contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Mitel MiCollab exploited

CVE-2026-133303 · on CISA's exploited list since 25 November 2026

Analysis Report

Anyone running Mitel MiCollab through version 10.3 (10.3.0.18) must apply the vendor's patch immediately — CISA's deadline is 28 November 2026, two days away. Check whether the AWV component is …

PREPARED BY	NamiQ	DATE	26 November 2026
FACTS AS OF	26 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.8**	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-2026-133303

The bottom line

> *Anyone running Mitel MiCollab through version 10.3 (10.3.0.18) must apply the vendor's patch immediately — CISA's deadline is 28 November 2026, two days away. Check whether the AWV component is active; if it faces the internet, treat this as urgent now.*

At a glance

Fact	Detail
Product	Mitel MiCollab (CVE-2026-133303)
Severity	Critical: 9.8 (CVSS 3.1)
CISA	On its exploited list since 25 November 2026. Deadline for US federal agencies: 28 November 2026.
Chance of exploitation (EPSS)	0.01, 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 a patch is available for release 10.3. The exact patched build number is not in the available source text; contact Mitel or your reseller for the specific package.
Who looks first	Any organisation running Mitel MiCollab through version 10.3 (10.3.0.18) with the Audio, Web and Video Conferencing (AWV) component active. The record places no restriction on deployment type.

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 organisation?	Nothing to do for this CVE.	Check the version.
Is your MiCollab version 10.3 (10.3.0.18) or earlier?	Nothing to do for this CVE.	Check whether the AWV component is active.
Is the Audio, Web and Video Conferencing (AWV) component active?	Lower immediate risk; still apply the patch this cycle.	Check who can reach it.

Can users outside your organisation reach the AWV component directly?	Patch this week; treat as medium priority.	Patch before 28 November 2026 — CISA deadline.

What it is

The record says an unauthenticated attacker can inject XML through the AWV component using pre-staged malicious content, allowing arbitrary commands to run on the system, with potential impact on its confidentiality, integrity, and availability.

Why it matters

A CVSS score of 9.8 reflects that no login is required. The pre-staged content condition in the record is less limiting than it appears: the same advisory lists CVE-2026-133275, an unauthenticated arbitrary file upload flaw in the same AWV component, rated medium. The vendor's advisory states that exploiting these vulnerabilities together can significantly amplify their impact. Our reading is that an attacker may use the file upload flaw to stage the content this flaw then executes, reducing the practical barrier substantially when AWV faces the internet.

What the vendor's advisory says

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

- The vendor's advisory (MISA-2026-0012, updated 24 November 2026) covers five flaws in the AWV component. CVE-2026-133275 (MTLVULN-1861, medium): unauthenticated arbitrary file upload due to insufficient file type validation.
- CVE-2026-133311 (MTLVULN-1863, medium): unauthenticated unauthorized access via a system-generated random identifier or pre-staged content; the advisory says it does not provide unrestricted access to arbitrary files elsewhere on the system.
- CVE-2026-133323 (MTLVULN-1864, critical): unauthenticated blind command injection due to insufficient parameter sanitisation, with impacts to integrity and availability.
- CVE-2026-133324 (MTLVULN-1877, medium): unauthenticated authentication bypass due to improper handling of authentication, allowing unauthorised actions within the application.
- The advisory states: 'Exploiting these vulnerabilities together can significantly amplify their impact.' A patch is available for release 10.3 and covers all five flaws.

Things people will get wrong

- Pre-staged content means an outsider cannot exploit this without prior access. The same advisory lists CVE-2026-133275, an unauthenticated file upload flaw in the same AWV component. The vendor notes that chaining the flaws amplifies impact, so an external attacker may stage content via the upload flaw.

How we would triage it

This is our judgement.

Step 1: Find the MiCollab version you run

- Ask your Mitel administrator to confirm the installed MiCollab version. The record says all versions through 10.3 (10.3.0.18) are affected.
- Confirm whether the Audio, Web and Video Conferencing (AWV) component is active and licensed in your deployment.

Step 2: Check who can reach the AWV component

- Determine whether AWV is reachable from outside your organisation. If it is, the CISA deadline of 28 November 2026 applies directly.
- If AWV cannot be restricted temporarily while the patch is obtained, record this and escalate to your IT provider immediately.

Step 3: Apply the vendor's patch

- The vendor's advisory (MISA-2026-0012) says a patch is available for release 10.3. Contact Mitel support or your reseller to obtain and apply it before 28 November 2026.
- The patch covers all five AWV flaws in the advisory, including CVE-2026-133275, CVE-2026-133311, CVE-2026-133323, and CVE-2026-133324.

Step 4: Review logs if AWV was internet-facing before patching

- Look for unexpected files deposited in AWV directories before the patch was applied.
- Look for unusual processes or commands spawned from the AWV service account following XML requests.

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 need urgent help with a critical security vulnerability in our Mitel MiCollab system. CVE-2026-133303 is an XML injection flaw in the Audio, Web and Video Conferencing (AWV) component that allows an unauthenticated attacker to run arbitrary commands on the system. It affects all versions through 10.3 (10.3.0.18), and CISA has set a remediation deadline of 28 November 2026. Mitel's advisory (MISA-2026-0012) says a patch is available for release 10.3. Please confirm whether we run this product, which version is installed, and whether AWV is active and reachable externally. We need written confirmation of the installed version and that the patch has been applied 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:

- Unexpected files or new content in AWV component directories deposited around the period the system was internet-facing before patching.
- Unusual processes or system commands spawned from the AWV service account following XML input processing.

The weakness behind it

The record classes this as CWE-91 (XML Injection).

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 public-facing web application requiring no credentials. The record describes network exploitation without authentication, which would typically align with this technique.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	The record states that a successful exploit executes arbitrary commands on the system. Command execution via the host interpreter would likely follow a successful injection.

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 XML injection vulnerability in its Audio, Web, and Video Conferencing (AWV) component that could allow an unauthenticated attacker to execute arbitrary commands using pre-staged malicious 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 to leverage pre-staged malicious content to conduct an XML injection attack due to insufficient parameter validation. A successful exploit could allow an attacker to execute arbitrary commands within the context of the system. This is MTLVULN-1862.*

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-2026-133303
```

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-2026-133303
```

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 source text ends before specifying the exact patched build number for release 10.3; contact Mitel or your reseller for the specific package to install.
- The record does not state whether pre-staged content must originate from a prior authenticated session or whether the unauthenticated file upload flaw alone is sufficient to stage it.
- No workaround short of applying the patch is stated in the available source text.
- 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-2026-133303: score 9, `CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/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	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	Changed	Damage reaches beyond 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
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 with AWV active and accessible from the internet, version 10.3 or earlier	High	Before 28 November 2026
MiCollab with AWV on internal network only, version 10.3 or earlier	Medium	This week
MiCollab version not yet confirmed, AWV status unknown	Medium	Confirm version today

MiCollab running but AWV component not active, version 10.3 or earlier	Low	Next scheduled patch cycle
Not running Mitel MiCollab	None	No action needed 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-2026-133303: https://www.cve.org/CVERecord?id=CVE-2026-133303
- 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