9.6
Cross-Site Scripting	31	3	15	6.9	9.6
SSRF	24	6	13	7.9	9.9
Injection	12	3	7	7.8	9.8
Insecure Design (File-Upload)	9	1	4	7.3	9.8
Uncontrolled Resource Consumption	6	0	3	6.7	8.1
XML Injection	1	0	1	7.5	7.5

Severity Snapshot

258 of the 323 blocked vulnerabilities (79.9%) were Critical or High severity, the tier organizations usually rush to patch first because it carries the highest risk. Here, no fast-track was needed: every one was already blocked at the edge, with no emergency patch cycle, out-of-band change, or manual configuration required.

BREAKDOWN BY SEVERITY

Critical	94	29.1%
High	164	50.8%
Medium	43	13.3%
Low	3	0.9%
Unscored	19	5.9%

258

CRITICAL + HIGH SEVERITY

These are the vulnerabilities most organizations rush to patch first, since an open exposure window here carries the highest risk. AppTrana had already blocked every one of them at the edge, with no emergency patch cycle, out-of-band change, or manual configuration needed.

Exploitation & KEV Status

Of the 323 vulnerabilities blocked, 33 were already confirmed by CISA as actively exploited and listed in the Known Exploited Vulnerabilities (KEV) catalog (10.2%). Another 32 had a public exploit or proof-of-concept in circulation (9.9%). The remaining 258 (79.9%) carried no known public exploit at the time of analysis.

33
CISA KEV · ACTIVELY EXPLOITED
10.2%

32
PUBLIC EXPLOIT / POC AVAILABLE
9.9%

258
NO KNOWN EXPLOIT
79.9%

NOTABLE CISA KEV ENTRIES BLOCKED

CVE	SEVERITY / CVSS	CATEGORY
CVE-2026-48558	Critical / 10.0	Command Injection
CVE-2026-48282	Critical / 10.0	Command Injection
CVE-2026-15409	Critical / 10.0	Command Injection
CVE-2026-57624	Critical / 10.0	Command Injection
CVE-2026-63030	Critical / 9.9	Command Injection
CVE-2026-60137	Critical / 9.9	Command Injection
CVE-2026-33017	Critical / 9.8	Command Injection
CVE-2026-5524	Critical / 9.8	Command Injection

05 • EMERGING RISK

Agentic AI & LLM Risk Coverage

Agentic AI and LLM components introduce a distinct exposure surface: prompt injection, insecure agent-to-tool trust boundaries, and exposed RAG data sources. Indusface identified 66 AI/LLM-tagged CVEs this period, and AppTrana blocked 47 of them automatically, concentrated heavily in Command Injection paths such as unauthenticated code-execution vulnerabilities in AI web-crawling and workflow-orchestration tools.

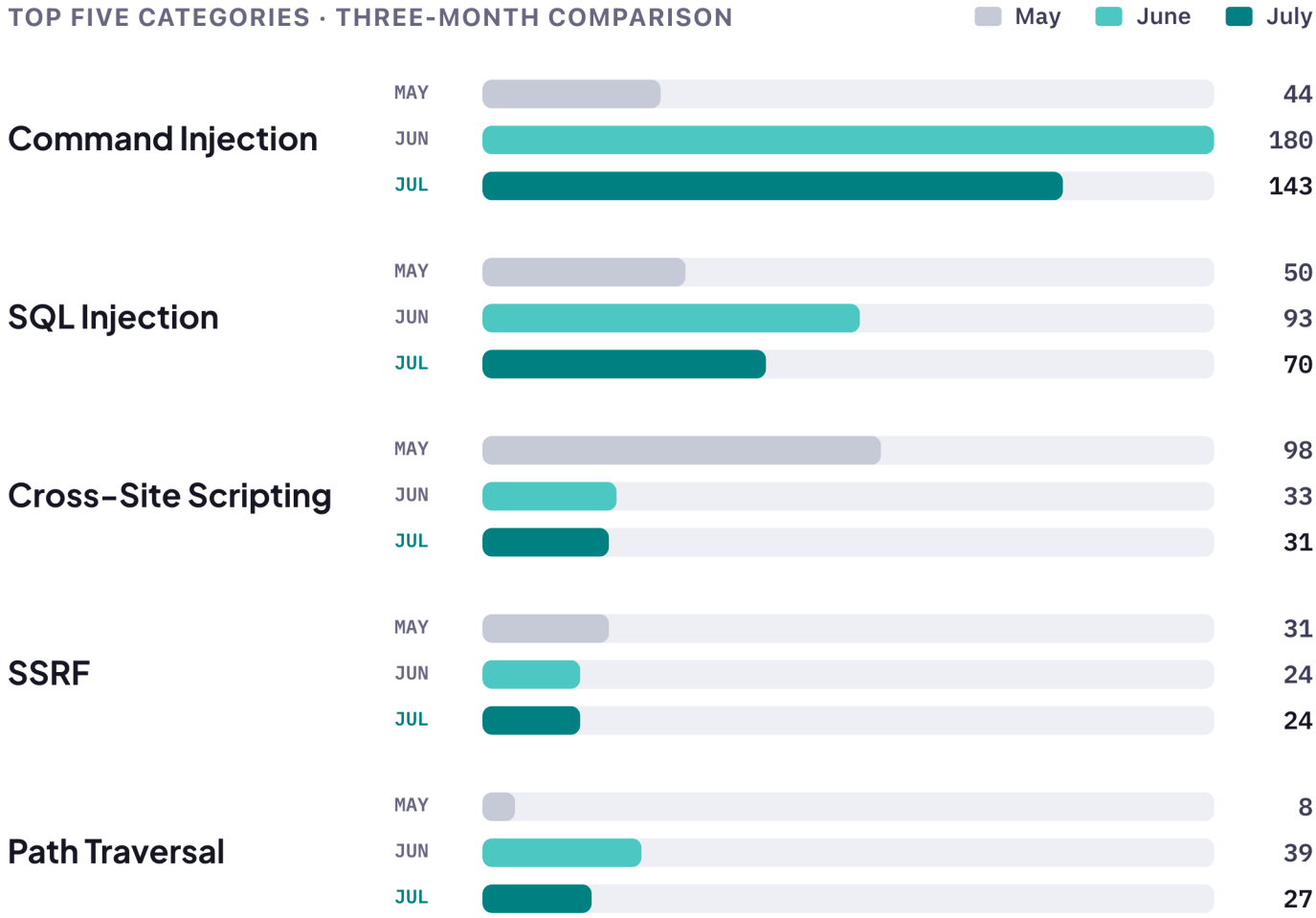
66	47	19	8.6	10.0
AI/LLM CVES IDENTIFIED	BLOCKED AUTOMATICALLY	CRITICAL SEVERITY	AVG CVSS (BLOCKED)	PEAK CVSS

