contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Mitel MiCollab exploited

CVE-2026-133323 · on CISA's exploited list since 25 November 2026

Analysis Report

Anyone running Mitel MiCollab on version 10.3 (10.3.0.18) or earlier must apply the vendor's patch before 28 November 2026 — CISA's deadline is three days away. No login is needed to exploit this …

PREPARED BY	NamiQ	DATE	26 November 2026
FACTS AS OF	26 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 10.0**	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-2026-133323

The bottom line

> *Anyone running Mitel MiCollab on version 10.3 (10.3.0.18) or earlier must apply the vendor's patch before 28 November 2026 — CISA's deadline is three days away. No login is needed to exploit this flaw; apply the patch immediately and isolate any internet-facing deployment until it is in place.*

At a glance

Fact	Detail
Product	Mitel MiCollab (CVE-2026-133323)
Severity	Critical: 10 (CVSS 3.1)
CISA	On its exploited list since 25 November 2026. Deadline for US federal agencies: 28 November 2026.
Chance of exploitation (EPSS)	0.03, 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	Vendor patch for MiCollab 10.3 (10.3.0.18); the advisory instructs upgrading to that release and applying the patch. The source text is truncated before the full steps; no higher version number is named.
Who looks first	Administrators of Mitel MiCollab on any version up to and including 10.3 (10.3.0.18). Any installation where the AWV component is reachable over a network is directly in scope.

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 which version is installed (next question).
Is your MiCollab version 10.3 (10.3.0.18) or earlier?	Confirm with Mitel whether later versions are covered; review the advisory.	Apply the vendor's patch without delay.
Is the AWV (Audio, Web, and Video Conferencing) component enabled?	Exposure is lower, but the patch still applies within CISA's window.	Check whether untrusted users can reach it from outside your network.

Can untrusted users reach the AWV interface from outside your network?	Internal exposure remains; apply the patch within CISA's window.	Treat as urgent — isolate the interface if the patch cannot be applied immediately.

What it is

The flaw is in MiCollab's Audio, Web, and Video Conferencing (AWV) component. The record says an unauthenticated attacker can inject operating-system commands through unsanitised parameters. A successful exploit lets the attacker run arbitrary commands within the context of the system.

What the vendor's advisory says

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

- MTLVULN-1862: XML injection in AWV, rated critical by Mitel. An unauthenticated attacker could execute arbitrary commands via pre-staged malicious content, affecting confidentiality, integrity, and availability.
- MTLVULN-1877: authentication bypass in AWV, rated medium by Mitel. An unauthenticated attacker could bypass authentication controls and perform unauthorised actions within the application.
- MTLVULN-1861: arbitrary file upload in AWV, rated medium by Mitel. An unauthenticated attacker could upload arbitrary files due to insufficient file type validation.
- MTLVULN-1863: unauthorised access in AWV, rated medium by Mitel. With knowledge of a system-generated random identifier, an unauthenticated attacker could obtain sensitive information.
- The vendor's advisory says the patch for MiCollab 10.3 (10.3.0.18) addresses all five flaws and notes that exploiting them together can significantly amplify their impact.

Things people will get wrong

- Running version 10.3 (10.3.0.18) means we are already protected. The vendor's advisory says version 10.3 (10.3.0.18) is affected and the fix is a separate patch applied on top of that release. The version number alone does not confirm the patch is in place.
- The flaw only affects the conferencing feature, not the broader system. The record says a successful exploit allows the attacker to execute arbitrary commands within the context of the system, not only within the conferencing component.

How we would triage it

This is our judgement.

Step 1: Find the MiCollab version you run

- Log in to the MiCollab administration interface and check the installed build number. The affected range is all versions up to and including 10.3 (10.3.0.18).

Step 2: Check whether AWV is active and reachable from outside

- Confirm whether the Audio, Web, and Video Conferencing component is enabled in the MiCollab configuration.
- Check whether its interface is accessible from outside your internal network. No login is needed to reach the vulnerable parameter, so an internet-facing AWV raises the urgency.

Step 3: Apply the vendor's patch

- The vendor's advisory says a patch is available for MiCollab 10.3 (10.3.0.18). Follow Mitel's instructions to upgrade to that release and apply the patch.
- Confirm the installed build number after patching to verify the fix is in place. The advisory text is truncated and does not state a post-patch build number.

Step 4: Check for signs of compromise if the system was exposed

- Review system process logs for unexpected commands or shells launched by the MiCollab AWV service process.
- Look for new files, changed permissions, or new user accounts created at times that do not match normal administrative activity on the MiCollab host.

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 a critical vulnerability in Mitel MiCollab, CVE-2026-133323. The flaw is in the Audio, Web, and Video Conferencing component and allows an unauthenticated attacker to run arbitrary system commands. All versions up to and including 10.3 (10.3.0.18) are affected. The vendor has released a patch for release 10.3 (10.3.0.18). CISA requires the fix to be applied by 28 November 2026. Please confirm whether we run MiCollab, on which version, whether AWV is enabled and internet-facing, and provide written confirmation of the build number after the patch is applied. We would like this confirmation 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 processes — particularly shells or scripting interpreters — spawned by the MiCollab AWV service, visible in system or application process logs.
- Outbound network connections from the MiCollab host to addresses outside its normal traffic pattern, which may indicate post-exploitation activity.
- New user accounts or changed file permissions on the MiCollab host created at times that do not correspond to known administrative actions.

The weakness behind it

The record classes this as CWE-78 (Improper Neutralization of Special Elements used in an OS Command).

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 network-facing and requires no authentication; a parameter injection flaw reachable over the network would typically be exploited as a public-facing application.
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 flaw directly enables arbitrary OS command execution on the system; a successful exploit would likely invoke a command interpreter, as CWE-78 describes.

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 improper neutralization of special elements used in an OS command (OS command injection) vulnerability in its Audio, Web, and Video Conferencing (AWV) component that could allow an unauthenticated attacker to execute arbitrary system commands.*

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 a blind command injection attack due to insufficient parameter sanitization. A successful exploit could allow an attacker to execute arbitrary commands within the context of the system. This is MTLVULN-1864.*

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-2026-133323
```

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-2026-133323
```

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 is truncated; the full patch installation steps and any post-patch build identifier are not stated in the available source.
- The system account under which injected commands run is not stated in the record or the advisory excerpt.
- No workaround short of patching is described in the available advisory text.
- It is not stated whether the AWV component can be disabled temporarily as a risk reduction measure while the patch is arranged.

- 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-2026-133323: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/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	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	Changed	Damage reaches beyond the vulnerable component.
Confidentiality	None	No data exposed.
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 reachable from the internet, version 10.3 (10.3.0.18) or earlier, unpatched	High	Before 28 November 2026
MiCollab on an internal network only, version 10.3 (10.3.0.18) or earlier, unpatched	High	Before 28 November 2026
MiCollab patched but AWV internet exposure not yet reviewed or confirmed	Medium	This week

MiCollab version not confirmed after patching — patch may not be in place	Medium	This week
No Mitel MiCollab in the estate	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-2026-133323: https://www.cve.org/CVERecord?id=CVE-2026-133323
- 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