contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Ivanti Connect Secure exploited

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

Analysis Report

If you run Ivanti Connect Secure, act now: CISA's deadline is 2 November 2026. First find out which version you run, then ask for the patch Ivanti published on 29 October 2026. If you do not run this …

PREPARED BY	NamiQ	DATE	5 November 2026
FACTS AS OF	5 November 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 bottom line

> *If you run Ivanti Connect Secure, act now: CISA's deadline is 2 November 2026. First find out which version you run, then ask for the patch Ivanti published on 29 October 2026. If you do not run this appliance, you can stop reading.*

At a glance

Fact	Detail
Product	Ivanti Connect Secure (CVE-2026-111357)
Severity	High: 7 (CVSS 3.1)
CISA	On its exploited list since 30 October 2026. Deadline for US federal agencies: 2 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	No source we read names a fixed version
Who looks first	Anyone running Ivanti Connect Secure VPN, especially 22.8R2.4, the only version the record lists as affected. Volexity found a fully patched 22.8R2.4 appliance compromised.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Ivanti Connect Secure?	Nothing to do for this CVE.	Check the version (next question).
Is the appliance on version 22.8R2.4?	Ask Ivanti in writing whether your version is affected.	Install the patch Ivanti published on 29 October 2026.
Can the appliance be reached from the internet?	Lower exposure, but still patch and check for compromise.	Treat as urgent and check for signs of compromise.

What it is

An attacker who is already logged in to the appliance can gain root, because the dsinvoked broker trusts DSCache configuration data it should not, the record says. Volexity reports it was the last step of a chain that began without a login.

Why it matters

Our reading is that the 'logged in' condition gives little comfort. Volexity says this flaw was the last step after an authentication bypass and a code execution flaw (CVE-2026-104935), which together gave root without a login. Volexity also says the actor went after Active Directory credentials, LAPS passwords and BitLocker recovery keys, and deleted evidence from logs. A VPN appliance sits in a trusted place on the network, so root on it is a foothold for everything behind it.

What the vendor's advisory says

We read one page on www.volexity.com. In short:

- Volexity says Ivanti published a patch for this flaw on 29 October 2026 and points to Ivanti's advisory. Our sources do not give the fixed version number.
- Volexity describes a chain of three flaws: an authentication bypass in welcome.cgi, a file write flaw in wu.cgi, and this privilege escalation.
- Volexity ties the authentication bypass and code execution flaws to CVE-2026-104935. CISA says this flaw can also be chained with CVE-2026-118527, which our sources do not describe.
- Volexity says Ivanti published an advisory with upgrade instructions for the chain, and that signs such as lateral movement from the appliance call for forensic investigation.

Things people will get wrong

- "It needs a login, so it is low risk." CISA says the attacker is authenticated, but Volexity says it was chained with an authentication bypass to give unauthenticated root.
- "We were fully patched, so we are fine." Volexity found a fully patched 22.8R2.4 appliance (Build 19097) compromised in early October 2026. The patch came on 29 October 2026.
- "No web shell was found, so nothing happened." Volexity says no backdoor or web shell was left, commands travelled in ordinary HTTPS requests, and the actor deleted evidence from logs.

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 versions you run

- Check the version of each Connect Secure appliance in its admin console. Only 22.8R2.4 is listed as affected.
- If you do not manage it yourself, ask whoever does.

Step 2: Read the vendor advisory for mitigations

- Volexity says Ivanti's advisory has upgrade instructions. Read it for any mitigation to apply before you can patch.

Step 3: Patch the appliance

- Apply the patch Ivanti published on 29 October 2026.
- Our sources do not name the fixed version, so ask for the resulting version number in writing.

Step 4: Check for signs of compromise

- The actor deleted evidence from debug and audit logs, so an empty log is not proof of safety.
- Volexity advises forensic investigation where there are signs such as lateral movement from the appliance.

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.

> *Hello, we need to know whether we run Ivanti Connect Secure, and if so where and on which version. This concerns CVE-2026-111357, a privilege escalation to root that CISA lists as exploited. The record names version 22.8R2.4 as affected. Ivanti published a patch on 29 October 2026, and CISA's deadline is 2 November 2026. Please confirm in writing by the end of tomorrow the version we run, whether the patch is installed, and whether the appliance has been checked for signs of compromise. 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:

- Signs of lateral movement starting from the VPN appliance, such as logins to internal systems from its address.
- Unexpected access to Active Directory credentials, LAPS passwords or BitLocker recovery keys, which Volexity says the actor targeted.
- Gaps or missing entries in the appliance's debug and audit logs, since the actor deleted evidence.

The weakness behind it

The record classes this as CWE-829.

The sources, in their words

CISA's catalogue entry:

> *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.*

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

> *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.*

Versions of Ivanti Connect Secure the record lists as affected:

- 22.8R2.4

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-2026-111357
```

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-2026-111357
```

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

- Which version number contains the fix; our sources do not name one.
- Whether versions other than 22.8R2.4 are affected; the record lists only that one.
- What CVE-2026-118527 is, beyond CISA's statement that it can be chained with this flaw.
- Whether Ivanti offers a workaround short of patching.
- 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-2026-111357: 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.
2 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
Internet-facing appliance on 22.8R2.4	High	within CISA's window
Appliance on 22.8R2.4 reachable only from the internal network	Medium	this week
Patched since 29 October 2026 but exposed while on 22.8R2.4	Medium	this week, check for compromise

Another Connect Secure version, not listed as affected	Low	when Ivanti confirms in writing
No Ivanti Connect Secure in the estate	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-2026-111357: https://www.cve.org/CVERecord?id=CVE-2026-111357
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: www.volexity.com/blog/2026/10/13/a-series-of-unauthenticated-eve: 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