ثغرة في مكوّن AWV ضمن Mitel MiCollab تتيح تجاوز المصادقة دون تسجيل دخول (CVE-2026-133324)



أدرجت CISA الثغرة CVE-2026-133324 في مكوّن الاجتماعات الصوتية والمرئية عبر الويب في Mitel MiCollab، وتتيح لمهاجم غير مصادَق تجاوز المصادقة. يُنصح بتطبيق إجراءات الشركة المصنّعة ومراجعة التعرّض للإنترنت.

- تؤثر CVE-2026-133324 على مكوّن الاجتماعات الصوتية والمرئية عبر الويب (AWV) في Mitel MiCollab.
- الخلل يتمثل في عدم الفشل بصورة آمنة، مما قد يتيح لمهاجم غير مصادَق تجاوز ضوابط المصادقة.
- قد ينفّذ المهاجم إجراءات غير مصرّح بها.
- تطلب CISA تطبيق إجراءات التخفيف وفق تعليمات الشركة المصنّعة، والموعد النهائي للجهات الفدرالية الأمريكية 28-11-2026.

- إذا لم تتوفر إجراءات تخفيف فتوجّه CISA إلى التوقف عن استخدام المنتج.

أدرجت CISA الثغرة CVE-2026-133324 في Mitel MiCollab، وهي منصة تعاون. يقع الخلل في مكوّن الاجتماعات الصوتية والمرئية عبر الويب (AWV) ويوصف بأنه عدم الفشل بصورة آمنة.

ما الذي تتيحه الثغرة

يمكن لمهاجم غير مصادَق تجاوز ضوابط المصادقة وتنفيذ إجراءات غير مصرّح بها. ولأن الهجوم لا يتطلب بيانات اعتماد، يرتبط حجم التعرّض إلى حد كبير بإمكانية الوصول إلى المكوّن من الإنترنت. لا يوضح المصدر نوع الإجراءات الممكنة ولا تفاصيل الاستغلال ولا الإصدارات المتأثرة، لذا يُرجع إلى نشرة الشركة المصنّعة.

ما تطلبه CISA

تطلب CISA تطبيق إجراءات التخفيف وفق تعليمات الشركة المصنّعة، مع الالتزام بتوجيه BOD 26-04 بشأن ترتيب أولويات التحديثات الأمنية بحسب المخاطر، ومتطلبات الفرز الجنائي الرقمي لديها. وبالنسبة للخدمات السحابية يُتّبع التوجيه المعني في BOD 26-04. وإذا لم تتوفر إجراءات تخفيف فيجب التوقف عن استخدام المنتج. وتقع على الجهات مسؤولية تقييم تعرّض كل أصل للإنترنت. الموعد النهائي 2026-11-28 ملزم للجهات الفدرالية الأمريكية، لكنه مرجع مفيد لغيرها.

نظرة عملية

على المؤسسات التي تشغّل MiCollab التأكد أولًا من نشر AWV ومن إتاحته خارجياً، ثم تنفيذ خطوات التخفيف الصادرة عن الشركة. ولأن تجاوز المصادقة قد لا يترك أثراً واضحاً، يُستحسن مراجعة سجلات الوصول بعد التخفيف.

ما يجب فعله الآن

1. حصر جميع نسخ Mitel MiCollab والتأكد من نشر مكوّن AWV.
2. تحديد النسخ المتاحة من الإنترنت ومنحها الأولوية.
3. تطبيق إجراءات التخفيف الصادرة عن الشركة وتوثيق التغيير ضمن إدارة التغيير.
4. مراجعة سجلات الوصول والإدارة في الأنظمة المتأثرة بحثاً عن نشاط غير متوقع.
5. عند عدم توفر إجراء تخفيف، التخطيط لتقييد الوصول أو إيقاف المنتج وإبلاغ مالك المخاطر.