contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Mitel MiCollab: new CVE

CVE-2026-133323 · record published 19 November 2026

Analysis Report

Anyone running Mitel MiCollab should act now; if you do not run it, you can stop reading. First find out whether the Audio, Web and Video Conferencing component is in use and on which version, so you …

PREPARED BY	NamiQ	DATE	20 November 2026
FACTS AS OF	20 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 10.0**	STATUS	Not on CISA's exploited list; exploitation not recorded

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 should act now; if you do not run it, you can stop reading. First find out whether the Audio, Web and Video Conferencing component is in use and on which version, so you can plan the vendor's patch.*

At a glance

Fact	Detail
Product	Mitel MiCollab (CVE-2026-133323)
Severity	Critical: 10 (CVSS 3.1)
Status	A new CVE record, published by Mitre on 19 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 20 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	The vendor's advisory says a patch is available for release 10.3 (10.3.0.18) that addresses this flaw; upgrade to that release and apply the patch. No higher fixed build is named.
Who looks first	Anyone running Mitel MiCollab at version 10.3 (10.3.0.18) or earlier, above all where the Audio, Web and Video Conferencing component is reachable. Your IT provider or phone-system supplier should check first.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Mitel MiCollab anywhere?	Nothing to do for this CVE.	Check the version and component next.
Is your MiCollab at 10.3 (10.3.0.18) or earlier?	Confirm with your supplier; no newer fixed build is named.	It is in range; keep going.
Is the Audio, Web and Video Conferencing component enabled?	Lower risk; still apply the vendor patch.	Check who can reach it next.
Can untrusted users reach that component over the network?	Patch at your next window.	Treat as urgent; restrict access and patch.

What it is

The record says an unauthenticated attacker who can reach the Audio, Web and Video Conferencing component can send crafted input that the system then runs as commands. It is blind command injection, so the attacker need not see any output to run those commands.

What the vendor's advisory says

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

- Mitel's advisory MISA-2026-0012, dated 16 November 2026, covers five flaws in the Audio, Web and Video Conferencing component and says a patch for release 10.3 (10.3.0.18) addresses them.
- Beside this command injection, the advisory lists an XML injection flaw (MTLVULN-1862), also unauthenticated and rated critical, that it says can run arbitrary commands.
- It also lists an unauthenticated arbitrary file upload (MTLVULN-1861, medium) and an authentication bypass (MTLVULN-1877, medium).
- It lists an unauthorized access flaw (MTLVULN-1863, medium) that it says can expose sensitive information to an attacker who knows a system-generated identifier or pre-staged content.
- The advisory says exploiting these vulnerabilities together can significantly amplify their impact.

Things people will get wrong

- We are safe because it is not on CISA's exploited list. The record gives it the top score and needs no login; absence from the list means not-yet-seen, not low risk.
- Only the newest version is at risk. The record says all versions up to and including 10.3 (10.3.0.18) are affected, so older ones are included, not exempt.
- We can just turn conferencing off instead of patching. The advisory names no workaround and says to apply the patch; the sources do not confirm that disabling the component removes the risk.

How we would triage it

This is our judgement.

Step 1: Find the versions you run

- Ask your supplier or check your system for every MiCollab install, its version, and whether the Audio, Web and Video Conferencing component is enabled, because the flaw is in that component.

- Note any install at 10.3 (10.3.0.18) or earlier, since the record says all those versions are affected.

Step 2: Reduce exposure

- Where the conferencing component can be reached from the internet or by untrusted users, restrict that access until the patch is applied, because the flaw needs no login to use.

Step 3: Apply the vendor patch

- Apply the patch the advisory says is available for release 10.3 (10.3.0.18), as that is the fix the vendor names for this flaw.

Step 4: Confirm the fix

- Get written confirmation from whoever runs the system of the version in use and that the patch has been applied, so you have evidence the fix is in place.

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.

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.

> *Hello, we need your help with a security issue. Please tell us whether we run Mitel MiCollab anywhere and, if so, at which version, and whether the Audio, Web and Video Conferencing component is enabled and reachable from outside. There is a flaw with the top severity score, CVE-2026-133323, in that component; the vendor's advisory of 16 November 2026 says a patch is available for release 10.3 (10.3.0.18) that fixes it. Versions up to and including 10.3 (10.3.0.18) are affected. Please confirm to us in writing which version we run and that the patch has been applied, within a week. Thank you.*

The weakness behind it

The record classes this as CWE-78.

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 record says the flaw is in a network-reachable conferencing component and needs no login, so it would likely be used to gain a first foothold on an exposed server.
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 says a successful exploit runs arbitrary commands within the system context, which points to driving the host's own command interpreter.

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

The CVE record:

> *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)

The record gives no version ranges. Use the vendor's advisory for the affected versions.

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 we have is truncated and gives no patch identifier or the exact steps to apply it.
- The sources do not say whether this flaw has been seen used against anyone.
- The sources do not confirm whether disabling the conferencing component blocks the flaw as an interim measure.
- Exploitation is not recorded. That is not the same as none.
- This is a new record: scores, versions and wording can change in the first days, and they are as at 20 November 2026. We read the vendor pages listed under Sources; nothing here has been tested.
- 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.

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.

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 the conferencing component reachable from the internet at an affected version	High	this week
MiCollab reachable only from inside your own network	Medium	this week
MiCollab run but the conferencing component disabled	Low	next patch cycle
You do not run Mitel MiCollab	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 fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

Sources

- CVE record for CVE-2026-133323: https://www.cve.org/CVERecord?id=CVE-2026-133323
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- 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