THREAT TAG	CVES	WHAT IT COVERS
Agent-Framework Risk	54	Autonomous-agent frameworks and trust boundaries
Prompt-Injection Vectors	40	Direct or indirect prompt-injection paths
General LLM Application Risk	20	LLM application code and integrations
RAG Data Exposure	6	RAG pipelines and connected data sources
Embedding-Pipeline Risk	2	Vector index and embedding-generation pipelines

> A CVE can carry more than one AI threat tag, so the counts above overlap. Agent-framework risk dominated the surface this period, followed by prompt-injection vectors, showing that most new exposure comes from autonomous orchestration .

Vulnerability Trend

Command Injection attempts nearly tripled from May to June and eased slightly in July, though it remained the largest category by volume. SQL Injection and Path Traversal both pulled back from their June peaks. Cross-Site Scripting and SSRF held roughly flat. AppTrana held 100% coverage across all five categories throughout, with no custom rule work or emergency patch cycles in any month.



High-Profile Attacks Blocked

THREAT	SEVERITY / CVSS	EXPLOITATION
Microsoft SharePoint RCE Cluster `CVE-2026-50522 / -32201 / -58644`	Critical / 9.8	CISA KEV
Langflow AI-Agent RCE Chain `CVE-2025-3248 / CVE-2026-33017`	Critical / 9.8	CISA KEV
ColdFusion Path-Traversal RCE `CVE-2026-48282`	Critical / 10.0	CISA KEV
SonicWall SMA1000 SSRF Pair `CVE-2026-15409 / CVE-2026-15410`	Critical / 10.0	CISA KEV

Microsoft SharePoint: RCE cluster blocked ahead of the patch cycle

A group of related SharePoint Server RCE vulnerabilities (CVE-2026-50522, CVE-2026-32201, CVE-2026-58644, Critical, CVSS 9.8, CISA KEV) saw active exploitation following a public proof-of-concept release. AppTrana's Command Injection policy blocked all three, ahead of and independent of Microsoft's patch cycle.

Langflow: cryptomining, then ransomware on AI-agent endpoints

An unauthenticated remote-code-execution vulnerability in Langflow (CVE-2025-3248, later joined by CVE-2026-33017) was first exploited to deploy cryptomining malware on exposed AI-agent endpoints. The same operator later reused it to deliver a newly observed ransomware strain built to encrypt AI model weights, vector indexes, and training data. AppTrana blocked both root-cause CVEs by default before either wave of exploitation was observed.

ColdFusion: CVSS 10.0 path traversal, no custom signature

CVE-2026-48282, a Critical (CVSS 10.0) path-traversal vulnerability in ColdFusion, was added to CISA's KEV catalog after active exploitation was confirmed. AppTrana's default rule set closed this instance without a custom signature.

SonicWall SMA1000: linked SSRF-to-code-injection pair

A linked pair of zero-days in SonicWall's SMA1000 appliance (CVE-2026-15409, CVE-2026-15410, Critical, CVSS 10.0) combined server-side request forgery with code injection and was added to CISA KEV shortly after disclosure. Both were blocked automatically.

