

CVE-2026-111357

Ivanti Connect Secure Missing Authentication for Critical Function Vulnerability

CISA KEV since Oct 30, 2026

Actively exploited

Ivanti Connect Secure 22.8R2.4 mishandles the manner in which the dsinvoked broker trusts DSCache configuration data, leading to privilege escalation to root, as exploited in the wild in October 2026.

<p>EVRS</p> <p>75_{/100}</p> <p>Urgent priority</p>	<p>CVSS V3.1</p> <p>7.0</p> <p>High · NVD</p>	<p>EPSS</p> <p>0.003</p> <p>24.6th percentile · FIRST</p>	<p>CISA DEADLINE</p> <p>Nov 2, 2026</p> <p>CISA federal deadline in 2 days</p>
---	--	--	---

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	No known ransomware campaign association	☒ KEV recency	Added to CISA KEV within the last 30 days
☒ EPSS	0.003 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
connect secure	≥ 25.1.0.0 < 25.1.1.3 22.8	25.1.1.3	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-fhw5-mpvj-x89m	hub.ivanti.com	hub.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-CVE-2026-104935?Language=en_US
cisa.gov	cisa.gov/news-events/alerts/2026/10/13/cisa-urges-patching-newly-exploited-vulnerability-ivanti-connect-secure	BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk
Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk	NVD	nvd.nist.gov/vuln/detail/CVE-2026-111357
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-102437
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-111357		

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