CISA تحذّر من ثغرة ضعف في المصادقة في مكوّن المؤتمرات بمنصة Mitel MiCollab



أدرجت CISA الثغرة CVE-2026-133311 في مكوّن المؤتمرات بمنصة Mitel MiCollab، وهي قد تتيح لمهاجم غير موثّق الاطلاع على معلومات حساسة. يُنصح بتطبيق إجراءات المعالجة الصادرة عن المورّد.

- الثغرة CVE-2026-133311 ضعف في المصادقة داخل مكوّن Audio, Web and Video Conferencing (AWV) في Mitel MiCollab.
- قد يتمكن مهاجم غير موثّق من الوصول إلى معلومات حساسة عبر معرّف عشوائي يولّده النظام أو محتوى مُعدّ مسبقًا.
- تطلب CISA تطبيق المعالجة وفق تعليمات المورّد وبما يتوافق مع BOD 26-04 ومتطلبات الفرز الجنائي (Forensics Triage Requirements).
- إذا لم تتوفر إجراءات معالجة، تتجه إرشادات CISA إلى التوقف عن استخدام المنتج.

- الموعد النهائي للجهات الفيدرالية الأمريكية هو 2026-12-09، وعلى المالكين تقييم تعرّض كل أصل للإنترنت.

أدرجت CISA الثغرة CVE-2026-133311 ضمن إرشاداتها، وهي ثغرة ضعف في المصادقة في مكوّن Audio, Web and Video Conferencing (AWV) ضمن منصة Mitel MiCollab.

ما الذي تتيحه الثغرة

وفق المصدر، يمكن لمهاجم غير موثّق الوصول إلى معلومات حساسة باستخدام معرّف عشوائي محدد يولّده النظام أو محتوى مُعدّ مسبقًا. لا يقدّم المصدر تفاصيل تقنية إضافية، ولا يحدد نوع المعلومات المكشوفة، ولا يذكر وجود هجمات مرصودة.

ما تطلبه CISA

توجّه CISA الجهات المتأثرة إلى تطبيق إجراءات المعالجة وفق تعليمات المورّد، وبما يتسق مع إرشاداتها BOD 26-04 بشأن ترتيب أولويات التحديثات الأمنية حسب المخاطر، ومع متطلبات الفرز الجنائي (Forensics Triage Requirements). وبالنسبة للخدمات السحابية تُتَّبع إرشادات BOD 26-04 ذات الصلة. وإذا لم تتوفر إجراءات معالجة فينبغي التوقف عن استخدام المنتج. ويقع على مالكي الأصول تقييم مدى تعرّض كل أصل للإنترنت والالتزام بمتطلبات التحديث. والموعد النهائي للجهات الفيدرالية الأمريكية هو 2026-12-09.

هذه المتطلبات ملزمة للجهات الفيدرالية الأمريكية، لكنها مرجع مفيد للمؤسسات السعودية التي تشغّل MiCollab، خصوصًا إذا كانت خدمات المؤتمرات متاحة من الإنترنت.

النهج المقترح

تأكدوا من وجود MiCollab مع مكوّن AWV في بيئتكم، وحدّدوا النسخ المكشوفة للإنترنت، ثم طبّقوا تعليمات المورّد للمعالجة، ووثّقوا القرارات وتواريخ التنفيذ لأغراض التدقيق.

ما يجب فعله الآن

1. حصر جميع نُسخ Mitel MiCollab والتأكد من استخدام مكوّن AWV.
2. تحديد النسخ المتاحة من الإنترنت ومنحها الأولوية.
3. تطبيق إجراءات المعالجة الصادرة عن المورّد للثغرة CVE-2026-133311.
4. التخطيط لإيقاف أو عزل أي نسخة لا تتوفر لها إجراءات معالجة.
5. مراجعة سجلات الوصول والنشاط على النسخ المكشوفة بحثًا عن وصول غير مصرّح به، وتوثيق النتيجة.