

SECURITY ADVISORY

Ivanti Connect Secure exploited

CVE-2026-118527 · on CISA's exploited list since 30 October 2026

Analysis Report

CISA added CVE-2026-118527 to its exploited list on 30 October 2026; its date is 13 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	Not scored yet	STATUS	On CISA's exploited list; due 13 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-2026-118527

The short version

CISA added Ivanti Connect Secure (CVE-2026-118527) 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 13 November 2026. Treat it as a date to aim for. It does not bind you.

No base score had been published when we read it. No EPSS figure was available yet. Read on 30 October 2026.

Our reading

Ivanti Connect Secure generates predictable numbers or identifiers (CWE-340). CISA says this lets a remote attacker who is logged in upload files with content they control to a known location on disk. The record says it can be chained with CVE-2026-104935 and CVE-2026-111357.

Anyone running Ivanti Connect Secure, especially where it can be reached remotely. The attacker must be logged in, so the accounts that can sign in to it matter as much as the device.

What happened

Ivanti Connect Secure contains a generation of predictable numbers or identifiers vulnerability that allows a remote authenticated attacker to upload files with attacker-controlled content to a known location on disk. This vulnerability can be chained with CVE-2026-104935 and CVE-2026-111357.

That is CISA's description from its catalogue entry.

The CVE record for CVE-2026-118527 was not available when we read it on 30 October 2026. CISA's entry is the only primary text until it is.

Are you affected?

Without the record we cannot give version ranges. Use the vendor's advisory for the affected versions.

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 13 November 2026. In order:

- Find every Ivanti Connect Secure device you run, including ones nobody has looked at lately, and note who owns each.
- Check whether CVE-2026-104935 and CVE-2026-111357 also apply to those devices, because CISA says this flaw can be chained with both.
- List the accounts that can log in to each device and remove any that are unused or that you cannot account for.
- 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).

- Files on the device that you did not put there, particularly new files in places where uploads should not land.
- Logins from accounts or locations that do not fit how your staff normally connect, in the period before you applied the vendor's mitigations.
- Signs that the same device was targeted through CVE-2026-104935 or CVE-2026-111357 as well.

The weakness behind it

CISA's entry classes this as CWE-340 (Generation of Predictable Numbers or Identifiers).

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 sources 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. Timeline

Date	Event
30 October 2026	CISA added it to its list of exploited vulnerabilities.
30 October 2026	The facts in this report were read.
13 November 2026	CISA's deadline for US federal agencies.

Appendix 2. 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-2026-118527: <https://www.cve.org/CVERecord?id=CVE-2026-118527>
- FIRST: Exploit Prediction Scoring System: <https://www.first.org/epss/>