Mitel MiCollab AWV flaw allows unauthenticated authentication bypass (CVE-2026-133324)



CISA lists CVE-2026-133324, a fail-open flaw in the Audio, Web and Video Conferencing component of Mitel MiCollab that lets an unauthenticated attacker bypass authentication. Apply vendor mitigations and review internet exposure.

- CVE-2026-133324 affects the Audio, Web and Video Conferencing (AWV) component of Mitel MiCollab.
- The weakness is a failure to fail securely, so an unauthenticated attacker could bypass authentication controls.
- A successful attacker could perform unauthorized actions.
- CISA requires mitigations per vendor instructions, with a federal due date of 2026-11-28.
- If no mitigation is available, CISA's guidance is to discontinue use of the product.

CISA has listed CVE-2026-133324, a vulnerability in Mitel MiCollab, a collaboration platform. The flaw sits in the Audio, Web and Video Conferencing (AWV) component and is described as a failure to fail securely.

What the flaw allows

An unauthenticated attacker could bypass authentication controls and perform unauthorized actions. No credentials are needed, so exposure depends largely on whether the component can be reached from the internet. The source does not describe which actions are possible, nor does it mention exploitation details or affected versions, so refer to the vendor's advisory for those.

What CISA requires

CISA asks for mitigations to be applied in line with vendor instructions, together with its BOD 26-04 guidance on prioritizing security updates based on risk and its forensics triage requirements. For cloud services, the applicable BOD 26-04 guidance should be followed. Where mitigations are not available, the product should no longer be used. Stakeholders are responsible for assessing each asset's internet exposure. The federal due date is 2026-11-28; this binds US federal agencies, but it is a useful benchmark for other organizations.

Practical view

Institutions running MiCollab should first confirm whether AWV is deployed and exposed externally, then follow the vendor's mitigation steps. Because authentication bypass may leave little trace, a review of access records is sensible after mitigation.

What to do now

1. Inventory all Mitel MiCollab instances and confirm whether the AWV component is deployed.
2. Identify which instances are reachable from the internet and prioritize them.
3. Apply the vendor's mitigations and record the change under your change-management process.
4. Review access and administrative logs on affected systems for unexpected activity.
5. Where no mitigation exists, plan to restrict access or retire the product, and report to the relevant risk owner.