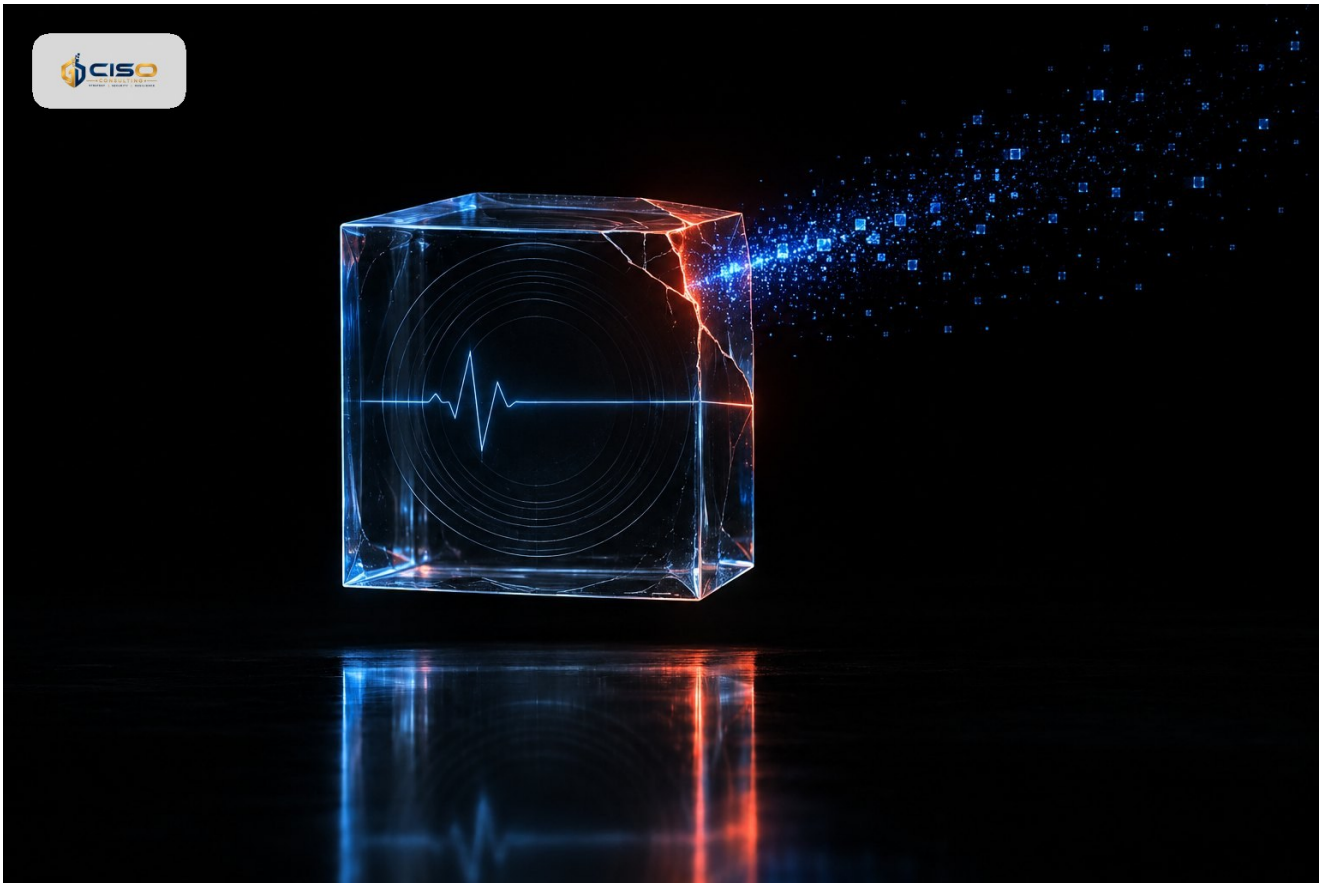
تقارير عن استغلال ثغرة في Microsoft Entra Connect Health لسرقة بيانات المستأجر



أفاد BleepingComputer باستغلال ثغرة في Microsoft Entra Connect Health لسرقة بيانات المستأجر. تعذّرت قراءة نص المصدر عدا العنوان، لذا لم تتأكد التفاصيل.

- تتعلق الثغرة المبلّغ عنها بخدمة Microsoft Entra Connect Health.
- وردت الثغرة على أنها مستغلة فعليًا وليست نظرية.
- الأثر المبلّغ عنه هو سرقة بيانات المستأجر.
- تعذّر التأكد من التفاصيل التقنية والإصدارات المتأثرة والإصلاحات من نص المصدر.

ما الذي ورد في التقرير

نشر BleepingComputer تقريرًا بعنوان يفيد باستغلال ثغرة في **Microsoft Entra Connect Health** لسرقة

بيانات المستأجر. العنوان هو الجزء الوحيد الذي أمكن قراءته من المصدر، ولذلك لا نذكر آلية الهجوم أو الجهة المنفذة أو الجهات المتضررة أو توفر تحديث أمني.

ما لا يمكن تأكيده

لا تتوفر لدينا معلومات مؤكدة عن رقم CVE أو الإصدارات المتأثرة أو نوع البيانات المسروقة أو عدد الضحايا أو موقف Microsoft. ولن نخمّن في هذه النقاط. ينبغي التعامل مع الخبر بوصفه إشارة مبكرة، والرجوع إلى إرشادات Microsoft والمقال الأصلي قبل استخلاص أي نتائج.

النهج الموصى به

على الجهات التي تزامن أدلتها المحلية مع Microsoft Entra ID أو تستخدم Entra Connect Health للمراقبة أن تتحقق من وجود الخدمة في بيئتها، وتحدد المسؤول عن إدارتها، وتراجع النشاط الحديث المرتبط بها. المراجعة الهادئة المبنية على الأدلة أفضل من تغييرات عاجلة دون تفاصيل. حدّثوا هذا التقييم عند صدور تفاصيل تقنية من Microsoft أو من المصدر الأصلي، ودوّنوا المراجعة في سجل المخاطر ضمن الرقابة المعتادة على خدمات السحابة والأطراف الخارجية.

ما يجب فعله الآن

1. تحققوا من نشر Entra Connect Health أو Entra Connect وحددوا مالك الخدمة.
2. راجعوا إرشادات Microsoft الرسمية والمقال الأصلي لمعرفة الإصدارات المتأثرة والإصلاحات.
3. افحصوا نشاط تسجيل الدخول والنشاط الإداري في Entra ID بحثًا عن أحداث غير معتادة.
4. راجعوا الأدوار ذات الامتيازات وحسابات الخدمة المرتبطة بمزامنة الدليل.
5. دوّنوا الأمر في سجل المخاطر وأطلعوا رئيس أمن المعلومات إلى حين تأكد التفاصيل.