INDUSFACE™

ZERO-DAY VULNERABILITY REPORT

• MONTHLY BULLETIN · AUGUST 2026

Zero-Day Vulnerability Coverage Report

August 2026: 204 zero-day attacks detected across AppTrana-protected traffic. All were autonomously blocked, with no manual intervention and no exposure window.

204	100%	13	35
ZERO-DAYS BLOCKED	CATEGORY COVERAGE	CISA KEV BLOCKED	AGENTIC AI / LLM BLOCKED

CONTENTS

In this Report

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

RESEARCH BASIS

Real enforcement data, August 2026. Each vulnerability ties to a CVE, a blocking rule, and a scanner check

Zero-Day Exposure Window: 0 Days

AppTrana's default rule set blocked 204 vulnerabilities in August 2026, with 100% coverage and no manual tuning required. The window between disclosure and protection, the window where exposure usually lives, stayed closed.

204

BLOCKED BY DEFAULT

AppTrana blocked 204 vulnerabilities by default, with 100% coverage across Command Injection, Cross-Site Scripting, SSRF, SQL Injection, Path Traversal, Injection, Uncontrolled Resource Consumption, and the file-upload pattern of Insecure Design.

13

CISA KEV CLOSED

CISA confirmed 13 of these vulnerabilities as actively exploited, twelve of them in a Command Injection cluster linked to Metabase, JetBrains TeamCity, VMware vCenter, Elementor Pro, and Microsoft SharePoint Server.

Day zero

PUBLIC EXPLOIT CLOSED

A public proof-of-concept for the Metabase password-reset SQL injection (CVE-2026-72898, CVSS 10.0) circulated while the CVE sat on CISA's KEV catalog. AppTrana blocked it on default rules, with no signature work and no patch dependency.

35

AGENTIC AI & LLM CLOSED

AppTrana autonomously blocked 35 AI/LLM-related CVEs identified in August 2026, spanning prompt injection, RAG data exposure, and agent-to-tool trust boundary violations

Coverage by Category

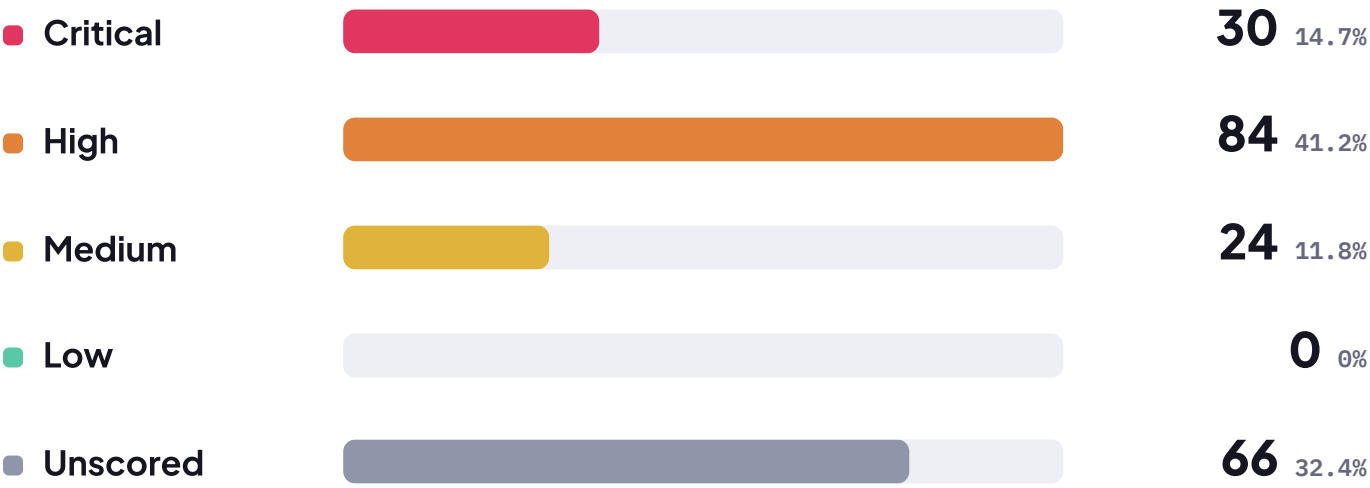
Command Injection again drew the heaviest attacker traffic, and AppTrana blocked all 138 attempts, including the Critical-severity Metabase, TeamCity, and vCenter disclosures covered in Section 07. Coverage stayed at 100% across every category.