08 • COMPLETE COVERAGE

Every Vulnerability Blocked, by Category

Each of the 323 vulnerabilities blocked in July 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: 143 blocked · avg CVSS 8.7 · 30 CISA KEV				
CVE-2026-48558	Horizon3.ai Joins Anthropic's Project Glasswing to Help ...	Critical / 10	CISA KEV	✓ Blocked
CVE-2026-48282	ColdFusion versions 2025.9, 2023.20 and earlier are affe...	Critical / 10	CISA KEV	✓ Blocked
CVE-2026-15409	CVE-2026-15409 / CVE-2026-15410 | SonicWall SMA10...	Critical / 10	CISA KEV	✓ Blocked
CVE-2026-57624	Unauthenticated Remote Code Execution (RCE) in Blocks...	Critical / 10	CISA KEV	✓ Blocked
CVE-2026-49869	Kestra is an open-source, event-driven orchestration plat...	Critical / 10	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-53576	Kestra is an open-source, event-driven orchestration plat...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-48286	Adobe Campaign Classic (ACC) versions 7.4.3 build 9396...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-50746	A malicious actor with access to the network could exploi...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57572	Crawl4AI is an open-source LLM-friendly web crawler an...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15410	CVE-2026-15409 / CVE-2026-15410 | SonicWall SMA10...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34038	Coolify is an open-source and self-hostable tool for mana...	Critical / 9.9	PUBLIC EXPLOIT/POC	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 143 blocked · avg CVSS 8.7 · 30 CISA KEV (continued)				
CVE-2026-63030	Cloudflare WAF protects WordPress applications from tw...	Critical / 9.9	CISA KEV	✓ Blocked
CVE-2026-60137	Cloudflare WAF protects WordPress applications from tw...	Critical / 9.9	CISA KEV	✓ Blocked
CVE-2026-50195	containerd is an open-source container runtime.	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9559	Mautic vulnerable to Path Traversal via Campaign Import	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-1731	Agentless Threat Detection: Illuminating Cloud Blind Spots	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-14847	Agentless Threat Detection: Illuminating Cloud Blind Spots	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-33017	Langflow RCE Exploited to Deploy Monero Miner on Expo...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2026-5524	The Divi Form Builder plugin for WordPress is vulnerable ...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2026-50522	Microsoft SharePoint Remote Code Execution Vulnerability	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2026-32201	Critical SharePoint RCE CVE-2026-50522 Under Active ...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2026-56290	The Joomla extension Page Builder CK is vulnerable to an...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2022-50973	Yonyou KSOA 9.0 contains an unauthenticated arbitrary fi...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2024-14037	Redsea Cloud eHR contains an arbitrary file upload vulne...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2026-58644	Microsoft SharePoint Remote Code Execution Vulnerability	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2026-58116	LLaMA-Factory through 0.9.5 contains a remote code ex...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-58138	Orkes Conductor 3.21.21 before 3.30.2 contains an unaut...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-57517	Control Web Panel before 0.9.8.1225 contains a blind SQ...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-51947	An issue in Pivotal CRM 6.6.4.08 and systems using patc...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-58455	Dockwatch through 0.6.567 contains an unauthenticated ...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2025-3248	New ENCFORGE Ransomware Targets AI Model Files in L...	Critical / 9.8	CISA KEV	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 143 blocked · avg CVSS 8.7 · 30 CISA KEV (continued)				
CVE-2026-43867	Deserialization of Untrusted Data vulnerability in Apache ...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2018-11511	China-Nexus JadeProx Uses New TriBack Loader in Gove...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2026-56700	Grav CMS before 2.0.0-beta.2 contains multiple code-ex...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34106	Guardian language-system passes the id GET parameter ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34107	Guardian language-system passes the id GET parameter ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34108	Guardian language-system passes the id GET parameter ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34109	Guardian language-system passes the id GET parameter ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34110	Guardian language-system passes the id GET parameter ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34111	Guardian language-system passes the id GET parameter ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34112	Guardian language-system passes the id GET parameter ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34113	Guardian language-system passes the id GET parameter ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34114	Guardian language-system passes the id GET parameter ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34115	Guardian language-system passes the id GET parameter ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34116	Guardian language-system passes the id GET parameter ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34117	Guardian language-system passes the id GET parameter ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-58453	JAIOTlink C492A-W6 Wi-Fi IP cameras running firmware ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57621	Unauthenticated PHP Object Injection in Booktics <= 1.0....	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57677	Unauthenticated PHP Object Injection in Novalnet Payme...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14345	The WPFunnels – Funnel Builder for WooCommerce with ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2024-27198	Introducing Internal Network Scanning: see your network...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 143 blocked · avg CVSS 8.7 · 30 CISA KEV (continued)				
