CISA تحذّر من ثغرة رفع ملفات في Mitel MiCollab ((CVE-2026-133275



أدرجت CISA الثغرة CVE-2026-133275 في مكوّن مؤتمرات AWV ضمن Mitel MiCollab، وتتيح لمهاجم غير مصادق رفع ملفات عشوائية. يُنصح بتطبيق معالجات المورّد وتقييم التعرّض للإنترنت.

- الثغرة من نوع رفع ملف بنوع خطر دون قيود، بسبب ضعف التحقق من نوع الملف.
- تؤثر على مكوّن AWV (Audio, Web and Video Conferencing) في Mitel MiCollab.
- يمكن لمهاجم غير مصادق رفع ملفات عشوائية.
- تطلب CISA تطبيق المعالجات وفق تعليمات المورّد، مع الالتزام بتوجيه BOD 26-04 ومتطلبات الفرز الجنائي.
- الموعد النهائي للجهات الفيدرالية الأمريكية 28-11-2026، وعند تعذّر المعالجة تدعو CISA إلى التوقف عن استخدام المنتج.

أضافت CISA الثغرة CVE-2026-133275 إلى قائمتها، وهي ثغرة رفع ملفات دون قيود في Mitel MiCollab. تقع المشكلة في مكوّن AWV (Audio, Web and Video Conferencing) بسبب عدم كفاية التحقق من نوع الملف.

ما الذي تتيحه الثغرة

يمكن لمهاجم غير مصادق رفع ملفات عشوائية إلى النظام المتأثر. ولأن الاستغلال لا يتطلب بيانات دخول، يتوقف حجم التعرّض إلى حد كبير على إمكانية الوصول إلى مكوّن AWV من الإنترنت. لا يتضمن المصدر تفاصيل عن الاستغلال أو الإصدارات المتأثرة أو أرقام التحديثات، لذا ينبغي التأكد منها مباشرة مع المورّد.

ما تطلبه CISA

تطلب CISA تطبيق المعالجات وفق تعليمات المورّد، والالتزام بتوجيه BOD 26-04 الخاص بترتيب أولويات التحديثات الأمنية بحسب المخاطر، إضافة إلى متطلبات الفرز الجنائي (Forensics Triage). وفي الخدمات السحابية يُتّبع التوجيه المعمول به ضمن BOD 26-04. وإذا لم تتوافر معالجات، فتدعو CISA إلى التوقف عن استخدام المنتج. وتقع على الجهات مسؤولية تقييم تعرّض كل أصل للإنترنت. والموعد النهائي للجهات الفيدرالية الأمريكية هو 28-11-2026.

ورغم أن هذه المواعيد تخص الجهات الفيدرالية الأمريكية، فهي مرجع مفيد للمؤسسات السعودية التي تشغّل MiCollab للاجتماعات الداخلية أو الموجهة للعملاء. وغالباً ما تكون منصات التعاون على حدود الشبكة، لذا فإن تحديد أماكن نشرها خطوة أولى مناسبة.

نهج عملي

يُعامل الأمر كبند أولوية في التحديث لأي نسخة MiCollab متاحة من الإنترنت، مع حفظ الأدلة قبل المعالجة وأثناءها لإتاحة التحقيق في أي استغلال سابق.

ما يجب فعله الآن

1. حصر جميع نسخ Mitel MiCollab وتحديد ما يعرّض مكوّن AWV للإنترنت.
2. التواصل مع Mitel للحصول على المعالجة أو التحديث المناسب وتطبيقه وفق أولوية عاجلة.
3. تقييد الوصول الخارجي إلى AWV عبر الجدار الناري أو الوكيل العكسي إلى حين تأكيد المعالجة.
4. حفظ السجلات وأدلة نظام الملفات، ومراجعة وجود ملفات مرفوعة غير متوقعة قبل المعالجة وبعدها.
5. عند عدم توافر معالجة، التخطيط لإخراج المنتج من الخدمة وفق توجيه CISA.
6. توثيق تقييم التعرّض وإجراءات المعالجة ضمن عملية إدارة الثغرات.