CATEGORY	BLOCKED	CRITICAL	HIGH	AVG CVSS	PEAK
Command Injection	138	18	60	8.3	10.0
Cross-Site Scripting	23	2	11	7.1	9.6
SSRF	17	3	9	7.9	10.0
SQL Injection	11	4	1	9.4	9.9
Path Traversal	7	3	1	8.9	9.9
Injection	5	0	0	5.5	5.9
Uncontrolled Resource Consumption	2	0	1	8.1	8.1
Insecure Design (File-Upload)	1	0	1	7.2	7.2

Severity Snapshot

Severity didn't change the outcome. 114 of the 204 blocked vulnerabilities (55.9%) were Critical or High, the tier that usually triggers emergency patching. All were blocked at the edge automatically. It worked without needing an emergency patch, an out-of-band change, or any manual fix. A further 66 (32.4%) had no published CVSS score yet and were still blocked, on the same default rules.

BREAKDOWN BY SEVERITY



114

CRITICAL + HIGH SEVERITY

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

04 • REAL-WORLD RISK

Exploitation & KEV Status

Of the 204 vulnerabilities blocked, 13 were already confirmed by CISA as actively exploited and listed in the Known Exploited Vulnerabilities (KEV) catalog (6.4%).

13

CISA KEV · ACTIVELY EXPLOITED

6.4%

7

PUBLIC EXPLOIT / POC AVAILABLE

3.4%

NOTABLE CISA KEV ENTRIES BLOCKED

CVE	SEVERITY / CVSS	CATEGORY
CVE-2026-72898	Critical / 10.0	Command Injection
CVE-2026-63077	Critical / 9.8	Command Injection
CVE-2026-59310	Critical / 9.8	Command Injection
CVE-2024-10914	Critical / 9.8	Command Injection
CVE-2026-32475	Critical / 9.0	Command Injection
CVE-2026-63520	High / 8.1	Command Injection

05 • EMERGING RISK

Agentic AI & LLM Risk Coverage

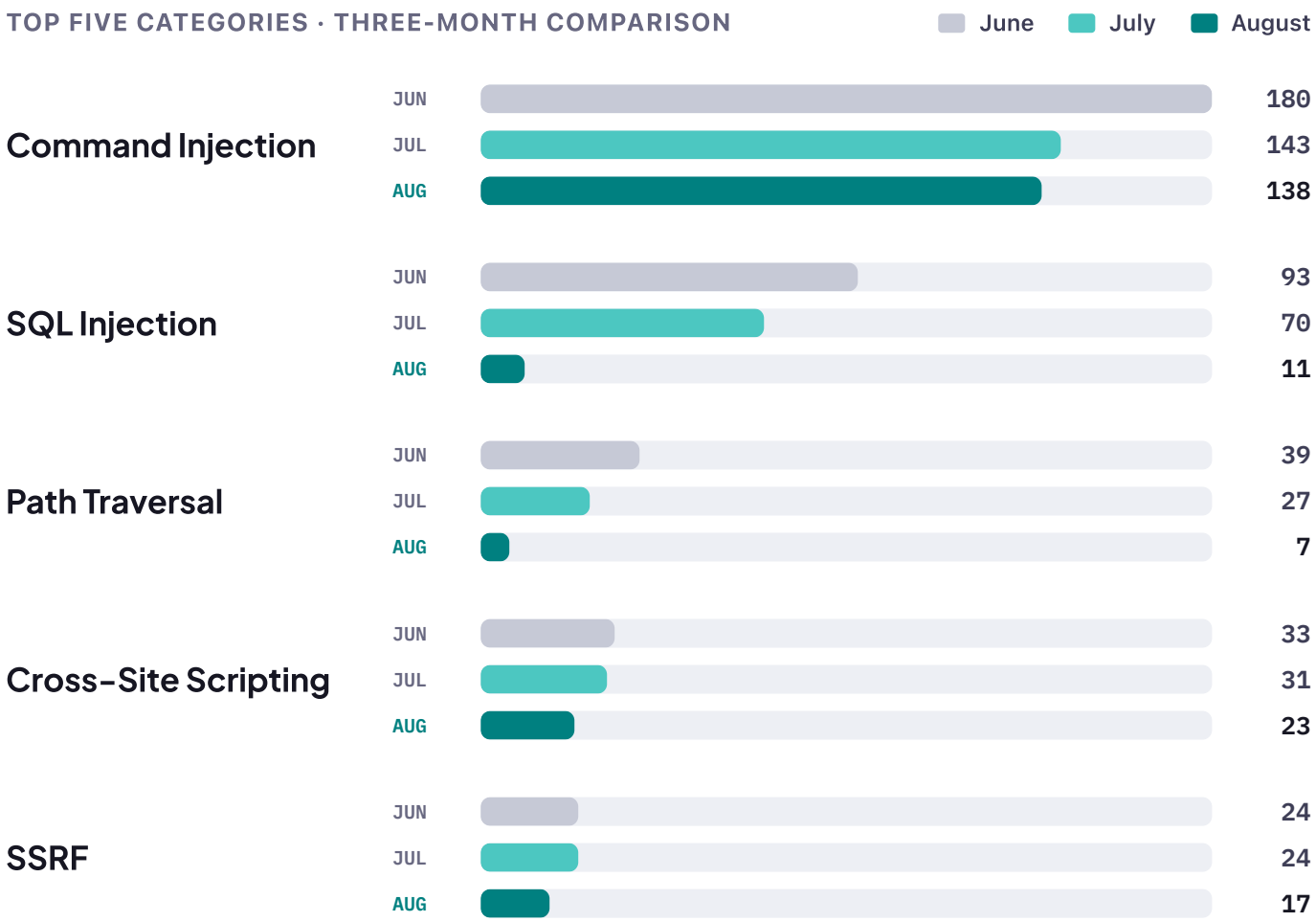
Agentic AI and LLM systems carry a distinct exposure surface: prompt injection, insecure agent-to-tool trust boundaries, and exposed RAG data sources. AppTrana automatically blocked 35 AI/LLM-tagged CVEs in August 2026, averaging CVSS 9.5, the highest severity of any category in this report.

