AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-133303

Befehlsausführung per XML-Injection in Mitel MiCollab (Konferenzkomponente AWV).

MiCollab ist die Kollaborations- und Konferenzplattform zu Mitel-Telefonanlagen und steht für Webkonferenzen häufig direkt im Internet. In der Konferenzkomponente AWV kann ein Angreifer ohne Anmeldung über vorab platzierte Inhalte eine XML-Injection auslösen und so Befehle im Systemkontext ausführen. Mitel hat am 16.11.2026 einen Patch für 10.3.0.18 veröffentlicht; die CISA führt die Lücke seit dem 25.11.2026 als aktiv ausgenutzt.

> **Geschäftsrisiko:** Übernahme des MiCollab-Servers in der DMZ mit Zugriff auf Konferenz-, Kontakt- und Kommunikationsdaten, einem Brückenkopf ins interne Netz und einem möglicherweise meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

9,0 / 10

KRITISCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | Hoch | Kritisch

`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H` – aus dem Netz, ohne Anmeldung, ohne Mitwirkung eines Nutzers, mit erhöhter Angriffskomplexität (vorab platzierte Inhalte nötig) und Wirkung über die Komponente hinaus. Basiswert laut Hersteller Mitel (MISA-2026-0012); das NVD bewertet abweichend mit 9,8.

AUSNUTZUNG BELEGT SEIT
25.11.2026 (Aufnahme in CISA KEV)

BETROFFEN
Mitel MiCollab 10.3 (10.3.0.18) und älter
Komponente Audio, Web and Video Conferencing (AWV)

HANDLUNGSBEDARF
Notfall-Change – sofort patchen oder AWV von außen sperren

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,0 · KRITISCH
CVSS-Schweregrad laut Mitel

Ohne Anmeldung
XML-Injection in AWV · CWE-91

Aktiv ausgenutzt
CISA KEV seit 25.11.2026

Patch für 10.3.0.18
laut MISA-2026-0012 (KB000129195)

Die Ursache: Die Komponente **Audio, Web and Video Conferencing (AWV)** von MiCollab prüft einen Parameter nicht ausreichend, bevor er in XML-Daten übernommen wird (**CWE-91, XML Injection**). Mit vorab auf dem System platzierten Inhalten kann ein Angreifer ohne Anmeldung die Verarbeitung so manipulieren, dass **beliebige Befehle im Systemkontext** ausgeführt werden. Die nötigen Inhalte lassen sich über eine weitere Lücke desselben Advisories einbringen: `CVE-2026-133275` erlaubt den Upload von Dateien ohne Anmeldung. Mitel warnt ausdrücklich, dass die Kombination der fünf AWV-Lücken die Wirkung deutlich verstärkt; die schwerste ist die Command Injection `CVE-2026-133323`.

ANGRIFFSKETTE

01	02	03	04
AWV erreichbar – MiCollab-Konferenzportal antwortet aus dem Internet	**Inhalte platzieren** – z. B. über den Datei-Upload ohne Anmeldung (CVE-2026-133275)	**XML-Injection** – manipulierter Parameter löst die Verarbeitung der Inhalte aus	**Befehlsausführung** – Befehle im Systemkontext, Brückenkopf ins interne Netz

Betroffenheit & Fixversionen

MiCollab-Version	Verwundbar bis	Fixversion (Ziel)
MiCollab 10.3	`10.3.0.18 und älter`	Patch laut KB000129195
Spätere MiCollab-Releases	nicht betroffen (Fix enthalten)	—

Angaben laut Mitel Product Security Advisory MISA-2026-0012 (16.11.2026, Revision 2.0 vom 24.11.2026). Das Advisory deckt nur unterstützte Versionen ab; ältere, nicht mehr unterstützte Stände sind als betroffen anzusehen. Übergangsweise empfiehlt Mitel, den externen Zugriff auf die AWV-Komponente zu sperren. **Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.**

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf den Kommunikationsserver kann eine meldepflichtige Verletzung darstellen; DSGVO unverzüglich (i. d. R. 72 h), NIS-2 nach den für Sie geltenden Fristen. Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung und Dokumentation.

ZEITACHSE

16.11.2026
Mitel MISA-2026-0012 · Patch für 10.3.0.18

19.11.2026
CVE-2026-133303 veröffentlicht (NVD)

24.11.2026
MISA-2026-0012 Revision 2.0 mit CVE-Nummern

25.11.2026
CISA KEV · Frist für US-Behörden 28.11.2026

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

In dieser Reihenfolge – Zugriff sperren vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
AWV von außen sperren	Mitel-Patch einspielen	Kompromittierung prüfen

01 Betroffenheit feststellen

Alle MiCollab-Server erfassen, auch Installationen beim Dienstleister oder in der DMZ. Betroffen ist `10.3.0.18` und älter. Klären, ob die Konferenzkomponente AWV aus dem Internet erreichbar ist.

