

CVE-2025-0282

Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability

Exigent

CISA KEV since Jan 8, 2025

Actively exploited

Ransomware use known

A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a remote unauthenticated attacker to achieve remote code execution.

EVRS 94/100 Immediate priority	CVSS V3.1 9.0 Critical · NVD	EPSS 0.999 99.98th percentile · FIRST	CISA DEADLINE Jan 15, 2025 KEV since 2025 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations as set forth in the CISA instructions linked below to include conducting hunt activities, taking remediation actions if applicable, and applying updates prior to returning a device to service.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
connect secure	22.7	no fixed version listed	NVD
neurons for zero-trust access	22.7	no fixed version listed	NVD
policy secure	22.7	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-rf94-f4r9-6gxx	Additional guidance	forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283
CISA Mitigation Instructions	cisa.gov/cisa-mitigation-instructions-CVE-2025-0282 Additional References: https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283	NVD	nvd.nist.gov/vuln/detail/CVE-2025-0282
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-1580
Current data	evulnable.com/vulnerability-management/cve/CVE-2025-0282		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.