CVE-2021-24139	China-Nexus JadeProx Uses New TriBack Loader in Gove...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2021-31755	China-Nexus JadeProx Uses New TriBack Loader in Gove...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2021-32305	China-Nexus JadeProx Uses New TriBack Loader in Gove...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62379	OpenAM: Unauthenticated Remote Code Execution via Cl...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57571	Crawl4AI is an open-source LLM-friendly web crawler an...	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-6875	Security Affairs newsletter Round 587 by Pierluigi Pagani...	Critical / 9.5	CISA KEV	✓ Blocked
GHSA-G6G7-PVMX-M74P	9router: Missing Authorization and OS Command Injection	Critical / 9.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-16232	Check Point Patches Exploited SmartConsole Flaw Allowi...	Critical / 9.3	CISA KEV	✓ Blocked
CVE-2026-62144	Check Point Patches Exploited SmartConsole Flaw Allowi...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62145	Check Point Patches Exploited SmartConsole Flaw Allowi...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-37637	An issue in Alexantr filemanager v.1.0 allows a remote att...	Critical / 9.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-40047	Improper Neutralization of Argument Delimiters in a Com...	Critical / 9.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-9725	The Printcart Web to Print Product Designer for WooCom...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-6382	The FileOrganizer WordPress plugin before 1.1.9, Advanc...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-16723	Fastjson 1.x RCE Vulnerability Targeted in Attacks With N...	Critical / 9	CISA KEV	✓ Blocked
CVE-2026-43921	FOSSBilling is a free, open-source billing and client mana...	High / 8.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-33053	Exposed Server Reveals AI-Assisted Phishing Toolkit Beh...	High / 8.8	CISA KEV	✓ Blocked
CVE-2026-46590	Deserialization of Untrusted Data vulnerability in Apache ...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-13545	A vulnerability has been found in D-Link DCS-935L 1.10.01.	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57516	Ray prior to 2.56.0 contains an unsafe deserialization vul...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 143 blocked · avg CVSS 8.7 · 30 CISA KEV (continued)				
CVE-2026-40521	FrontAccounting before 2.4.20 contains a path traversal ...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-27957	Coolify is an open-source and self-hostable tool for mana...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-27060	Contributor PHP Object Injection in ARMember Premium ...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-27414	Contributor PHP Object Injection in Werkstatt <= 4.8.3 ve...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-11962	The FileOrganizer WordPress plugin before 1.2.0 does no...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34599	Coolify is an open-source and self-hostable tool for mana...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42153	Coolify is an open-source and self-hostable tool for mana...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42204	Coolify is an open-source and self-hostable tool for mana...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34057	Coolify is an open-source and self-hostable tool for mana...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34168	Coolify is an open-source and self-hostable tool for mana...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34158	Coolify is an open-source and self-hostable tool for mana...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54117	Microsoft SQL Server Remote Code Execution Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54118	Microsoft SQL Server Remote Code Execution Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-21513	Exposed Server Reveals AI-Assisted Phishing Toolkit Beh...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-24054	Exposed Server Reveals AI-Assisted Phishing Toolkit Beh...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
GHSA-G3HQ-HPHG-8FHH	Pheditor: Terminal command-allowlist bypass via argume...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55794	Craft CMS is a content management system (CMS).	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-53691	An Unrestricted File Upload vulnerability in Redeight CM...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14637	A security vulnerability has been detected in kirilkirkov E...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40859	Deserialization of Untrusted Data vulnerability in Apache ...	High / 8.1	PUBLIC EXPLOIT/POC	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 143 blocked · avg CVSS 8.7 · 30 CISA KEV (continued)				
CVE-2026-43865	Deserialization of Untrusted Data vulnerability in Apache ...	High / 8.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-10818	WPForms Pro <= 1.10.1.1 - Unauthenticated Arbitrary File ...	High / 8.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-56264	Crawl4AI before 0.8.7 contains an arbitrary JavaScript ex...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-7311	The TinyPNG – JPEG, PNG & WebP image compression p...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12240	The Export User Data plugin for WordPress is vulnerable ...	High / 8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-35425	Azure API Management (APIM) Remote Code Execution V...	High / 8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-8933	The AI Trust Paradox: Businesses Are Racing Ahead, but ...	High / 7.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-3888	Ubuntu snap-confine Flaw Could Give Local Users Root o...	High / 7.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2021-44731	Ubuntu snap-confine Flaw Could Give Local Users Root o...	High / 7.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2022-3328	Ubuntu snap-confine Flaw Could Give Local Users Root o...	High / 7.8	NO KNOWN EXPLOIT	✓ Blocked
GHSA-PVCR-8MVP-W8QR	Budibase: Chat-Link Handoff Identity Confusion (Same-T...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2024-58352	Landray OA contains an unauthenticated HQL injection v...	High / 7.5	CISA KEV	✓ Blocked
CVE-2026-58169	Vibe-Trading before 0.1.10 contains a DNS rebinding auth...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13759	IBM WebSphere Extreme Scale 8.6.1.0 through 8.6.1.6 shi...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49353	9router has an Incomplete Fix: Local-Only Access Gate B...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-43866	Deserialization of Untrusted Data vulnerability in Apache ...	High / 7.3	PUBLIC EXPLOIT/POC	✓ Blocked
