CISA تضيف 10 ثغرات مستغلة إلى كتالوج KEV، منها خمس في Mitel MiCollab



أضافت CISA عشر ثغرات إلى كتالوج الثغرات المستغلة المعروفة، خمس منها في Mitel MiCollab وكُشف عنها الأسبوع الماضي. ويذكر عنوان المصدر أيضاً منتجات Juniper وVatesg وDanfossg.

- أضافت CISA يوم الأربعاء 10 ثغرات أمنية إلى كتالوج KEV.
- خمس من هذه الثغرات تمس Mitel MiCollab وقد كُشف عنها في الأسبوع السابق.
- إحدى ثغرات Mitel المدرجة، CVE-2026-133275 (بدرجة CVSS تبلغ 5.3)، هي رفع ملفات عشوائية.
- يشير العنوان إلى أن منتجات Juniper وVatesg وDanfossg متأثرة أيضاً.

أضافت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية (CISA) عشر ثغرات إلى كتالوج **الثغرات المستغلة المعروفة (KEV)**. ويعني إدراج الثغرة في الكتالوج رصد استغلالها فعلياً، ما يجعلها أولى بالمعالجة من الثغرات النظرية.

ما الذي ورد في الخبر

خمس من الثغرات المضافة تمس Mitel MiCollab، وهو منتج للتعاون والاتصالات، وقد كُشف عنها قبل أسبوع فقط. ومنها CVE-2026-133275 بدرجة CVSS تبلغ 5.3، وهي ثغرة رفع ملفات عشوائية في أحد مكونات المنتج. ويذكر عنوان المصدر كذلك منتجات Juniper وVatesg وDanfossg ضمن المنتجات المتأثرة.

لا يتضمن المقتطف المتاح لنا بقية معرّفات CVE ولا الإصدارات المتأثرة ولا تفاصيل التصحيح، لذا ينبغي التحقق منها في نشرات الموردين وفي مدخلات كتالوج CISA.

أهمية الخبر

لا ينبغي أن تقلل درجة CVSS المتوسطة من أولوية ثغرة معروف استغلالها، فحالة الاستغلال غالباً دليل أفضل على الإلحاح من الدرجة وحدها. وعلى الجهات التي تشغّل أياً من المنتجات المذكورة، لا سيما الأنظمة المتاحة من الإنترنت، مراجعة تعرضها الآن.

النهج المقترح

ابدأوا بجرد المنتجات التابعة للموردين المذكورين، ثم طبّقوا التحديثات أو الإجراءات الوقائية المتاحة، وراجعوا السجلات بحثاً عن مؤشرات إساءة الاستخدام قبل التصحيح وبعده.

ما يجب فعله الآن

1. مراجعة سجلات الأصول بحثاً عن منتجات Mitel MiCollab وJuniperg وVatesg وDanfossg.
2. الحصول على القائمة الكاملة لثغرات CVE العشر من كتالوج CISA KEV ونشرات الموردين.
3. إعطاء أولوية لتصحيح أو تخفيف مخاطر نسخ MiCollab المكشوفة بغض النظر عن درجة CVSS المتوسطة.
4. مراجعة سجلات الأنظمة المتأثرة بحثاً عن رفع ملفات مشبوه أو نشاط غير متوقع.
5. إدراج متابعة كتالوج KEV ضمن عملية إدارة الثغرات.