contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Mitel MiCollab exploited

CVE-2026-133324 · on CISA's exploited list since 25 November 2026

Analysis Report

Anyone running Mitel MiCollab up to and including 10.3 (10.3.0.18) must act by 28 November 2026 — CISA's deadline. Apply Mitel's patch to release 10.3 or upgrade, or block external access to the ...

PREPARED BY	NamiQ	DATE	26 November 2026
FACTS AS OF	26 November 2026	VERSION	1.0
SEVERITY	**Medium: CVSS 3.1 5.3**	STATUS	On CISA's exploited list; due 28 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/mitel-micollab-cve-2026-133324

The bottom line

> *Anyone running Mitel MiCollab up to and including 10.3 (10.3.0.18) must act by 28 November 2026 — CISA's deadline. Apply Mitel's patch to release 10.3 or upgrade, or block external access to the conferencing component while patching is arranged.*

At a glance

Fact	Detail
Product	Mitel MiCollab (CVE-2026-133324)
Severity	Medium: 5.3 (CVSS 3.1)
CISA	On its exploited list since 25 November 2026. Deadline for US federal agencies: 28 November 2026.
Chance of exploitation (EPSS)	0.00, the estimated chance in the next 30 days, as at 26 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	The vendor's advisory says: apply Mitel's patch to release 10.3 (10.3.0.18) following KB000129195, or upgrade to a later release. No specific later version number is named in the advisory.
Who looks first	Anyone running Mitel MiCollab at version 10.3 (10.3.0.18) or earlier, especially where the Audio, Web, and Video Conferencing (AWV) component is reachable from outside the organisation.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Mitel MiCollab anywhere in your estate?	Nothing to do for this CVE.	Check the version installed.
Is the installed version 10.3 (10.3.0.18) or earlier?	Outside the stated affected range; monitor Mitel's advisory for updates.	Check whether the AWV component is active.
Is the Audio, Web, and Video Conferencing (AWV) component enabled?	Lower risk; apply the patch before 28 November 2026 at next opportunity.	Check whether untrusted users can reach it from outside the network.

Can anyone outside the network reach the AWV component?	Apply the patch before 28 November 2026.	Apply the interim workaround and patch immediately — before 28 November 2026.

What it is

The record says an unauthenticated attacker can exploit improper handling of authentication in MiCollab's Audio, Web, and Video Conferencing component to bypass login checks and perform actions the application should not permit without credentials.

What the vendor's advisory says

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

- The same advisory covers five CVEs in the AWV component. CVE-2026-133303 (Critical, CVSS 9.0) and CVE-2026-133323 (Critical, CVSS 10.0) are also unauthenticated, network-reachable flaws addressed by the same patch.
- The advisory states that exploiting these vulnerabilities together can significantly amplify their impact.
- The advisory recommends restricting external access to the AWV component as an interim mitigation for those unable to patch immediately.
- The fix is to apply Mitel's provided patch to release 10.3 (10.3.0.18) following KB000129195, or upgrade to a later release. Products at End of Support are not covered by the advisory.

Things people will get wrong

- The medium CVSS score (5.3) means this fits a normal patch queue. The same advisory contains a CVSS 10.0 flaw in the identical component; the vendor says the two flaws together amplify impact, and the remediation window is three days.
- Being on 10.3 (10.3.0.18) without upgrading means the system stays vulnerable. The vendor's advisory says a patch is provided specifically for 10.3 (10.3.0.18); applying it addresses the vulnerability on that release.

How we would triage it

This is our judgement.

Step 1: Find the MiCollab version installed

- Log into the MiCollab administration portal and note the displayed build or release number. The record lists all versions up to and including 10.3 (10.3.0.18) as affected.

- Confirm the version with your Mitel reseller or support contact if it is not visible in the portal.

Step 2: Restrict external access to AWV as an interim measure

- The vendor's advisory says restricting external access to the AWV component mitigates risk for those unable to patch immediately. Apply this at the network perimeter or firewall before patching is complete.

