استغلال ثغرات يوم الصفر في Mitel MiCollab في حملة سرقة بيانات مع مؤشرات على استخدام الذكاء الاصطناعي



أفادت Apex Labs التابعة لـ Accenture باستغلال خمس ثغرات في MiCollab قبل صدور تصحيحات Mitel. وأضافتها CISA إلى كتالوج KEV، ويُنصح بالتصحيح والتحقق من أي اختراق سابق.

- خمس ثغرات في MiCollab (CVE-2026-133275 وCVE-2026-133303 وCVE-2026-133311 وCVE-2026-133323 وCVE-2026-133324) يمكن استغلالها دون مصادقة، واثنتان منها حرجتان وتتيحان تنفيذ أوامر.
- رصدت Accenture استغلالاً سبق نشر Mitel لنشرتها، مع نشر web shell في 15 نوفمبر.
- في إحدى الحالات نفّذ المهاجمون أوامر بعد 12 دقيقة من أول طلب، وحصلوا على صلاحيات root خلال نصف ساعة، ووصلوا إلى خوادم النسخ الاحتياطي وقواعد البيانات بعد نحو 20 ساعة.
- تواصلت بنية المهاجمين مع خدمتي واجهة برمجة ذكاء اصطناعي تجاريتين، دون أن تتمكن

Accenture من تحديد طريقة استخدامهما بدقة.

- أضافت CISA الثغرات الخمس إلى KEV، بينما لا تشير نشرة Mitel إلى استغلالها فعليًا.

أفادت Apex Labs التابعة لـ Accenture بأن جهات تهديد استغلت عدة ثغرات في منصة Mitel MiCollab بوصفها ثغرات يوم الصفر ضمن حملة لسرقة البيانات. وأضافت CISA لاحقًا خمس ثغرات في المنصة إلى كتالوج الثغرات المستغَلة المعروفة (KEV).

ما الذي رُصد

أعلنت Mitel في 16 نوفمبر عن تصحيحات لخمس ثغرات في مكوّن الاجتماعات الصوتية والمرئية والويب، وهي: رفع ملفات تعسفي، وحقن XML، ووصول غير مصرح به، وحقن أوامر، وتجاوز المصادقة. يمكن استغلالها جميعًا من مهاجمين غير موثّقين، وتتيح ثغرتان حرجتان تنفيذ أوامر تعسفية. وهي: CVE-2026-133275 وCVE-2026-133303 وCVE-2026-133311 وCVE-2026-133323 وCVE-2026-133324.

وجدت Accenture أدلة على الاستغلال قبل نشرة Mitel، منها نشر web shell على أنظمة إحدى الضحايا في 15 نوفمبر. وفي تلك الحالة نُفذت أوامر على خادم MiCollab بعد 12 دقيقة من أول طلب، وتبعتها صلاحيات root خلال نصف ساعة. وجمع المهاجمون بيانات اعتماد إضافية، ووصلوا بعد نحو 20 ساعة إلى خوادم النسخ الاحتياطي وقواعد البيانات الداخلية. وترى Accenture أن تعرّض المنتج المتكرر للإنترنت وتكامله مع Active Directory يجعلانه هدفًا جذابًا.

دور الذكاء الاصطناعي والأثر الأوسع

تواصلت بنية المهاجم مع خدمتي واجهة برمجة ذكاء اصطناعي تجاريتين لم تُسمَّيا. ولأن بيانات القياس عن بُعد مأخوذة بالعينة، لا تستطيع Accenture تحديد طريقة الاستخدام، لكن النشاط يتسق مع فرز البيانات، أو دعم الاستغلال وعمل web shell، أو إعداد مواد ابتزاز. وكان خادم ضحية ثانية يتصل بالبنية نفسها منذ 9 نوفمبر، لكن طريقة اختراقه غير واضحة لتأثره أيضًا بثغرات أقدم. ولم تُنسب الهجمات إلى مجموعة معروفة، وقد تكون جزءًا من حملة ابتزاز.

ولا تذكر نشرة Mitel، المحدّثة آخر مرة في 24 نوفمبر، أي استغلال فعلي. وحددت CISA مهلة 28 نوفمبر لأربع ثغرات و9 ديسمبر للخامسة.

لماذا يهم ذلك

قد لا يكفي التصحيح وحده، فربما اختُرقت الخوادم قبل تطبيق الإصلاحات، ويمكن أن يقود موطئ قدم على MiCollab سريعًا إلى أنظمة الهوية والنسخ الاحتياطي.

ما يجب فعله الآن

1. حصر جميع نسخ MiCollab، وخاصة المكشوفة للإنترنت، وتطبيق تصحيحات Mitel للثغرات الخمس دون تأخير.
2. البحث عن مؤشرات الاختراق على خوادم MiCollab، ومنها web shells والاتصالات الصادرة غير المتوقعة، مع اعتبار الخوادم التي صُححت متأخرة مشتبهًا باختراقها.

3. عند الاشتباه بالاختراق، تدوير بيانات الاعتماد بما فيها حسابات Active Directory المتاحة من MiCollab، ومراجعة النشاط على خوادم النسخ الاحتياطي وقواعد البيانات.
4. تقليص تعرّض واجهات الإدارة والاجتماعات في MiCollab للإنترنت بقدر ما تسمح به احتياجات العمل.
5. إدراج الحالة في خطط الاستجابة للحوادث، والاستعداد لسيناريوهات الابتزاز، وإبلاغ الجهة التنظيمية وفق المتطلبات إذا تأثرت بيانات.