contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Mitel MiCollab exploited

CVE-2026-133275 · on CISA's exploited list since 25 November 2026

Analysis Report

Any organisation running Mitel MiCollab on version 10.3 (10.3.0.18) or earlier must apply the vendor patch before 28 November 2026. Contact your IT provider today and ask them to apply the patch ...

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-2026-133275

The bottom line

> *Any organisation running Mitel MiCollab on version 10.3 (10.3.0.18) or earlier must apply the vendor patch before 28 November 2026. Contact your IT provider today and ask them to apply the patch Mitel issued for release 10.3; if you do not run MiCollab, you can stop here.*

At a glance

Fact	Detail
Product	Mitel MiCollab (CVE-2026-133275)
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 states a patch is available for MiCollab release 10.3; the specific patch version number is not given in the advisory text available.
Who looks first	Organisations running Mitel MiCollab version 10.3 (10.3.0.18) or earlier with the Audio, Web and Video Conferencing (AWV) component in use. The record does not list a condition that limits which users can reach the vulnerable endpoint.

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 version running.
Is your MiCollab version 10.3 (10.3.0.18) or earlier?	Nothing to do for this CVE; confirm this with your IT provider.	Apply the vendor patch immediately.
Is the AWV conferencing component enabled and reachable from outside your network?	Internal exposure still applies; apply the patch before 28 November 2026.	Treat as urgent; patch before 28 November 2026.

What it is

An unauthenticated attacker can send files of any type to a MiCollab server through the AWV conferencing component, because the application does not check what kind of file is being submitted. The record says a successful exploit allows the attacker to upload arbitrary files to the target system.

Why it matters

The CVSS score is 5.3 (medium), which on its own suggests lower urgency; the broader context changes that. The vendor's advisory describes four companion flaws in the same AWV component, two rated critical (CVE-2026-133303 and CVE-2026-133323), both reachable without authentication. The advisory states that exploiting these vulnerabilities together can significantly amplify their impact. Our reading is that the file upload flaw is likely a staging step: placing a file on the server can support the critical command-injection and authentication-bypass flaws fixed in the same patch.

What the vendor's advisory says

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

- CVE-2026-133303 (MTLVULN-1862): XML injection in AWV, rated critical by the vendor; unauthenticated attacker can execute arbitrary commands, with potential impact on confidentiality, integrity, and availability.
- CVE-2026-133311 (MTLVULN-1863): Unauthorized access in AWV, rated medium; unauthenticated attacker with knowledge of a system-generated identifier can obtain sensitive information; limited to AWV functionality.
- CVE-2026-133323 (MTLVULN-1864): Blind command injection in AWV, rated critical; unauthenticated, with potential impact on integrity and availability.
- CVE-2026-133324 (MTLVULN-1877): Authentication bypass in AWV, rated medium; unauthenticated attacker can bypass authentication and perform unauthorised actions within the application.
- Advisory MISA-2026-0012 (last updated 24 November 2026) states: 'Exploiting these vulnerabilities together can significantly amplify their impact.' A patch for release 10.3 is available.

Things people will get wrong

- A CVSS 5.3 medium score means this can wait until the next scheduled patch cycle. The vendor's advisory notes that exploiting this flaw alongside the companion flaws in the same release significantly amplifies the impact. Two of those companion flaws are rated critical by the vendor, and both are reachable without authentication.

- Disabling the AWV conferencing component removes the risk and avoids the need to patch. The record and the vendor's advisory do not describe disabling AWV as an accepted workaround. The vendor's advisory recommends applying the patch.

How we would triage it

This is our judgement.

Step 1: Find the MiCollab version you run

- Log in to the MiCollab administration console and check the version displayed. The record identifies all versions up to and including 10.3 (10.3.0.18) as affected.
- Confirm with your IT provider whether more than one MiCollab server is in use, as each must be checked separately.

Step 2: Check whether AWV is enabled and who can reach it

- In the MiCollab admin console, check whether the Audio, Web and Video Conferencing (AWV) component is enabled.
- Confirm whether AWV endpoints are reachable from outside your network; internet-facing instances carry the highest exposure.

Step 3: Apply the vendor patch for MiCollab release 10.3

- The vendor's advisory (MISA-2026-0012) states a patch is available for release 10.3. Obtain it from Mitel support and apply it before 28 November 2026.
- The same patch addresses four companion flaws including two the vendor rates as critical: CVE-2026-133303 and CVE-2026-133323.

Step 4: Confirm the patched version is running

- After patching, log in to the MiCollab admin console and verify the version shown matches the patched release confirmed by Mitel support.
- Obtain written confirmation from your IT provider of the version installed and the date 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 are writing about CVE-2026-133275, an arbitrary file upload vulnerability in Mitel MiCollab affecting version 10.3 (10.3.0.18) and earlier. The remediation deadline is 28 November 2026. We need to know: (1) whether we run Mitel MiCollab, and if so, on which version; (2) whether the Audio, Web and Video Conferencing (AWV) component is enabled; and (3) whether the vendor patch for release 10.3 has been applied. The same patch also covers two companion flaws the vendor rates as critical (CVE-2026-133303 and CVE-2026-133323). Please confirm in writing the version installed, whether the patch is in place, and the date it was applied.*

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 with unusual extensions appearing in directories associated with the AWV conferencing component, particularly those created during any period of untrusted external access.
- HTTP POST requests in web server access logs directed at AWV component endpoints from addresses outside normal user ranges, especially those transferring file content.
- New or modified files in AWV component directories with timestamps that fall outside expected maintenance or conferencing activity windows.

The weakness behind it

The record classes this as CWE-434 (Unrestricted Upload of File with Dangerous Type).

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 conferencing component is a web-facing service; the flaw would likely serve as an initial foothold by exploiting a public-facing application endpoint that requires no authentication.
Ingress Tool Transfer (T1105): Downloading more attacker tools onto the machine.	Command and Control: talking to the attacker	Uploading arbitrary files to the target system would likely be used to transfer attacker tools for follow-on activity, as the record confirms files land on the target system.

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 an unrestricted upload of file with dangerous type vulnerability in the Audio, Web and Video Conferencing (AWV) component due to insufficient file type validation that could allow an unauthenticated attacker to upload arbitrary files.*

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 arbitrary file upload attack due to insufficient file type validation. A successful exploit could allow an attacker to upload arbitrary files to the target system. This is MTLVULN-1861.*

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-2026-133275
```

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-2026-133275
```

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 advisory text does not state the specific patch version identifier; contact Mitel support to confirm the exact build number before and after patching.
- Whether versions earlier than 10.3 receive a separate patch, or are end-of-life and ineligible, is not stated in the available advisory text.
- The record does not describe where uploaded files are stored on the server or whether they can be executed directly after upload.
- Whether disabling the AWV component is an accepted temporary workaround for environments that cannot patch immediately is not stated in the advisory.

- 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", "Why it matters", "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-2026-133275: 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 AWV component reachable from the internet, running version 10.3 or earlier, unpatched.	High	Before 28 November 2026
MiCollab AWV reachable only from internal networks, version 10.3 or earlier, unpatched.	Medium	Before 28 November 2026
MiCollab installed on version 10.3 or earlier but AWV conferencing component not in active use.	Medium	Before 28 November 2026

MiCollab version 10.3 or earlier with patching already scheduled but not yet complete.	Medium	Complete before 28 November 2026
MiCollab not installed, or confirmed patched version already running.	None	None 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-2026-133275: https://www.cve.org/CVERecord?id=CVE-2026-133275
- 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