02 Sofort Zugriff einschränken

Den externen Zugriff auf die AWV-Komponente per Firewall oder Reverse Proxy sperren, bis der Patch eingespielt ist. Wird AWV extern nicht gebraucht, dauerhaft nur intern freigeben.

03 Patchen

Den Mitel-Patch für MiCollab `10.3.0.18` nach Knowledge-Base-Artikel `KB000129195` einspielen oder auf ein späteres Release aktualisieren. Der Patch schließt alle fünf Lücken aus MISA-2026-0012.

04 Kompromittierung ausschließen

Webserver- und Proxy-Logs der AWV-Komponente auf ungewöhnliche Anfragen ohne Anmeldung prüfen, mindestens zurück bis Mitte November 2026. Auf dem Server nach unerwarteten Prozessen, neuen Benutzerkonten, Cron-Einträgen, Webshells und ausgehenden Verbindungen suchen. Bei Auffälligkeiten den Server isolieren und Zugangsdaten rotieren.

Kompromittierungs-Indikatoren (IoCs)

ANGREIFER-IPS

Bislang nicht veröffentlicht

AUFFÄLLIGE DATEIEN

unerwartet hochgeladene Dateien in AWV-Verzeichnissen

neue Cron-Einträge, Benutzerkonten, SSH-Keys

AUFFÄLLIGE MUSTER

Shell-Prozesse als Kind des Webserver-Prozesses

unerwartete ausgehende Verbindungen des MiCollab-Servers

Zur Einordnung: Mitel und CISA haben bisher keine Indikatoren veröffentlicht. Die Muster sind Suchansätze aus dem Angriffsweg (Upload + XML-Injection), kein vollständiger Ausschluss.

Wichtig: MiCollab-Konferenzportale stehen bewusst im Internet, damit externe Teilnehmer einwählen können. Ältere MiCollab-Lücken wurden bereits in der Vergangenheit aktiv ausgenutzt – Patches gehören hier in die Notfall-Spur.

Bildmotive: KI-generierte Symbolbilder

Lassen Sie das von unseren Experten prüfen.

Drei Bausteine, die genau auf diese Schwachstelle einzahlen – vom schnellen Exposure-Check bis zur laufenden Absicherung.

Cyber Defense Center

Worauf wir bei dieser Schwachstelle achten: Unerwarteter Datei-Upload an AWV, gefolgt von Prozessstart durch den Webserver. Das setzt voraus, dass die nötigen Logquellen angebunden sind.

Vulnerability & Exposure Management

Wir finden Aus dem Internet erreichbare MiCollab-Server bis 10.3.0.18 mit AWV über Ihren gesamten Perimeter – bevor Angreifer sie finden – und priorisieren nach realer Ausnutzung.

Incident-Response-Retainer

Bei Verdacht auf einen bereits erfolgten Zugriff übernimmt unser IR-Team Forensik und Eindämmung – mit vertraglich zugesicherter Reaktionszeit.

SO GEHEN WIR VOR

01 Exposure-Check

Wir prüfen, ob Ihre MiCollab-Systeme verwundbar konfiguriert und exponiert sind.

02 Sofortmaßnahmen begleiten

Mitigation und Patch-Fahrplan gemeinsam mit Ihrem Team umgesetzt.

03 Absichern & überwachen

Threat Hunting auf die IoCs, danach laufendes Monitoring und IR-Bereitschaft – 24/7, wenn Ihr Team das nicht selbst leisten kann.

Empfehlung für die Geschäftsleitung

- Patch aller MiCollab-Server als Notfall-Change anordnen.
- Bis dahin die Konferenzkomponente AWV von außen sperren lassen.
- Eine Prüfung der MiCollab-Server auf Kompromittierung beauftragen.

Ihr Part · unser Part. **Sie behalten die Kontrolle über Konfiguration und Freigaben; wir liefern Analyse, Bewertung und – im Retainer – die Reaktionskette.**

Rollen, Eingriffstiefe und SLAs im Erstgespräch (RACI, AVV/TOM auf Anfrage) · Datenhaltung auf Wunsch in Deutschland · ISO/IEC 27001 (TÜV SÜD) · deutschsprachige Analysten.

Sprechen Sie mit uns, bevor es ein Angreifer tut.

Kostenloses 30-Minuten-Erstgespräch – wir prüfen Ihre Exposure gegenüber CVE-2026-133303 und dem MiCollab-Perimeter.

+49 89 45 24 24-100 · kontakt@argos.security · www.argos.security

Termin buchen

Quellen: Mitel Product Security Advisory MISA-2026-0012 (16.11.2026, Rev. 2.0 vom 24.11.2026; CVSS 3.1 9,0, betroffen bis 10.3.0.18, Patch laut KB000129195) · NVD/CVE.org CVE-2026-133303 (veröffentlicht 19.11.2026, NVD-Bewertung 9,8, CWE-91) · CISA KEV (aufgenommen 25.11.2026, Frist 28.11.2026). Stand 25.11.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.

Bildmotive: KI-generierte Symbolbilder