

CVE-2024-21887

Ivanti Connect Secure and Policy Secure Command Injection Vulnerability

Exigent

CISA KEV since Jan 10, 2024

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance.

EVRs

93/100

Immediate priority

CVSS V3.1

9.1

Critical · NVD

EPSS

0.999

99.99th percentile · FIRST

CISA DEADLINE

Jan 22, 2024

KEV since 2024 · 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	On the CISA KEV catalog for over two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified**CISA required action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. **CISA****note:** Please apply mitigations per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
connect secure	9.0	no fixed version listed	NVD
	9.1		
	22.1		
	22.2		
	22.3		
	22.4		
	22.5		
	22.6		
policy secure	9.0	no fixed version listed	NVD
	9.1		
	22.1		
	22.2		
	22.3		
	22.4		
	22.5		
	22.6		



Sources

Vendor guidance	github.com/advisories/GHSA-87qj-c5f7-6c8q	Additional guidance	forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US
forums.ivanti.com	forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US	NVD	nvd.nist.gov/vuln/detail/CVE-2024-21887
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-19498
Current data	evulnable.com/vulnerability-management/cve/CVE-2024-21887		

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