contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Ivanti Connect Secure exploited

CVE-2026-104935 · on CISA's exploited list since 13 October 2026

Analysis Report

If you run Ivanti Connect Secure, treat this as urgent: CISA's deadline of 16 October 2026 has already passed. First find your version, and if it is below 25.1.3.0 on the 25.1 line, get it patched ...

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
SEVERITY	**High: CVSS 3.1 8.6**	STATUS	On CISA's exploited list; due 16 October 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-2026-104935

The bottom line

> *If you run Ivanti Connect Secure, treat this as urgent: CISA's deadline of 16 October 2026 has already passed. First find your version, and if it is below 25.1.3.0 on the 25.1 line, get it patched and checked for compromise.*

At a glance

Fact	Detail
Product	Ivanti Connect Secure (CVE-2026-104935)
Severity	High: 8.6 (CVSS 3.1)
CISA	On its exploited list since 13 October 2026. Deadline for US federal agencies: 16 October 2026.
Chance of exploitation (EPSS)	0.87, the estimated chance in the next 30 days, as at 1 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	Unaffected per the record: 25.1.3.0, 25.1.3.1, 22.8R2.5 and 22.7R2.14. No vendor advisory could be read to confirm the fix.
Who looks first	Anyone who runs Ivanti Connect Secure, especially owners of an appliance that remote staff reach from the internet, and the IT provider who manages it.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Ivanti Connect Secure (also called ICS)?	Nothing to do for this CVE.	Check the version (next question).
Is your version below 25.1.3.0, and not 22.8R2.5 or 22.7R2.14 or later?	The record lists your version as unaffected. Keep a written note of it.	You are in the affected range. Go to the next question.
Can anyone on the internet reach the appliance's sign-in or service address?	Risk is lower, but still patch and check for compromise.	Treat it as exposed now: patch and review for compromise.

What it is

An attacker on the network, with no login, can pretend to be a legitimate user and make the appliance run commands of their choosing. The record calls this an authentication bypass by spoofing.

Why it matters

The record says no login is needed and the result is command execution on the appliance. Our reading is that a remote access gateway sits between the internet and your internal network, so an attacker who controls it is well placed to reach what lies behind it. The record's score and the exploitation listing both point the same way, so do not wait for a routine patch cycle.

Things people will get wrong

- "Our version is old, so we are safe." Not always. The record says 22.7R2.14 and earlier are not affected, but it gives no range for the other versions. Check the exact version.
- "It needs a valid login first." The record describes a remote, unauthenticated attacker. A login is not required.

How we would triage it

This is our judgement.

Step 1: Find the versions you run

- Ask whoever manages the appliance for the exact Connect Secure version.
- Compare it with the unaffected versions the record lists: 25.1.3.0, 25.1.3.1, 22.8R2.5 and 22.7R2.14.

Step 2: Reduce exposure

- If you cannot patch today, ask your provider whether access from the internet can be restricted until you can.
- Follow the vendor's mitigation instructions, as CISA's required action says.

Step 3: Patch to an unaffected version

- Move to a version the record lists as unaffected.
- The record names no workaround, and no vendor page could be read. Get the vendor's own instructions.

Step 4: Check for compromise

- Because exploitation is listed, ask your provider to review the appliance for signs of misuse, not only to patch it.
- Ask for the result in writing.

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.

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.

> *Hello, we need to know whether we run Ivanti Connect Secure, and if so on which version. This concerns CVE-2026-104935, an authentication bypass that lets an unauthenticated attacker run commands. The record lists 25.1.3.0, 25.1.3.1, 22.8R2.5 and 22.7R2.14 as unaffected. CISA's deadline of 16 October 2026 has passed. Please confirm in writing which version each appliance runs, whether it is patched, and whether you have checked it for signs of compromise. Please reply by a date you propose this week. Thank you.*

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:

- Sign-ins or admin sessions on the appliance that nobody on your team can account for.
- Commands, new files or changed settings on the appliance that no one on your team made.
- Unexpected outbound connections from the appliance to addresses you do not recognise.

The weakness behind it

The record classes this as CWE-290 (Authentication Bypass by Spoofing).

The sources, in their words

CISA's catalogue entry:

> *Ivanti Connect Secure contains an authentication bypass by spoofing vulnerability that allows a remote unauthenticated attacker to execute arbitrary commands.*

The CVE record, published by Ivanti on 13 October 2026:

> *Authentication bypass by spoofing in ICS before version 25.1.3.0 allows a remote unauthenticated attacker to execute arbitrary commands. This does not impact ICS version 22.7R2.14 or prior.*

It lists these as unaffected:

- 25.1.3.0
- 25.1.3.1
- 22.8R2.5
- 22.7R2.14

CISA's 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).*

What we do not know yet

- Which versions between 22.7R2.14 and 25.1.3.0 are affected: the record gives no ranges, only unaffected versions.
- What the vendor's advisory says about fixes or workarounds: no vendor page could be read.
- How attacks are carried out, and what signs they leave on the appliance.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 1 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-2026-104935: score 8.6, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L` 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	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	Low	Some data or behaviour can be altered.
Availability	Low	Reduced performance or interruptions.

Appendix 2. Timeline

Date	Event
13 October 2026	CVE record published by Ivanti.
13 October 2026	CISA added it to its list of exploited vulnerabilities.
16 October 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
Internet-facing appliance on a version below 25.1.3.0	High	Now; CISA's date has passed
Appliance on the 22.8 line, version not confirmed	High	Now, until the version is confirmed
Appliance on 22.7R2.14 or earlier	Low	Confirm the version; no action for this CVE

Appliance reachable only from inside the network	Medium	This week
You do not run Ivanti Connect Secure	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.
- 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-2026-104935: https://www.cve.org/CVERecord?id=CVE-2026-104935
- 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