ZD-F9D690C27D8DD66A	A project is publishing full analyses of AI-discovered 0-d...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14749	A vulnerability was identified in mjperpinosa stumasy up t...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-43825	Untrusted Java Deserialization in Apache OpenNLP Svm...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9834	The WP Database Backup – Unlimited Database & Files B...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 143 blocked · avg CVSS 8.7 · 30 CISA KEV (continued)				
CVE-2026-65693	Microweber CMS 2.0.20 Server-Side Template Injection v...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-65711	sysPass 3.2.11 Authenticated OS Command Injection via ...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-27955	Coolify is an open-source and self-hostable tool for mana...	Medium / 6.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55223	c3p0 is a JDBC Connection pooling library.	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14691	A security vulnerability has been detected in SourceCode...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13773	IBM WebSphere Extreme Scale 8.6.1.0 through 8.6.1.6 Ap...	Medium / 6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-60167	CVE-2026-15409 / CVE-2026-15410 | SonicWall SMA10...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-60168	CVE-2026-15409 / CVE-2026-15410 | SonicWall SMA10...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-60169	CVE-2026-15409 / CVE-2026-15410 | SonicWall SMA10...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-60170	CVE-2026-15409 / CVE-2026-15410 | SonicWall SMA10...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-58057	Flowise before 3.1.3 validates Custom MCP stdio environ...	Medium / 5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-14633	A vulnerability was determined in kirilkirkov Ecommerce-...	Medium / 4.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42201	Coolify is an open-source and self-hostable tool for mana...	Low / 3.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-10591	ICYMI: June 2026 @AWS Security	Low / 3.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-40947	Three Steps to the Terminal: A Siemens ROX II Zero-Day ...	Low / 3.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-41940	Attackers Weaponize GitHub Actions Runners to Target c...	Unknown	CISA KEV	✓ Blocked
CVE-2024-25600	[webapps] WordPress Bricks Builder Theme - RCE	Unknown	CISA KEV	✓ Blocked
CVE-2023-26360	Defence Impairment Olympics	Unknown	CISA KEV	✓ Blocked
CVE-2026-53913	Improper Authentication, Missing Authentication for Criti...	Unknown	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2024-42009	Suspected Chinese Threat Group Targets Universities vi...	Unknown	CISA KEV	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 143 blocked · avg CVSS 8.7 · 30 CISA KEV (continued)				
CVE-2026-34197	Horizon3.ai Joins Anthropic's Project Glasswing to Help ...	Unknown	CISA KEV	✓ Blocked
CVE-2026-25089	CISA Adds Three Known Exploited Vulnerabilities to Catal...	Unknown	CISA KEV	✓ Blocked
CVE-2026-39808	CISA Adds Three Known Exploited Vulnerabilities to Catal...	Unknown	CISA KEV	✓ Blocked
CVE-2024-6587	ChatGPT AgentForger Flaw Could Deploy Rogue Worksp...	Unknown	CISA KEV	✓ Blocked
ZD-7BAAC3CBEB6C86AB	CISA: Microsoft SharePoint RCE flaw now actively exploit...	Unknown	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-25592	Open-Source Android AI Agents Could Let Invisible Scre...	Unknown	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-50055	Zimbra Patches Critical SNMP Command Injection and Fo...	Unknown	NO KNOWN EXPLOIT	✓ Blocked
ZD-3601310EFCED7903	Tycoon2FA takedown reshapes the phishing landscape	Unknown	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32194	Bing Images Flaws Let Crafted SVGs Run Commands as S...	Unknown	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32191	Bing Images Flaws Let Crafted SVGs Run Commands as S...	Unknown	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-40217	ChatGPT AgentForger Flaw Could Deploy Rogue Worksp...	Unknown	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-35029	ChatGPT AgentForger Flaw Could Deploy Rogue Worksp...	Unknown	NO KNOWN EXPLOIT	✓ Blocked
SQL Injection: 70 blocked · avg CVSS 7.8 · 0 CISA KEV				
CVE-2026-54350	Budibase is an open-source low-code platform.	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49048	The Joomla extension JoomCCK exposes a front-end co...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-9711	The EventON - WordPress Virtual Event Calendar Plugin ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34099	Guardian language-system passes the id GET parameter ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34100	Guardian language-system passes the id GET parameter ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34101	Guardian language-system passes the id GET parameter ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 70 blocked · avg CVSS 7.8 · 0 CISA KEV (continued)				
CVE-2026-34102	Guardian language-system passes the id GET parameter ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34103	Guardian language-system passes the id GET parameter ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34104	Guardian language-system passes the name GET parame...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34105	Guardian language-system passes the id GET parameter ...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
GHSA-Q6X4-V3QX-85QW	Budibase: SQL Injection via `multipleStatements: true`	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12076	Raytha CMS is vulnerable to SQL Injection within the ODa...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-53690	An SQL Injection vulnerability exists in Redeight CMS ver...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-47295	Microsoft SQL Server Elevation of Privilege Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-11590	The WP Support Plus Responsive Ticket System WordPr...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-58376	Dolibarr through 23.0.3, fixed in commit 14db36e, contai...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