35	6	9.5	10.0
BLOCKED AUTOMATICALLY	CRITICAL SEVERITY	AVG CVSS (BLOCKED)	PEAK CVSS

THREAT TAG	CVES	WHAT IT COVERS
Agent-Framework Risk	29	Autonomous-agent frameworks and trust boundaries
General LLM Application Risk	19	LLM application code and integrations
Prompt-Injection Vectors	2	Direct or indirect prompt-injection paths
RAG Data Exposure	1	RAG pipelines and connected data sources

Vulnerability Trend

Command Injection remained the dominant category, holding near its June peak at 138. SQL Injection fell sharply, from 70 in July to 11, and Path Traversal dropped to 7. Cross-Site Scripting and SSRF both declined as well. Across all five categories, AppTrana held 100% coverage every month, with no custom rule work and no emergency patch cycles.



High-Profile Attacks Blocked

THREAT	SEVERITY / CVSS	EXPLOITATION
Metabase Password-Reset SQL Injection CVE-2026-72898	Critical / 10.0	CISA KEV
JetBrains TeamCity RCE CVE-2026-63077	Critical / 9.8	CISA KEV
VMware vCenter RCE CVE-2026-59310	Critical / 9.8	CISA KEV
Elementor Pro File-Upload RCE CVE-2026-32475	Critical / 9.0	CISA KEV
Microsoft SharePoint Server RCE CVE-2026-63520	High / 8.1	CISA KEV

Metabase: password-reset injection at CVSS 10.0

CVE-2026-72898, a Critical SQL injection reachable through Metabase's password-reset flow, was confirmed as actively exploited and carried a 12% EPSS exploitation probability. The default rule set closed it without a custom signature.

JetBrains TeamCity: unpatched instance used to extract AWS credentials

Attackers breached JetBrains Cadence through an unpatched TeamCity server (CVE-2026-63077, Critical, CVSS 9.8) and extracted AWS credentials. A Metasploit module is public. AppTrana blocked the request pattern by default.

VMware vCenter: exploited five days after disclosure

CVE-2026-59310 (Critical, CVSS 9.8) moved from disclosure to confirmed in-the-wild exploitation in five days. Coverage was already in place, so the compressed window left no exposure gap.

Elementor Pro: unauthenticated file upload to RCE

CVE-2026-32475 (Critical, CVSS 9.0) allowed unauthenticated file upload leading to remote code execution in Elementor Pro, with active exploitation across WordPress estates. AppTrana blocked the upload path on default rules.

