contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

# Ivanti Connect Secure exploited

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

## Analysis Report

Any organisation running Ivanti Connect Secure before version 25.1.1.3 or 22.8R2.6 must patch by 13 November 2026. If you do not run Connect Secure at all, stop here; otherwise find which version is …

| | | | |
|---|---|---|---|
| PREPARED BY | NamiQ | DATE | 5 November 2026 |
| FACTS AS OF | 5 November 2026 | VERSION | 1.0 |
| SEVERITY | **Medium: CVSS 3.1 4.3** | 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 bottom line

> *Any organisation running Ivanti Connect Secure before version 25.1.1.3 or 22.8R2.6 must patch by 13 November 2026. If you do not run Connect Secure at all, stop here; otherwise find which version is installed first.*

## At a glance

| Fact | Detail |
|---|---|
| Product | Ivanti Connect Secure (CVE-2026-118527) |
| Severity | Medium: 4.3 (CVSS 3.1) |
| CISA | On its exploited list since 30 October 2026. Deadline for US federal agencies: 13 November 2026. |
| Chance of exploitation (EPSS) | 0.01, the estimated chance in the next 30 days, as at 5 November 2026 |
| Ransomware use | Not recorded by CISA. That is not the same as none. |
| Fixed in | Ivanti Connect Secure 25.1.1.3 and 22.8R2.6, as the record states. |
| Who looks first | Teams running Ivanti Connect Secure on any version below 25.1.1.3 or 22.8R2.6 where any user — not only trusted administrators — holds valid credentials. |

## Does this apply to you?

**Answer in order. Stop at the first no.**

| Question | If no | If yes |
|---|---|---|
| Do you run Ivanti Connect Secure anywhere? | Nothing to do for this CVE. | Check the version you are running (next question). |
| Is your version below 25.1.1.3 (22.x branch: below 22.8R2.6)? | You are on a fixed version; confirm and close. | Plan an update to 25.1.1.3 or 22.8R2.6 (next question). |
| Can any user other than a fully trusted administrator authenticate to the system? | Risk is lower; still patch within the CISA window. | Treat this as urgent; patch before 13 November 2026. |

## What it is

Because filenames are predictable, an attacker who is already logged in to Ivanti Connect Secure can upload files containing whatever they choose to a location on disk that they know in advance.

## Why it matters

The score of 4.3 reflects the authentication requirement: an attacker must already hold a valid account on the system. The record notes this flaw chains with CVE-2026-104935 and CVE-2026-111357. Our reading is that the value lies in that chain: a file written to a known path is a stable foothold a second flaw can act on — the kind of primitive that turns a bounded weakness into a complete attack path. Each flaw alone may be contained; together they may not be.

## Things people will get wrong

- A score of 4.3 means this can wait until the next routine patch cycle. CISA listed it with a deadline of 13 November 2026, and the record ties it to two further CVEs in a chain. The score reflects the authentication bar, not the potential impact of the chain.
- Only a logged-in attacker can exploit this, so our perimeter firewall is protection enough. The condition is a valid account on Connect Secure itself, not access to the internal network. Any user who can reach the login page and authenticate meets the bar.

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.

## How we would triage it

This is our judgement.

## Step 1: Find the version of Connect Secure you run

- Check the appliance admin console or system information page for the current version string; note whether it falls in the 22.x or 25.x branch.
- Compare against the record's first unaffected versions: 25.1.1.3 and 22.8R2.6; anything below those in the respective branch is affected.

## Step 2: Check whether the two chained CVEs are also open

- The record notes this flaw chains with CVE-2026-104935 and CVE-2026-111357; confirm whether those are also unpatched on the same appliance.
- A system carrying all three raises the urgency, though each should be fixed regardless.

## Step 3: Apply the update

- The record names 25.1.1.3 and 22.8R2.6 as the first unaffected versions; apply whichever matches your branch.
- No vendor advisory was available to read; follow your standard Ivanti Connect Secure update procedure and verify the version string shown in the console afterwards.

## Step 4: Check for signs of exploitation if the system was exposed

- Review authentication logs for accounts that logged in during the period an affected version was running but had no known business reason to do so.
- Look for unexpected files in paths normally written by Connect Secure; the flaw places files at a known location, so unusual content there is a signal worth investigating.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then. CISA's wording adds that you should stop using the product if no mitigation is available.

## Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *We are writing about CVE-2026-118527, which affects Ivanti Connect Secure before versions 25.1.1.3 and 22.8R2.6. CISA has set a remediation deadline of 13 November 2026. The flaw allows an authenticated user to upload files to a known location on disk, and the record notes it chains with CVE-2026-104935 and CVE-2026-111357. Could you please confirm whether we run Ivanti Connect Secure, which version is installed, whether the update to 25.1.1.3 or 22.8R2.6 has been applied or is scheduled, and whether the two chained CVEs are also addressed? We would like written confirmation of the current version and the patch status by 12 November 2026.*

## Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Unexpected files in paths normally written by the Connect Secure application, particularly any that appeared while an affected version was running.
- Authentication log entries for accounts that accessed the system at unusual times or from unexpected locations with no known business justification.

## The weakness behind it

The record classes this as CWE-340 (Generation of Predictable Numbers or Identifiers).

## The sources, in their words

CISA's catalogue entry:

> *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.*

The CVE record, published by Ivanti on 3 November 2026:

> *Use of predictable filenames in Ivanti Connect Secure before versions 25.1.1.3 and 22.8R2.6 allows a remote authenticated attacker to upload files with attacker-controlled content to a known location on disk.*

It lists these as unaffected:

- 25.1.1.3
- 22.8R2.6

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

## Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-118527
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

## Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the names of running container images and the kernel version, compares them on the spot, and only the CVE ids leave the machine;

the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-118527
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. It reads the names of the running images, not what is inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

## What we do not know yet

- No vendor advisory was available; whether Ivanti has published a workaround or mitigation short of patching is not known from the record alone.
- The specific conditions under which CVE-2026-104935 and CVE-2026-111357 combine with this flaw to form a complete attack path are not described in the record.
- Whether updating to 25.1.1.3 or 22.8R2.6 also remediates the two chained CVEs, or whether separate patches are needed for each, is not stated in the record.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 5 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

## Appendix 1. Severity decoded

**CVE-2026-118527**: score 4.3, `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N` 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 | Network | Reachable over a network, with no need to be on the same segment. |
| Attack complexity | Low | No special conditions beyond the flaw itself. |
| 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 | None | No data exposed. |
| Integrity | Low | Some data or behaviour can be altered. |
| Availability | None | No effect on availability. |

## Appendix 2. Timeline

| Date | Event |
|---|---|
| 30 October 2026 | CISA added it to its list of exploited vulnerabilities. |
| 3 November 2026 | CVE record published by Ivanti. |
| 13 November 2026 | CISA's deadline for US federal agencies. |

## Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

| Your situation | Priority | Timeframe |
|---|---|---|
| Affected Connect Secure version is internet-facing and any authenticated user can reach it | High | Before 13 November 2026 |
| Affected version, CVE-2026-104935 or CVE-2026-111357 also unpatched on the same system | High | Before 13 November 2026 |
| Affected version, authentication limited to trusted staff, no direct internet exposure | Medium | Within the CISA window |

| | | |
|---|---|---|
| Affected version confirmed but all three chained CVEs are separately mitigated | Medium | This patch cycle |
| Running fixed version 25.1.1.3 or 22.8R2.6 | None | None for this CVE |

## Appendix 4. 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.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- 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/
- Reference in the CVE record: hub.ivanti.com: https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-CVE-2026-104935?language=en_US