GHSA-2XGG-R2WC-C5R2	Budibase: MySQL DESCRIBE Backtick Injection via multip...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-11823	The BookingPress Appointment Booking Pro plugin for W...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-8441	The WP Review Slider Pro plugin for WordPress is vulner...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14762	A vulnerability was detected in code-projects Hotel and T...	High / 7.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-13485	A vulnerability was found in SourceCodester Class and E...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13486	A vulnerability was determined in SourceCodester Class ...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13487	A vulnerability was identified in SourceCodester Class an...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13488	A security flaw has been discovered in SourceCodester C...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13498	A vulnerability was identified in yashpokharna2555 resta...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13521	A vulnerability was identified in SourceCodester Class an...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 70 blocked · avg CVSS 7.8 · 0 CISA KEV (continued)				
CVE-2026-13526	A flaw has been found in SourceCodester Class and Exam...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13527	A vulnerability has been found in SourceCodester Class a...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13550	A weakness has been identified in itsourcecode Baptism I...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13551	A security vulnerability has been detected in itsourcecod...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13552	A vulnerability was detected in itsourcecode Online Hotel...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13555	A vulnerability was found in itsourcecode Online Hotel M...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13559	A weakness has been identified in code-projects Real Sta...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13565	A vulnerability was determined in SourceCodester Class ...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13566	A vulnerability was identified in SourceCodester Class an...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14640	A vulnerability was found in CodeAstro Apartment Visitor ...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14641	A vulnerability was determined in SourceCodester Class ...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14642	A vulnerability was identified in SourceCodester Class an...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14648	A security vulnerability has been detected in code-projec...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14649	A vulnerability was detected in code-projects Online Voti...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14652	A vulnerability was found in SourceCodester Simple and ...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14653	A vulnerability was determined in SourceCodester Simpl...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14654	A vulnerability was identified in SourceCodester Simple a...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14660	A vulnerability was found in code-projects Online Job Por...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14688	A vulnerability was identified in itsourcecode Online Hote...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14695	A vulnerability was found in SourceCodester Multi-Vendo...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 70 blocked · avg CVSS 7.8 · 0 CISA KEV (continued)				
CVE-2026-14700	A security vulnerability has been detected in code-projec...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14705	A vulnerability was determined in code-projects Online E...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14713	A security flaw has been discovered in SourceCodester P...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14732	A security vulnerability has been detected in SourceCode...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14733	A vulnerability was detected in SourceCodester Class an...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14734	A flaw has been found in SourceCodester Class and Exam...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14735	A vulnerability has been found in code-projects Smart Pa...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14743	A vulnerability was identified in code-projects Real State ...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14744	A security flaw has been discovered in code-projects Rea...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14745	A weakness has been identified in code-projects Real Sta...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14746	A security vulnerability has been detected in code-projec...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14747	A vulnerability was detected in code-projects Real State ...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14750	A security flaw has been discovered in mjperpinosa stum...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14754	A flaw has been found in code-projects Hotel and Touris...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14755	A vulnerability has been found in code-projects Hotel and...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14756	A vulnerability was found in code-projects Hotel and Tour...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14763	A flaw has been found in code-projects Hotel and Touris...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14764	A vulnerability has been found in code-projects Hotel and...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14768	A weakness has been identified in code-projects Real Sta...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14769	A security vulnerability has been detected in code-projec...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 70 blocked · avg CVSS 7.8 · 0 CISA KEV (continued)				
CVE-2026-14770	A vulnerability was detected in SourceCodester Class an...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14771	A flaw has been found in SourceCodester Class and Exam...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14772	A vulnerability has been found in SourceCodester Class a...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-60188	[webapps] Atarim WordPress Plugin 4.2.2 - Sensitive Info...	Unknown	PUBLIC EXPLOIT/POC	✓ Blocked
Path Traversal: 27 blocked · avg CVSS 7.5 · 0 CISA KEV				