Microsoft SharePoint Server: KEV-listed RCE with a public PoC

A remote-code-execution vulnerability in Microsoft SharePoint Server (CVE-2026-63520, High, CVSS 8.1) is listed on CISA's KEV catalog and has a proof-of-concept published on GitHub. The exploitation path runs over ordinary HTTP requests to the SharePoint web front end, and AppTrana's Command Injection policy blocked it by default, independent of the patch cycle.

Blocked Vulnerabilities by Category

Each of the 204 vulnerabilities blocked in August 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: 138 blocked · avg CVSS 8.3 · 12 CISA KEV				
CVE-2026-18556	N-able Issues Fourth N-central Hotfix in Five Weeks for U...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-72898	Critical SQL Injection in Metabase via Password Reset: C...	Critical / 10	CISA KEV	✓ Blocked
CVE-2026-14682	Security Bulletin - August 18 2026 — Bamboo Data Cente...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-65770	Azure Managed Instance for Apache Cassandra Remote ...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69836	Microsoft Entra ID Remote Code Execution Vulnerability	Critical / 10	CISA KEV	✓ Blocked
CVE-2026-50515	Azure Service Bus Remote Code Execution Vulnerability	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-28220	ZDI-26-528: Wazuh Cluster DAPI Protocol Deserializatio...	Critical / 9.9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-44901	ZDI-26-527: Wazuh Cluster DAPI Protocol Deserializatio...	Critical / 9.9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-18265	ZDI-26-480: OSNEXUS QuantaStor Missing Authenticati...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-63077	Attackers Breached JetBrains Cadence via Unpatched Te...	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2026-69264	ZDI-26-546: Flowise Airtable_Agent Code Injection Rem...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 138 blocked · avg CVSS 8.3 · 12 CISA KEV (continued)				
CVE-2026-59124	Microsoft High Performance Computing (HPC) Pack Rem...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59310	vCenter Flaw Exploited Just Five Days After Disclosure	Critical / 9.8	CISA KEV	✓ Blocked
CVE-2024-10914	[remote] D-Link DNS_340L - OS Command Injection	Critical / 9.8	CISA KEV	✓ Blocked
ZD-07EE7EAC404A9C43	Australia Warns of Active Exploitation of Critical TeamCit...	Critical / 9.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2023-45133	Security Bulletin - August 18 2026 — Arbitrary code exec...	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-68823	Azure Confidential Ledger Remote Code Execution Vulne...	Critical / 9.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-32475	Critical Unauthenticated File Upload to RCE in Elementor ...	Critical / 9	CISA KEV	✓ Blocked
CVE-2026-15962	Fluent Forms Pro Add On Pack <= 6.2.6 - Authenticated (...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-44827	Bugs in Hugging Face Diffusers Bypass Custom Code Saf...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-45804	Bugs in Hugging Face Diffusers Bypass Custom Code Saf...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-44513	Bugs in Hugging Face Diffusers Bypass Custom Code Saf...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59689	ZDI-26-482: Progress Software Kemp LoadMaster enabl...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-18264	ZDI-26-483: NoMachine getstat Command Injection Re...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-69256	ZDI-26-545: Flowise CSV_Agent customReadCSV Code I...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-65665	Microsoft SharePoint Server Remote Code Execution Vul...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63514	Microsoft SharePoint Server Remote Code Execution Vul...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-64901	Microsoft SharePoint Server Remote Code Execution Vul...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-65658	Microsoft SharePoint Server Remote Code Execution Vul...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-65660	Microsoft SharePoint Server Remote Code Execution Vul...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-65663	Microsoft SharePoint Server Remote Code Execution Vul...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 138 blocked · avg CVSS 8.3 · 12 CISA KEV (continued)				
CVE-2026-66805	Microsoft SharePoint Server Remote Code Execution Vul...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66808	Microsoft SharePoint Server Remote Code Execution Vul...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70321	Microsoft SharePoint Remote Code Execution Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-65815	Microsoft Dynamics 365 On-Premises Remote Code Exe...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59113	Visual Studio Code Remote Code Execution Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-65768	Microsoft Teams Remote Code Execution Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70337	Microsoft PowerShell Remote Code Execution Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49179	Windows Active Directory Domain Services Remote Cod...