CISA flags Mitel MiCollab OS command injection flaw (CVE-2026-133323)



CISA lists CVE-2026-133323, an OS command injection flaw in the Audio, Web and Video Conferencing component of Mitel MiCollab that an unauthenticated attacker could use to run arbitrary system commands.

- The flaw is an OS command injection issue in the AWV component of Mitel MiCollab.
- An unauthenticated attacker could execute arbitrary system commands.
- CISA requires mitigation per vendor instructions, alongside BOD 26-04 and its Forensics Triage Requirements.
- If mitigations are unavailable, CISA says to discontinue use of the product.
- The federal due date is 2026-11-28.

CISA has published an entry for CVE-2026-133323, an OS command injection vulnerability in Mitel MiCollab. The weakness sits in the Audio, Web, and Video Conferencing (AWV) component and stems from improper neutralization of special elements in commands passed to the operating system.

What the source says

According to the entry, an unauthenticated attacker could exploit the flaw to execute arbitrary system commands. No prior access or credentials are described as necessary.

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, as well as its Forensics Triage Requirements. Where mitigations are not available, organisations should follow the BOD 26-04 guidance for cloud services or stop using the product. Stakeholders are expected to assess each asset's internet exposure themselves. The federal due date is 2026-11-28.

What this means for Saudi institutions

The CISA deadline binds US federal agencies, but the exposure applies to any organisation running MiCollab. Collaboration platforms are often reachable from the internet, so confirming where AWV is deployed and how it is exposed is the sensible first step. The source gives no details on affected versions or patches, so the vendor's advisory remains the reference for those.

What to do now

1. Inventory all Mitel MiCollab instances and identify where the AWV component is deployed.
2. Check which instances are reachable from the internet and prioritise them.
3. Apply the mitigations in Mitel's instructions as soon as possible.
4. Review logs and systems on exposed instances for signs of compromise, following forensic triage practice.
5. If no mitigation is available, plan to restrict access or retire the affected product.
6. Record the exposure and remediation in your vulnerability and risk registers.