

CVE-2025-22457

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

Exigent CISA KEV since Apr 4, 2025 Actively exploited Ransomware use known Public exploit module (Metasploit)

A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.6, Ivanti Policy Secure before version 22.7R1.4, and Ivanti ZTA Gateways before version 22.8R2.2 allows a remote unauthenticated attacker to achieve remote code execution.

EVRS 95/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.98th percentile · FIRST	CISA DEADLINE Apr 11, 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 9.8	☐ 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.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
connect secure	< 22.7 22.7	22.7	NVD
policy secure	< 22.7 22.7	22.7	NVD
zero trust access gateway	< 22.8 22.8	22.8	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-jjr5-fpcg-gc53	Additional guidance	forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457
CISA Mitigation Instructions	cisa.gov/cisa-mitigation-instructions-cve-2025-22457	NVD	nvd.nist.gov/vuln/detail/CVE-2025-22457
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-9646
Current data	evulnable.com/vulnerability-management/cve/CVE-2025-22457		

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