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-65811	Power BI Remote Code Execution Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69320	Visual Studio Code Remote Code Execution Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70329	Microsoft Outlook Remote Code Execution Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70336	Visual Studio Code Remote Code Execution Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-24301	Microsoft Copilot Information Disclosure Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-58060	Security Bulletin - August 18 2026 — RCE (Remote Code ...	High / 8.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69419	Azure Data Manager for Energy Remote Code Execution ...	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-17497	NoteGen arbitrary OS command execution via Tauri shell:...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63520	Microsoft SharePoint Server Remote Code Execution Vul...	High / 8.1	CISA KEV	✓ Blocked
CVE-2026-41907	Security Bulletin - August 18 2026 — RCE (Remote Code ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18309	ZDI-26-462: GIMP APNG File Parsing Integer Overflow R...	High / 7.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-18308	ZDI-26-461: GIMP TIF File Parsing Integer Overflow Rem...	High / 7.8	PUBLIC EXPLOIT/POC	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 138 blocked · avg CVSS 8.3 · 12 CISA KEV (continued)				
CVE-2026-18306	ZDI-26-459: GIMP SGI File Parsing Integer Overflow Re...	High / 7.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-18305	ZDI-26-458: GIMP TIF File Parsing Integer Overflow Rem...	High / 7.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-18304	ZDI-26-457: GIMP TIF File Parsing Integer Overflow Rem...	High / 7.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-18301	ZDI-26-454: GIMP PSD File Parsing Integer Overflow Re...	High / 7.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-18300	ZDI-26-453: GIMP HDR File Parsing Integer Overflow Re...	High / 7.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-43780	ZDI-26-492: Apple macOS ImageIO Numeric Truncation ...	High / 7.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-18287	ZDI-26-470: Aeon load_time_series_segmentation_ben...	High / 7.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-18286	ZDI-26-469: Aeon load_human_activity_segmentation_...	High / 7.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-18285	ZDI-26-468: Aeon load_rehab_pile_dataset Deserializati...	High / 7.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-15679	ZDI-26-523: Hugging Face PyTorch Image Models check...	High / 7.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-24232	ZDI-26-564: NVIDIA Transformers4Rec load_model_trai...	High / 7.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-24238	ZDI-26-592: NVIDIA TensorRT ONNX File Parsing Impro...	High / 7.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-63720	datamodel-code-generator Code Injection via Unvalidate...	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-44103	ZDI-26-520: (Pwn2Own) Phoenix Contact CHARX SEC-...	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-44099	ZDI-26-519: (Pwn2Own) Phoenix Contact CHARX SEC-3...	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-44104	ZDI-26-510: (Pwn2Own) Phoenix Contact CHARX SEC-3...	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-7849	ZDI-26-504: (Pwn2Own) Phoenix Contact CHARX SEC-...	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-19909	ZDI-26-525: (0Day) PAX Technology Q80 AIP File Parsin...	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-61352	Remote Desktop Client Remote Code Execution Vulnerab...	High / 7.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-19910	ZDI-26-526: (0Day) PAX Technology Q80 Application In...	High / 7.5	PUBLIC EXPLOIT/POC	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 138 blocked · avg CVSS 8.3 · 12 CISA KEV (continued)				
CVE-2026-44387	Multiple vulnerabilities in ELECOM wireless LAN routers a...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-59764	Multiple vulnerabilities in ELECOM wireless LAN routers a...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-61376	Multiple vulnerabilities in ELECOM wireless LAN routers a...	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18274	ZDI-26-479: Heimdall Data Database Proxy uploadJar Dir...	High / 7.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-15686	ZDI-26-478: Adminer multi_query Incorrect Check of Fu...	High / 7.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-47299	Azure Monitor Agent Elevation of Privilege Vulnerability	High / 7.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-20147	ZDI-26-581: Cisco Identity Services Engine invokeScript ...	High / 7.2	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-44098	ZDI-26-517: (Pwn2Own) Phoenix Contact CHARX SEC-3...	Medium / 6.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-62912	Microsoft Exchange Server Denial of Service Vulnerability	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63516	Microsoft SharePoint Server Spoofing Vulnerability	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-47285	Visual Studio Code Information Disclosure Vulnerability	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-44091	ZDI-26-518: (Pwn2Own) Phoenix Contact CHARX SEC-3...	Medium / 6.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-20148	ZDI-26-582: Cisco Identity Services Engine PatchUpdat...	Medium / 4.9	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-66783	Submariner-operator: release workflow consumes same-...	Medium / 4.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-3854	Wiz's First 6 Months as Part of Google	Unscored	PUBLIC EXPLOIT/POC	✓ Blocked
