

SECURITY ADVISORY

Ivanti Connect Secure exploited

CVE-2026-111357 · on CISA's exploited list since 30 October 2026

Analysis Report

CISA added CVE-2026-111357 to its exploited list on 30 October 2026; its date is 2 November 2026. What it is, who is affected, and what to do first.

PREPARED BY	NamiQ	DATE	30 October 2026
FACTS AS OF	30 October 2026	VERSION	1.0
SEVERITY	High: CVSS 3.1 7.0	STATUS	On CISA's exploited list; due 2 November 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.

Companion article: namiq.io/insights/ivanti-connect-secure-cve-2026-111357

The short version

CISA added Ivanti Connect Secure (CVE-2026-111357) to its list of exploited vulnerabilities on 30 October 2026. That list holds only flaws CISA has evidence are being used in attacks.

Its deadline for US federal agencies is 2 November 2026. Treat it as a date to aim for. It does not bind you.

The base score is 7 (CVSS 3.1). EPSS, the estimated chance of exploitation in the next 30 days, is 0.00. Read on 30 October 2026.

Our reading

A user who is already logged in to Ivanti Connect Secure 22.8R2.4 can raise their access to root. The record says the dsinvoked broker wrongly trusts DSCache configuration data. The record also says it was exploited in the wild in October 2026.

Anyone running Connect Secure 22.8R2.4. The attacker must be logged in first, so check who holds accounts on the appliance.

What happened

Ivanti Connect Secure contains a missing authentication for critical function vulnerability that could allow a local authenticated attacker to escalate their privileges. This vulnerability can be chained with CVE-2026-104935 and CVE-2026-118527.

That is CISA's description from its catalogue entry.

The CVE record, published by Mitre on 15 October 2026, says:

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.

Are you affected?

The record lists these versions of Ivanti Connect Secure as affected:

- 22.8R2.4

The wording includes conditions the score may not show: the attacker must be logged in. Read the record before you decide it does not apply to you.

If you run it, find the version number first. If you cannot say what you run, that is the first job, and your IT provider can answer it in minutes.

What to do first

CISA's required action:

Apply mitigations in accordance with vendor instructions.

CISA's date is 2 November 2026. In order:

- Check the version your Connect Secure appliance reports. The record lists 22.8R2.4 as the affected version.
- CISA says this flaw can be chained with CVE-2026-104935 and CVE-2026-118527. Check whether your appliance is exposed to those as well.
- List the accounts that can log in to the appliance and confirm each one is expected.
- CISA's wording adds that you should stop using the product if no mitigation is available.
- If you cannot do it today, write down who owns it, the new date, and what limits exposure until then, such as restricting the interface to administrator networks.

How to check it is fixed

- The product reports a version outside the affected list. Read it from the product itself, not from an old inventory.
- Save the output or a screenshot with the date, so you can show later when it was done.

If it was exposed before you updated

CISA lists this because attacks have happened. An update closes the hole. It does not tell you whether someone used it first. Look in the product's logs and the web server's logs for the weeks before the update, and for accounts or files you did not create. CISA's required action also points to its forensic triage requirements (BOD 26-04).

- Logins to the appliance from accounts or sources you do not recognise, since the attacker must be logged in first.
- Signs that an ordinary account gained root access, such as unexpected changes to DSCache configuration data.
- Activity from the dsinvoked broker that you cannot explain.

The weakness behind it

The record classes this as CWE-829.

What we could not confirm

- CISA records ransomware use as not recorded. That means not recorded, not that none has happened. No attacker is named in the sources.
- We have not tested this against any environment. This note reports what the sources say and what we would check first.
- Version ranges are as the CVE record state them. The vendor's advisory wins where it differs.
- EPSS and scores move. The figures are as at 30 October 2026.
- The paragraphs headed "Our reading" and the numbered steps are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-111357: score 7, CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Local	Needs an account or code already running on the machine.
Attack complexity	High	Needs conditions outside the attacker's control.
Privileges required	Low	An ordinary account is enough.
User interaction	None	No one has to do anything.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
15 October 2026	CVE record published by Mitre.
30 October 2026	CISA added it to its list of exploited vulnerabilities.
30 October 2026	The facts in this report were read.
2 November 2026	CISA's deadline for US federal agencies.

Appendix 3. Definition of done

- Every Ivanti Connect Secure you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- CVE record for CVE-2026-111357: <https://www.cve.org/CVERecord?id=CVE-2026-111357>
- FIRST: Exploit Prediction Scoring System: <https://www.first.org/epss/>
- Reference in the CVE record: www.volexity.com: <https://www.volexity.com/blog/2026/10/13/a-series-of-unauthenticated-events-chained-exploitation-of-ivanti-connect-secure-zero-days/>
- Reference in the CVE record: hub.ivanti.com: <https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-CVE-2026-104935>