Mitel MiCollab zero-days exploited in data theft campaign, with signs of AI assistance



Accenture's Apex Labs says five MiCollab flaws were exploited before Mitel's patches. CISA added all five to its KEV catalog. Organizations should patch and check for signs of prior compromise.

- Five MiCollab vulnerabilities (CVE-2026-133275, -133303, -133311, -133323, -133324) can be exploited without authentication; two critical ones allow command execution.
- Accenture found exploitation before Mitel's advisory; a web shell was deployed on November 15.
- In one case, attackers ran commands 12 minutes after their first request, gained root within half an hour, and reached backup and database servers after about 20 hours.
- The attacker infrastructure contacted two commercial AI API services, though Accenture could not say exactly how they were used.

> - CISA added all five flaws to KEV; Mitel's advisory does not mention exploitation in the wild.

Accenture's Apex Labs reports that threat actors exploited several Mitel MiCollab vulnerabilities as zero-days in a data theft campaign. CISA has since added five MiCollab flaws to its Known Exploited Vulnerabilities (KEV) catalog.

What was observed

Mitel announced patches on November 16 for five flaws in the product's audio, web and video conferencing component: arbitrary file upload, XML injection, unauthorized access, command injection and authentication bypass. All can be exploited by unauthenticated attackers, and two critical bugs allow arbitrary command execution. They are tracked as CVE-2026-133275, CVE-2026-133303, CVE-2026-133311, CVE-2026-133323 and CVE-2026-133324.

Accenture found evidence of exploitation before Mitel's advisory, including a web shell deployed on a victim's systems on November 15. In that case, commands ran on the MiCollab server 12 minutes after the first request and root access followed within half an hour. The attackers harvested more credentials and, about 20 hours in, reached internal backup and database servers. Accenture says the product's frequent internet exposure and Active Directory integration make it an attractive target.

AI involvement and wider impact

The attacker's infrastructure communicated with two unnamed commercial AI API services. Because the telemetry is sampled, Accenture cannot say how they were used, but the activity fits data triage, support for exploitation or web-shell work, and preparing extortion material. A second victim's server had contacted the same infrastructure since November 9, but how it was compromised is unclear because older vulnerabilities also affected it. No known group has been linked, and the campaign may be extortion-driven.

Mitel's advisory, last updated November 24, does not mention exploitation in the wild. CISA set deadlines of November 28 for four of the flaws and December 9 for the fifth.

Why it matters

Patching alone may not be enough: servers could have been compromised before fixes were applied, and a foothold on MiCollab can lead quickly to identity and backup systems.

What to do now

1. Identify all MiCollab instances, especially internet-facing ones, and apply Mitel's patches for the five CVEs without delay.
2. Hunt for indicators of compromise on MiCollab servers, including web shells and unexpected outbound connections, treating servers patched late as possibly already compromised.

3. If compromise is suspected, rotate credentials, including Active Directory accounts reachable from MiCollab, and review activity on backup and database servers.
4. Restrict internet exposure of MiCollab management and conferencing interfaces where business needs allow.
5. Include the case in incident-response planning: prepare for extortion scenarios and notify your regulator as required if data was affected.