NS-88571D3C3D876280	The Generator Can't Be the Validator: What OpenAI's Hu...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
ZD-4676374AC535298E	The risk hiding behind exposed MCP servers	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66066	CVE-2026-66066: Defending Against the "KindaRails2S...	Unscored	CISA KEV	✓ Blocked
NS-6CD8D5BC81B5F714	CosmosEscape: Taking Over Every Database in Azure Co...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15969	VU#281278: SGLang contains six different vulnerabilities...	Unscored	PUBLIC EXPLOIT/POC	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 138 blocked · avg CVSS 8.3 · 12 CISA KEV (continued)				
CVE-2026-15971	VU#281278: SGLang contains six different vulnerabilities...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15974	VU#281278: SGLang contains six different vulnerabilities...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15976	VU#281278: SGLang contains six different vulnerabilities...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15977	VU#281278: SGLang contains six different vulnerabilities...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15978	VU#281278: SGLang contains six different vulnerabilities...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
NS-5EAF5C26A862BEB7	Intigriti Bug Bytes #238 - July 2026 🚀	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-33824	CVE-2026-33824 Windows Internet Key Exchange (IKE) ...	Unscored	CISA KEV	✓ Blocked
CVE-2026-15782	Vulnerability & Patch Roundup — July 2026	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15787	Vulnerability & Patch Roundup — July 2026	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15145	Vulnerability & Patch Roundup — July 2026	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15156	Vulnerability & Patch Roundup — July 2026	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-65497	Vulnerability & Patch Roundup — July 2026	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-65496	Vulnerability & Patch Roundup — July 2026	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-12900	Vulnerability & Patch Roundup — July 2026	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-65498	Vulnerability & Patch Roundup — July 2026	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-17555	Vulnerability & Patch Roundup — July 2026	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-14073	Vulnerability & Patch Roundup — July 2026	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-65458	Vulnerability & Patch Roundup — July 2026	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-16655	Vulnerability & Patch Roundup — July 2026	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-16597	Vulnerability & Patch Roundup — July 2026	Unscored	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 138 blocked · avg CVSS 8.3 · 12 CISA KEV (continued)				
ZD-5E067EE217D27D35	China-Linked Threat Actors Weaponize New Vulnerabiliti...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
ZD-54E922BDD6E29BD1	Inside an Oracle Database SQL Injection Attack | Huntress	Unscored	NO KNOWN EXPLOIT	✓ Blocked
ZD-E25A5C8F3F3B8469	Cloud Threat Highlights: H1 2026	Unscored	NO KNOWN EXPLOIT	✓ Blocked
ZD-3070D9D42E5786C2	Toolkit Hidden Inside Oracle Database Evades Endpoint T...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-64638	WordPress 7.0.3 Released: 12 Vulnerabilities Found and F...	Unscored	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-43760	From Screen Share to Root Access: Breaking Down CVE-...	Unscored	PUBLIC EXPLOIT/POC	✓ Blocked
NS-A06F2863F0285210	WordPress Plugins Compromised Without a Single File C...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
NS-9E950B64816168CF	When a PNG Isn't a PNG: WordPress Patches an Author-L...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
NS-EA9D6A0F4EFC0CC7	Black Hat USA 2026: What the Hugging Face hack tells u...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
ZD-73CD01FD83D52CA4	Education Under Attack: The Pattern Behind Recent Univ...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-48907	[webapps] Joomla JCE_2.9.15 - Remote Code Execution	Unscored	CISA KEV	✓ Blocked
