CISA flags Mitel MiCollab file upload flaw (CVE-2026-133275)



CISA lists CVE-2026-133275, an unrestricted file upload flaw in the AWV conferencing component of Mitel MiCollab that an unauthenticated attacker could abuse. Apply vendor mitigations and assess internet exposure.

- The flaw is an unrestricted upload of a file with a dangerous type, caused by insufficient file type validation.
- It affects the Audio, Web and Video Conferencing (AWV) component of Mitel MiCollab.
- An unauthenticated attacker could upload arbitrary files.
- CISA requires mitigations per vendor instructions, plus its BOD 26-04 guidance and forensics triage requirements.
- The federal due date is 2026-11-28; if mitigations are unavailable, CISA says to stop using the

> product.

CISA has added CVE-2026-133275 to its catalogue, describing an unrestricted file upload vulnerability in Mitel MiCollab. The issue sits in the Audio, Web and Video Conferencing (AWV) component, where file type validation is insufficient.

What the flaw allows

An unauthenticated attacker could upload arbitrary files to an affected system. Because no credentials are needed, exposure depends largely on whether the AWV component can be reached from the internet. The source does not provide details on exploitation, affected versions or patch numbers, so those should be confirmed directly with the vendor.

What CISA requires

CISA's required action is to apply mitigations in line with the vendor's instructions and to follow its BOD 26-04 guidance on prioritizing security updates based on risk, together with its forensics triage requirements. For cloud services, the applicable BOD 26-04 guidance should be followed. Where mitigations are not available, CISA says use of the product should be discontinued. Stakeholders are responsible for evaluating the internet exposure of each asset. The federal due date is 2026-11-28.

Although these deadlines apply to US federal agencies, they are a useful benchmark for Saudi institutions that run MiCollab for internal or customer-facing conferencing. Collaboration platforms often sit at the network edge, so confirming where they are deployed is a sensible first step.

Practical approach

Treat this as a prioritized patching item for any internet-facing MiCollab instance, and preserve evidence before and during remediation so that any prior misuse can be investigated.

What to do now

1. Inventory all Mitel MiCollab deployments and identify which expose the AWV component to the internet.
2. Contact Mitel for the applicable mitigation or fix and apply it on a prioritized timeline.
3. Restrict external access to AWV through firewall or reverse proxy rules until mitigation is confirmed.
4. Preserve logs and file system evidence, and review for unexpected uploaded files before and after remediation.
5. If no mitigation is available, plan to take the product out of service, following CISA's guidance.
6. Record the exposure assessment and remediation under your vulnerability management process.