contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Mitel MiCollab exploited

CVE-2026-133311 · on CISA's exploited list since 25 November 2026

Analysis Report

If you do not run Mitel MiCollab, stop reading. Those on version 10.3 (10.3.0.18) or earlier must act by 9 December 2026: apply Mitel's patch for release 10.3, or upgrade to a later release — the fix ...

PREPARED BY	NamiQ	DATE	26 November 2026
FACTS AS OF	26 November 2026	VERSION	1.0
SEVERITY	**Medium: CVSS 3.1 5.9**	STATUS	On CISA's exploited list; due 9 December 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-2026-133311

The bottom line

> *If you do not run Mitel MiCollab, stop reading. Those on version 10.3 (10.3.0.18) or earlier must act by 9 December 2026: apply Mitel's patch for release 10.3, or upgrade to a later release — the fix also covers four other flaws in the same component, two of which the vendor rates as critical.*

At a glance

Fact	Detail
Product	Mitel MiCollab (CVE-2026-133311)
Severity	Medium: 5.9 (CVSS 3.1)
CISA	On its exploited list since 25 November 2026. Deadline for US federal agencies: 9 December 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 the patch provided for release 10.3 (10.3.0.18), or upgrade to a later release.
Who looks first	Anyone running Mitel MiCollab up to and including version 10.3 (10.3.0.18) with the Audio, Web and Video Conferencing (AWV) component active. No login is required to exploit this.

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 environment?	Nothing to do for this CVE.	Check the installed version.
Is your MiCollab version 10.3 (10.3.0.18) or earlier?	Nothing to do for this CVE.	Check whether AWV is active.
Is the AWV (conferencing) component active on that instance?	Lower urgency; still plan an upgrade — two critical flaws share this fix.	Check who can reach it (next question).

Can untrusted or external users reach the AWV component?	Lower urgency; patch this cycle — two critical flaws in the same component share this fix.	Act now: apply the patch or upgrade before 9 December 2026.

What it is

An unauthenticated attacker who knows a specific system-generated random identifier, or who has pre-staged content, can access the AWV conferencing component and obtain sensitive information. The record says access is limited to the affected functionality and does not extend to arbitrary files elsewhere on the system.

What the vendor's advisory says

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

- CVE-2026-133275 (MTLVULN-1861): arbitrary file upload in the AWV component, rated medium by the vendor; an unauthenticated attacker could upload arbitrary files to the target system.
- CVE-2026-133303 (MTLVULN-1862): XML injection in the AWV component, rated critical by the vendor; an unauthenticated attacker could execute arbitrary commands, with potential impacts on confidentiality, integrity and availability.
- CVE-2026-133323 (MTLVULN-1864): blind command injection in the AWV component, rated critical by the vendor; an unauthenticated attacker could execute arbitrary commands, with potential impacts on integrity and availability.
- CVE-2026-133324 (MTLVULN-1877): authentication bypass in the AWV component, rated medium by the vendor; an unauthenticated attacker could bypass authentication controls and perform unauthorised actions.
- The advisory states that exploiting these vulnerabilities together can significantly amplify their impact, and recommends applying the patch for 10.3 (10.3.0.18) or upgrading to a later release.

Things people will get wrong

- The flaw is described as limited, so it cannot enable serious damage. The record limits access to AWV functionality, but the vendor's advisory warns that chaining these five AWV flaws — two rated critical — can significantly amplify the impact.

How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page

before you run them. Words in capitals are for you to fill in.

Step 1: Find the MiCollab version you run

- Log in to the MiCollab administration console and check the system information or about page for the installed version number.
- If you have more than one MiCollab instance, check each one separately — versions may differ across deployments.
- Confirm whether the AWV component is enabled in the system configuration.

```
rpm -qa | grep -i micollab
dpkg -l | grep -i micollab
```

Step 2: Determine who can reach the AWV component

- Check whether AWV conferencing endpoints are accessible from outside your network or from untrusted users.
- If a firewall restricts AWV to known internal users only, external exploitation is harder, though internal risk remains.
- Two critical flaws in the same component share this fix; patch regardless of network exposure.

Step 3: Apply the vendor's patch or upgrade

- The vendor's advisory says to apply the patch provided for release 10.3 (10.3.0.18) or upgrade to a later release.
- Follow Mitel's patching procedure for your deployment type.
- After patching, confirm the installed version to verify the fix is in place.

Step 4: Check logs for signs of prior access

- Review AWV access logs for unauthenticated requests, especially those with unusual or random-looking identifiers in session or conferencing parameters.
- Look for access from IP addresses not associated with known users or active conferencing sessions, particularly before the patch was applied.

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 run Mitel MiCollab and need to understand our exposure to CVE-2026-133311. This is an unauthenticated access vulnerability in the AWV (conferencing) component, affecting all versions up to and including 10.3 (10.3.0.18). CISA has listed it with a remediation deadline of 9 December 2026. Please confirm: which version we are running on each instance, whether the AWV component is active, and whether Mitel's patch for release 10.3 or an upgrade to a later release has been applied. We need written confirmation of the installed version and fix status by 5 December 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:

- Unauthenticated requests to AWV endpoints, particularly from external IP addresses or at unusual hours, in the period before the patch was applied.
- Requests carrying random-looking or unexpected identifiers in parameters associated with AWV conferencing sessions.
- Access to AWV from IP addresses not associated with any known conferencing session or registered user.

The weakness behind it

The record classes this as CWE-1390 (Weak Authentication).

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 AWV component is a network-accessible conferencing service; exploiting an unauthenticated flaw in it with no prior access would likely follow exploitation of a public-facing application.

File and Directory Discovery (T1083): Listing files and folders to find what is there.	Discovery: looking around	The flaw allows an attacker to obtain sensitive information within the AWV scope; the record's reference to file access limits suggests file or directory discovery within that context would likely be involved.

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 weak authentication vulnerability in the Audio, Web and Video Conferencing (AWV) component that could allow an unauthenticated attacker to access sensitive information using a specific system-generated random identifier or pre-staged content.*

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, with knowledge of a specific system-generated random identifier or pre-staged content, to conduct an unauthorized access attack due to improper authentication mechanisms. A successful exploit could allow an attacker to obtain sensitive information. The vulnerability is limited to the affected functionality and does not provide unrestricted access to arbitrary files elsewhere on the system. This is MTLVULN-1863.*

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-2026-133311
```

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-2026-133311
```

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 sources do not describe how difficult it is to obtain or predict the system-generated random identifier the flaw relies on.
- The advisory does not name a specific later release version beyond 10.3 (10.3.0.18) with the patch that is confirmed unaffected.
- The sources do not say whether exploitation of this CVE has been observed in combination with the other four AWV flaws in the same advisory.
- The record does not describe what category of sensitive information can be obtained through the affected AWV functionality.
- 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-2026-133311: score 5.9, `CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/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	High	Needs conditions outside the attacker's control.
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	None	Nothing 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.
9 December 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 AWV on version 10.3 or earlier, exposed to the internet	High	By 9 December 2026
MiCollab AWV on an affected version, reachable by untrusted or external users	High	By 9 December 2026
MiCollab AWV on an affected version, internal network only, trusted users only	Medium	This patch cycle

MiCollab on affected version but AWV component not in active use	Low	Next maintenance window
MiCollab already patched or upgraded past the affected release	None	None

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-2026-133311: https://www.cve.org/CVERecord?id=CVE-2026-133311
- 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