CVE-2026-29053	[webapps] Ghost_CMS 6.19.0 - Remote Code Execution	Unscored	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2025-49132	Metasploit Wrap Up: Lot of summer shells and fit http pro...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-27760	Metasploit Wrap Up: Lot of summer shells and fit http pro...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-22594	[webapps] Ghost_CMS 6.19.0 - Remote Code Execution	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54566	Supply Chain Security Analysis of a 9.5M-Install VS Code...	Unscored	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-54701	Supply Chain Security Analysis of a 9.5M-Install VS Code...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54702	Supply Chain Security Analysis of a 9.5M-Install VS Code...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-54703	Supply Chain Security Analysis of a 9.5M-Install VS Code...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-50733	Supply Chain Security Analysis of a 9.5M-Install VS Code...	Unscored	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Command Injection: 138 blocked · avg CVSS 8.3 · 12 CISA KEV (continued)				
CVE-2026-15826	WordPress Plugin Flaw Exposes 40,000 Sites to Admin T...	Unscored	CISA KEV	✓ Blocked
NS-A0B1DCB3EF8747C1	NASA Ground Control Software Flaw Enables Unauthenti...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2019-1257	Rapid7 Analysis: Microsoft SharePoint Remote Code Exe...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-42167	[remote] CVE-2026-42167 - ProFTPD mod_sql post-aut...	Unscored	CISA KEV	✓ Blocked
CVE-2026-19913	VU#308749: Remote Code Execution and Arbitrary File R...	Unscored	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-19912	VU#308749: Remote Code Execution and Arbitrary File R...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18431	Wordfence Argus Finds Complex 6 Step Critical RCE in A...	Unscored	PUBLIC EXPLOIT/POC	✓ Blocked
Cross-Site Scripting: 23 blocked · avg CVSS 7.1 · 0 CISA KEV				
CVE-2026-70332	Microsoft Office SharePoint Spoofing Vulnerability	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70306	Microsoft Office SharePoint Spoofing Vulnerability	Critical / 9.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-61876	[dos] LuCI DHCPv6 - Lease Hostname Stored Cross-Site...	High / 8.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-57104	Azure Storage Explorer Elevation of Privilege Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-65767	Microsoft Teams for Android Spoofing Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66358	Multiple vulnerabilities in acmailer (CVE-2026-66358)	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70408	Multiple vulnerabilities in acmailer (CVE-2026-70408)	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-15928	CVE-2026-15928: XMLRPC-C Library versions 1.07 thro...	High / 8.2	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-17496	NoteGen chat preview XSS via unsanitized AI/skill HTML ...	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57105	Microsoft Office SharePoint Spoofing Vulnerability	High / 8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62914	Microsoft Exchange Server Spoofing Vulnerability	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Cross-Site Scripting: 23 blocked · avg CVSS 7.1 · 0 CISA KEV (continued)				
CVE-2026-64900	Microsoft SharePoint Server Spoofing Vulnerability	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70355	Microsoft SharePoint Server Elevation of Privilege Vulner...	High / 7.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-57279	Cybozu Garoon vulnerable to cross-site scripting (CVE-2...	Medium / 6.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66779	Cross-Site Scripting (XSS) vulnerability in SAP NetWeave...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-71368	F-RevoCRM vulnerable to cross-site scripting (CVE-202...	Medium / 6.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-73537	Miraikan Assist App vulnerable to cross-site scripting (C...	Medium / 4.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62829	Microsoft SharePoint Server Spoofing Vulnerability	Medium / 4.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-64897	Microsoft SharePoint Server Spoofing Vulnerability	Medium / 4.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-64902	Microsoft SharePoint Server Spoofing Vulnerability	Medium / 4.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-64916	Microsoft SharePoint Server Spoofing Vulnerability	Medium / 4.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-64922	Microsoft SharePoint Server Spoofing Vulnerability	Medium / 4.6	NO KNOWN EXPLOIT	✓ Blocked
ZD-BE4DA1AF665C2A69	Agents vs. agents: how we triage HackerOne reports for ...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
SSRF: 17 blocked · avg CVSS 7.9 · 0 CISA KEV				
CVE-2026-65801	Microsoft Exchange Online Elevation of Privilege Vulnera...	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69502	Azure SQL Database Elevation of Privilege Vulnerability	Critical / 10	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69851	Microsoft Entra ID Elevation of Privilege Vulnerability	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70324	Microsoft SharePoint Elevation of Privilege Vulnerability	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-70326	Microsoft SharePoint Server Elevation of Privilege Vulner...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-66800	Azure Data Factory Information Disclosure Vulnerability	High / 8.6	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SSRF: 17 blocked · avg CVSS 7.9 · 0 CISA KEV (continued)				
