ثغرة في Microsoft Entra Connect Health كشفت بيانات وصفية للمستأجرين أمام المهاجمين



أبلغت Microsoft العملاء المتأثرين بأن مهاجمين استغلوا ثغرة في واجهة Entra Connect Health API لقراءة بيانات وصفية للمستأجر، منها بريد جهات الاتصال التقنية. لم تُكشف كلمات مرور أو رموز، والتصيد هو الخطر الرئيسي.

- أُدخلت الثغرة في 23 يوليو 2026 ولم تُكتشف حتى 9 نوفمبر.
- نشرت Microsoft إصلاحاً من جانب الخدمة في 19 نوفمبر وأنهت تحقيقها في اليوم التالي.
- شملت البيانات المكشوفة بريد جهات الاتصال التقنية ومعرّف المستأجر واسمه ونوع الترخيص وحالة المزامنة، ولم تُكشف كلمات المرور ولا قيم التجزئة ولا الرموز ولا المفاتيح.
- لم تجد Microsoft أي تغييرات غير مصرح بها في الإعدادات، ولا يلزم العملاء تثبيت أي تحديث.
- لم يُعلن عدد المستأجرين المتأثرين ولا هوية المهاجمين.

أبلغت Microsoft عدداً من المؤسسات بأن مهاجمين استغلوا ثغرة في واجهة Microsoft Entra Connect Health API لقراءة بيانات وصفية على مستوى المستأجر. وConnect Healthy خدمة مراقبة سحابية تمنح مسؤولي النظم رؤية موحدة لحالة البنية التحتية للهوية المحلية وتنبيهاتها.

ما الذي حدث

بحسب الإشعار، أُدخلت الثغرة في 23 يوليو 2026 ولم تُكتشف حتى 9 نوفمبر. طبّقت Microsoft إصلاحاً من جانب الخدمة في 19 نوفمبر وأنهت تحقيقها في اليوم التالي، وأكدت حدوث وصول غير مصرح به للقراءة فقط إلى البيانات الوصفية، ولم تجد أي تغييرات غير مصرح بها في الإعدادات.

احتوت الاستجابات التي وصل إليها المهاجمون على عناوين بريد جهات الاتصال التقنية ومعرّف المستأجر واسمه المعروض والنطاق الأولي ورمز الدولة ونطاق المنطقة ومستوى ترخيص Entra وحالة مزامنة الدليل وآخر وقت مزامنة وحالة التسجيل في Connect Health. ولم تُكشف كلمات المرور ولا قيم التجزئة ولا رموز المصادقة ولا المفاتيح التشفيرية الصالحة ولا تفاصيل خوادم Active Directory المحلية ولا معلومات اشتراكات Azure. ولم تذكر Microsoft عدد المستأجرين المتأثرين ولا الجهة المنفذة.

لماذا يهم ذلك

لا يتطلب الأمر إجراءً من العملاء لمعالجة الثغرة نفسها، لكن عناوين البريد وحقائق المستأجر المكشوفة تجعل رسائل التصيد الموجهة أكثر إقناعاً، خصوصاً التي تذكر Entra أو Connect Health. ويزداد الخطر إذا كانت جهة الاتصال التقنية تحمل دوراً ذا صلاحيات مثل Global Administrator.

وتنصح Microsoft بالتحقق من الإشعار عبر الدخول مباشرة إلى بوابة Azure ومراجعة التنبيه الأمني في Azure Service Health بدل النقر على روابط في البريد.

ما يجب فعله الآن

1. تنبيه مركز العمليات الأمنية وفرق تقنية المعلومات وجهات الاتصال التقنية للمستأجر إلى رسائل التصيد التي تذكر المؤسسة أو Entra أو Connect Health.
2. التحقق من أي إشعار منسوب إلى Microsoft بالدخول مباشرة إلى بوابة Azure ومراجعة Azure Service Health لا عبر روابط البريد.
3. فرض المصادقة متعددة العوامل المقاومة للتصيد واستخدام Privileged Identity Management للتفعيل الآني للأدوار على جهات الاتصال التقنية ذات الصلاحيات.
4. تشغيل سكربت PowerShell للقراءة فقط الذي نشرته Microsoft لمعرفة ما قد تعيده الواجهة لمستأجركم، مع مراعاة أن القيم قد تكون تغيرت منذ الكشف.
5. مراجعة سجلات التدقيق وتسجيل الدخول في Entra وسجلات نشاط Azure بحثاً عن تغييرات غير متوقعة في Connect Health أو نشاط إداري غير معتاد.