Step 3: Apply Mitel's patch or upgrade

- The advisory says apply the provided patch to release 10.3 (10.3.0.18) following instructions in KB000129195, or upgrade to a later release.
- Products at End of Support status are not covered by the advisory; verify support status before relying on this guidance.

Step 4: Confirm the patch level after applying

- After applying, verify the installed build in the administration portal matches the patched state described in KB000129195.
- Record the confirmed version and date for your remediation log.

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 have been alerted to CVE-2026-133324, an authentication bypass in the Audio, Web, and Video Conferencing component of Mitel MiCollab. All versions up to and including 10.3 (10.3.0.18) are listed as affected. CISA added this to its Known Exploited Vulnerabilities catalogue on 25 November 2026 with a remediation deadline of 28 November 2026. The vendor recommends applying the provided patch to release 10.3 (10.3.0.18) or upgrading to a later release. Please confirm whether we run MiCollab, which version is installed, whether the conferencing component is externally accessible, and what patch or upgrade action has been taken. We need written confirmation of the installed version and fix status by 27 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:

- Authentication failures or unexpected successful sessions in AWV component logs, particularly from unfamiliar source addresses or outside normal business hours.
- Conference sessions or administrative changes in MiCollab that cannot be matched to a known user action.

The weakness behind it

The record classes this as CWE-636 (Not Failing Securely).

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so
Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	The flaw is in a network-reachable conferencing component requiring no authentication (AV:N, AC:L, PR:N); an attacker with network access would likely exploit it directly as an entry point.
Account Manipulation (T1098): Changing an existing account, for example adding permissions or keys, to keep access.	Persistence: staying in	After bypassing authentication, an attacker can perform unauthorised actions within the application; this would typically include manipulating account or session state within the conferencing system.
Data Manipulation: Stored Data Manipulation (T1565.001): Changing stored data without permission.	Impact: causing damage or disruption	The CVSS vector shows integrity impact (I:L); unauthorised writes within the application context following the bypass would typically manifest as stored data manipulation.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

CISA's catalogue entry:

> *Mitel MiCollab contains a not failing securely vulnerability in the Audio, Web and Video Conferencing (AWV) component that could allow an unauthenticated attacker to bypass authentication controls and perform unauthorized actions.*

The CVE record, published by Mitre on 19 November 2026:

> *A vulnerability in the Audio, Web, and Video Conferencing (AWV) component of Mitel MiCollab through 10.3 (10.3.0.18) could allow an unauthenticated attacker to conduct an authentication bypass attack due to improper handling of authentication. A successful exploit could allow an attacker to bypass authentication and perform unauthorized actions within the context of the application. This is MTLVULN-1877.*

Versions of Mitel MiCollab the record lists as affected:

- all versions up to and including 10.3 (10.3.0.18)

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-2026-133324
```

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 hardware (maker, model, firmware), the running container images with their operating system and packages, 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-2026-133324
```

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. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages 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

- The record does not describe what specific actions an attacker can perform after bypassing authentication — whether that includes reading data, modifying settings, or accessing other users' sessions.
- No specific later release beyond 10.3 is named in the advisory as confirmed unaffected.
- The record does not say whether the AWV component is externally accessible by default in a standard MiCollab deployment.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 26 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping", "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-2026-133324: score 5.3, `CVSS:3.1/AV:N/AC:L/PR:N/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	None	No account is needed.
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
19 November 2026	CVE record published by Mitre.
25 November 2026	CISA added it to its list of exploited vulnerabilities.
28 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
MiCollab 10.3 (10.3.0.18) or earlier with AWV accessible from the internet, unpatched.	High	Before 28 November 2026
MiCollab 10.3 (10.3.0.18) or earlier with AWV restricted to the internal network, unpatched.	Medium	This week; before 28 November 2026
MiCollab 10.3 (10.3.0.18) or earlier with AWV disabled or not deployed.	Low	Apply patch this patch cycle

MiCollab not present in the estate.	None	Nothing to do for this CVE

Appendix 4. Definition of done

- Every Mitel MiCollab 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-2026-133324: https://www.cve.org/CVERecord?id=CVE-2026-133324
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: www.mitel.com/support/security-advisories/mitel-product-secur: https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2026-0012