CISA flags weak authentication flaw in Mitel MiCollab conferencing component



CISA lists CVE-2026-133311, a weak authentication flaw in the conferencing component of Mitel MiCollab that may let an unauthenticated attacker read sensitive information. Vendor mitigations should be applied.

- CVE-2026-133311 is a weak authentication vulnerability in the Audio, Web and Video Conferencing (AWV) component of Mitel MiCollab.
- An unauthenticated attacker could access sensitive information using a system-generated random identifier or pre-staged content.
- CISA requires mitigation per vendor instructions, in line with BOD 26-04 and its Forensics Triage Requirements.
- If mitigations are unavailable, CISA's guidance is to discontinue use of the product.

> - The federal due date is 2026-12-09; asset owners must assess each asset's internet exposure.

CISA has added CVE-2026-133311 to its guidance. The issue is a weak authentication vulnerability in the Audio, Web and Video Conferencing (AWV) component of Mitel MiCollab.

What the flaw allows

According to the source, an unauthenticated attacker could reach sensitive information by using a specific system-generated random identifier or pre-staged content. No further technical detail is given, and the source does not describe the type of information exposed or any observed attacks.

What CISA requires

CISA directs affected organisations to apply mitigations according to the vendor's instructions, consistent with its BOD 26-04 guidance on prioritising security updates by 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. Asset owners are responsible for judging each asset's internet exposure and for meeting the patching expectations. The federal due date is 2026-12-09.

These requirements bind US federal agencies, but they are a useful benchmark for Saudi institutions that run MiCollab, particularly where conferencing services are reachable from the internet.

Recommended approach

Confirm whether MiCollab with the AWV component is deployed, establish which instances are internet-facing, and follow the vendor's mitigation instructions. Keep a record of the decisions and dates for audit purposes.

What to do now

1. Inventory all Mitel MiCollab deployments and confirm whether the AWV component is in use.
2. Identify which instances are reachable from the internet and prioritise them.
3. Apply the vendor's mitigation instructions for CVE-2026-133311.
4. Plan to retire or isolate any instance for which no mitigation is available.
5. Review access and activity records on exposed instances for signs of unauthorised access, and document the outcome.