CVE-2026-54352	Budibase is an open-source low-code platform.	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-6070	The WP-BusinessDirectory plugin for WordPress is vulne...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-47896	Improper Limitation of a Pathname to a Restricted Direct...	High / 8.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-47897	Improper Limitation of a Pathname to a Restricted Direct...	High / 8.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42200	Coolify is an open-source and self-hostable tool for mana...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-64400	ksmbd: prevent path traversal bypass by restricting casel...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56876	extract-zip does not validate symlink targets when extrac...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49297	Apache Airflow's Google provider operators `GCSToSFT...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-45807	Kestra is an open-source, event-driven orchestration plat...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49984	Kestra is an open-source, event-driven orchestration plat...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14468	HashiCorp Terraform Enterprise contained an issue in its ...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-36848	Gigamon GVOS v5.16.1 and below is vulnerable to Directo...	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-8023	Zephyr's HTTP server (subsys/net/lib/http) provides a sta...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12243	NLTK version 3.9.4 is vulnerable to a path traversal attack...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Path Traversal: 27 blocked · avg CVSS 7.5 · 0 CISA KEV (continued)				
CVE-2026-13251	The Perfmatters plugin for WordPress is vulnerable to Dir...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13369	The Ninja Forms - File Uploads plugin for WordPress is v...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-58467	Cockpit CMS before release 364 contains a path traversa...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14327	The AR for WordPress plugin for WordPress is vulnerable ...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14352	The AR for WooCommerce plugin for WordPress is vulner...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14635	A security flaw has been discovered in kirilkirkov Ecomm...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-58451	Horde IMP before 7.0.1 contains a path traversal vulnerabi...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9145	The Database for Contact Form 7, WPforms, Elementor fo...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66007	Datasets Path Traversal via Unsanitized file_name Metad...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14955	Checkout Field Editor for WooCommerce (Pro) <= 3.7.7 - ...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-58015	A flaw was found in GLib.	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14628	A vulnerability was detected in NousResearch hermes-ag...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66004	BlenderMCP Path Traversal via download_polyhaven_ass...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
Cross-Site Scripting: 31 blocked · avg CVSS 6.9 · 3 CISA KEV				
CVE-2026-55008	Microsoft Exchange Server Spoofing Vulnerability	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-11708	IBM WebSphere Application Server 9.0, and 8.5 is affecte...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-11712	IBM WebSphere Application Server 9.0, and 8.5 is affecte...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-11589	The WP Support Plus Responsive Ticket System WordPr...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
GHSA-FP43-VJ7G-PG92	OmniFaces: Forged combined-resource IDs and related o...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 31 blocked · avg CVSS 6.9 · 3 CISA KEV (continued)				
CVE-2026-13731	The WPBot – AI ChatBot for Live Support, Lead Generatio...	High / 7.2	CISA KEV	✓ Blocked
CVE-2026-8141	The Ajax Load More - Filters plugin for WordPress is vuln...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-10513	The Webmention plugin for WordPress is vulnerable to St...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-7517	The Custom Payment Gateways for WooCommerce plugi...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12142	The NEX-Forms – Ultimate Forms Plugin for WordPress p...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13040	The NEX-Forms – Ultimate Forms Plugin for WordPress p...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9148	The Comments – wpDiscuz plugin for WordPress is vulne...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-56011	Unauthenticated Cross Site Scripting (XSS) in MapPress ...	High / 7.1	CISA KEV	✓ Blocked
CVE-2025-69152	Unauthenticated Cross Site Scripting (XSS) in Artale | We...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-69154	Unauthenticated Cross Site Scripting (XSS) in SpaLab | B...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-69155	Unauthenticated Cross Site Scripting (XSS) in Fitness Zo...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-69156	Unauthenticated Cross Site Scripting (XSS) in Kids Zone ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-27402	Unauthenticated Cross Site Scripting (XSS) in Kids Life | ...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9107	The Kali Forms — Contact Form & Drag-and-Drop Builder...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-9626	The JSON API User plugin for WordPress is vulnerable to ...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-4804	The Zakra theme for WordPress is vulnerable to Stored C...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15425	Yoast SEO <= 28.0 - Authenticated (Author+) Stored Cro...	Medium / 6.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-50765	A stored cross-site scripting (XSS) vulnerability in the pa...	Medium / 6.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-62280	OpenAM Reflected XSS in the OAuth2/OIDC `wap` conse...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55793	Craft CMS is a content management system (CMS).	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 31 blocked · avg CVSS 6.9 · 3 CISA KEV (continued)				
CVE-2026-50766	A stored cross-site scripting (XSS) vulnerability in the OP...	Medium / 5.4	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-50767	A stored cross-site scripting (XSS) vulnerability in the ite...	Medium / 5.4	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-54477	The admin panel lacks standard security headers, enablin...	Medium / 5.4	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-13323	In Open VSX Registry before 1.0.2, the /vscode/unpkg/ en...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-10104	The Product Video Gallery for Woocommerce plugin for ...	Medium / 4.4	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2025-27915	Critical Zimbra security update fixes 9 vulnerabilities	Unknown	CISA KEV	✓ Blocked
SSRF: 24 blocked · avg CVSS 7.9 · 0 CISA KEV				
CVE-2026-45499	Server-side request forgery (ssrf) in Azure OpenAI allow...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-22874	Gitea versions up to and including 1.26.2 have incomplet...	Critical / 9.6	PUBLIC EXPLOIT/POC	✓ Blocked