CVE-2026-69543	Azure Virtual Machines Elevation of Privilege Vulnerability	High / 8.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69192	Security Bulletin - August 18 2026 — SSRF (Server-Side ...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69855	Microsoft Copilot in Azure Information Disclosure Vulner...	High / 7.7	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-50237	Openshift/console: namespace tenant ssrf with egress b...	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-50236	Openshift/console: authenticated ssrf with full response ...	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-58612	PowerShell Information Disclosure Vulnerability	High / 7.4	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69223	Apache Allura vulnerable to server-side request forgery (...	Medium / 6.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-58639	Microsoft SharePoint Server Spoofing Vulnerability	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-65813	Microsoft Exchange Server Elevation of Privilege Vulnera...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62902	.NET Information Disclosure Vulnerability	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-17458	mf-yang openclaw-cn Browser Control HTTP API agent.a...	Medium / 6.3	NO KNOWN EXPLOIT	✓ Blocked
SQL Injection: 11 blocked · avg CVSS 9.4 · 0 CISA KEV				
CVE-2026-68782	Azure SQL Database Elevation of Privilege Vulnerability	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-68789	Azure SQL Database Elevation of Privilege Vulnerability	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18072	Protect The Shire solves one problem, but risks making a...	Critical / 9.8	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2025-12420	Evo Continuous Offensive Security Is Here Pentesting Gr...	Critical / 9.3	PUBLIC EXPLOIT/POC	✓ Blocked
CVE-2026-0603	Security Bulletin - August 18 2026 — SQLi (SQL Injection...	High / 8.3	NO KNOWN EXPLOIT	✓ Blocked
NS-EC3B013EB78B7B3E	What Is AI Pentesting and How Does It Work?	Unscored	NO KNOWN EXPLOIT	✓ Blocked
NS-EC276845F369E046	Rethinking Scanning for the AI Era: Wiz's Agentic Code S...	Unscored	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
SQL Injection: 11 blocked · avg CVSS 9.4 · 0 CISA KEV (continued)				
NS-FECAF70800DF79D2	Anthropic Reveals Claude Escaped Testing, Breaching Th...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
NS-EEE44F26F5FEF3B5	Korea's Largest Telco KT Fined $38m After Femtocell Ca...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-34191	CVE-2026-34191 Apache Portable Runtime Utility: SQL I...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
NS-381A587B00E265C6	Benchmarking Secure-and-Functional Remediation and ...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
Path Traversal: 7 blocked · avg CVSS 8.9 · 0 CISA KEV				
CVE-2026-59115	Microsoft Entra Provisioning Service Elevation of Privileg...	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-63509	Microsoft Fabric Elevation of Privilege Vulnerability	Critical / 9.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-69400	Azure Logic Apps Elevation of Privilege Vulnerability	Critical / 9.6	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-49163	Application Insights Profiler Elevation of Privilege Vulner...	High / 8.8	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-62837	Microsoft SharePoint Server Information Disclosure Vuln...	Medium / 6.5	NO KNOWN EXPLOIT	✓ Blocked
CVE-2025-62725	CVE-2025-62725 Docker Compose Vulnerable to Path Tr...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-18412	VU#614868: OpenCart ecommerce platform contains dir...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
Injection: 5 blocked · avg CVSS 5.5 · 0 CISA KEV				
CVE-2026-62899	.NET Security Feature Bypass Vulnerability	Medium / 5.9	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-44092	ZDI-26-505: (Pwn2Own) Phoenix Contact CHARX SEC-...	Medium / 5	PUBLIC EXPLOIT/POC	✓ Blocked
ZD-7883BFD1659300C3	Can AI do novel security research? Meet the HTTP Termi...	Unscored	NO KNOWN EXPLOIT	✓ Blocked
ZD-FE5B46E68876A690	CRLF-Powered Desync Attacks: Beheading HTTP Streams	Unscored	NO KNOWN EXPLOIT	✓ Blocked
ZD-74AFBB4899CE6AB1	CSS:the bomb inside your inbox	Unscored	NO KNOWN EXPLOIT	✓ Blocked

CVE	VULNERABILITY	SEVERITY	EXPLOITATION	STATUS
Uncontrolled Resource Consumption: 2 blocked · avg CVSS 8.1 · 1 CISA KEV				
CVE-2026-60680	Oracle WebLogic Server (CVE-2026-60680)	High / 8.1	NO KNOWN EXPLOIT	✓ Blocked
CVE-2026-20349	Cisco Secure Firewall Adaptive Security Appliance and S...	Unscored	CISA KEV	✓ Blocked
Insecure Design (File-Upload): 1 blocked · avg CVSS 7.2 · 0 CISA KEV				
CVE-2026-67243	freo2 vulnerable to unrestricted upload of file with dange...	High / 7.2	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