GHSA-68R5-9HPG-7QW9	OpenDJ unauthenticated SSRF, local file read and unbou...	Critical / 9.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-48205	Improper Input Validation, Server-Side Request Forgery (...	Critical / 9.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-48203	Improper Neutralization of Special Elements in Output Us...	Critical / 9.1	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-13603	The payment integration pretix-oppwa provides support ...	Critical / 9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57573	Crawl4AI is an open-source LLM-friendly web crawler an...	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54353	Budibase is an open-source low-code platform.	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-10129	IBM Langflow OSS 1.0.0 through 1.9.3 contains a Server-...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-11714	IBM WebSphere Application Server - Liberty 17.0.0.3 thro...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
GHSA-XG5G-26X8-CVF4	Budibase: DNS rebinding SSRF bypasses remain in Open...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
GHSA-V42F-V8XC-J435	Budibase: SSRF via DNS rebinding in the REST datasourc...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 24 blocked · avg CVSS 7.9 · 0 CISA KEV (continued)				
CVE-2026-44937	Potential forgery of webhook requests when using a unau...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14336	PIA's OIDC issuer allowlist for Jenkins tokens uses a bare ...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54640	OpenRemote has an incomplete fix for CVE-2026-40882...	High / 7.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55994	Improper Input Validation, Exposure of Sensitive Informat...	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-46726	Improper Input Validation, Exposure of Sensitive Informat...	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-55113	A malicious actor with access to the network could exploi...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
GHSA-PPR4-5F46-J9C6	Budibase: Server Filesystem Existence/Read Oracle via B...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55051	Microsoft SharePoint Server Information Disclosure Vuln...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
GHSA-8Q49-2H5H-434X	FrontMCP: Server-Side Request Forgery (SSRF) in the O...	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54430	liboauth2 is vulnerable to Server-Side Request Forgery in...	Medium / 5.8	NO KNOWN EXPLOIT	✓ Blocked
GHSA-V6W6-358X-2433	Cloudreve Admin.Read OAuth tokens can trigger server-...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-28385	In Canonical LXD versions 4.12 through 6.9, a Server-Sid...	Medium / 5	NO KNOWN EXPLOIT	✓ Blocked
Injection (General): 12 blocked · avg CVSS 7.8 · 0 CISA KEV				
CVE-2026-48204	Improper Input Validation, Improper Access Control vuln...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-13762	Inconsistent interpretation of HTTP/2 requests in Amazo...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13763	Inconsistent interpretation of HTTP/2 requests in AWS A...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
GHSA-QW6M-8FW2-2V64	Budibase: NoSQL Injection via JSON Parameter Interpola...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-46591	Improper Neutralization of Special Elements in Data Quer...	High / 8.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-48743	Envoy is an open source edge and service proxy designe...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Injection (General): 12 blocked · avg CVSS 7.8 · 0 CISA KEV (continued)				
CVE-2026-11541	IBM WebSphere Application Server 9.0, and 8.5 and IBM ...	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
GHSA-MHVJ-JHPQ-885V	blaze: Multiple HTTP/1.1 request-smuggling primitives in ...	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
GHSA-46Q4-43PH-C6FR	blaze: Chunked-body trailer fields promoted into Reques...	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
GHSA-PMPG-2MXQ-6XWR	Budibase: NoSQL injection in MongoDB integration: colle...	High / 7.1	NO KNOWN EXPLOIT	✓ Blocked
GHSA-3R53-75J5-3G7J	Quasar: Prototype pollution in the extend() utility	Medium / 5.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-58055	nghttp2's nghttpx proxy through 1.69.0 forwards an HTT...	Medium / 5.4	NO KNOWN EXPLOIT	✓ Blocked
Insecure Design (File-Upload Pattern): 9 blocked · avg CVSS 7.3 · 0 CISA KEV				
CVE-2026-24014	Apache IoTDB DataNode's internal RPC interface for crea...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-47303	ASP.NET Core Elevation of Privilege Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13547	A vulnerability was determined in Hanwang e-Face Gener...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-13553	A flaw has been found in itsourcecode Online Hotel Mana...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14736	A vulnerability was found in Ruijie RG-UAC up to 1.0-R1.8....	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14698	A security flaw has been discovered in SourceCodester S...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14775	A vulnerability was identified in SourceCodester Onlne Ex...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14776	A security flaw has been discovered in SourceCodester O...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-14777	A weakness has been identified in SourceCodester Onlne...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
Uncontrolled Resource Consumption: 6 blocked · avg CVSS 6.7 · 0 CISA KEV				
CVE-2026-5821	The Image Optimizer plugin for WordPress is vulnerable t...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Uncontrolled Resource Consumption: 6 blocked · avg CVSS 6.7 · 0 CISA KEV (continued)				
CVE-2026-9165	A flaw was found in Red Hat Advanced Cluster Security f...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-44907	react-server-dom: Denial of Service in Server Functions	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-55497	Cloudreve: Denial of Service - Image decompression / pix...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
GHSA-CR7P-CR3Q-H5CM	Budibase: Account Enumeration via Login Lockout Respo...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
GHSA-JPCW-4WR7-C3VQ	kin-openapi openapi3filter: unauthenticated nil-pointer p...	Medium / 5.3	NO KNOWN EXPLOIT	✓ Blocked
XML Injection: 1 blocked · avg CVSS 7.5 · 0 CISA KEV				
CVE-2026-48042	Envoy is an open source edge and service proxy designe...	High / 7.5	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