استغلال ثغرة ScreenConnect (CVE-2026-84869) ضد أجهزة فنيي مزودي الخدمات المُدارة



يستغل مهاجمون الثغرة (CVSS 9.9) CVE-2026-84869 في عميل ConnectWise ScreenConnect، وقد صدر لها تصحيح، لتنفيذ حمولة خبيثة على جهاز الفني المتصل بجلسة الضيف.

- تبلغ درجة الثغرة CVE-2026-84869 نحو 9.9 وفق CVSS، وتمس عميل ScreenConnect.
- يستطيع الضيف نقل حمولة خبيثة وتنفيذها على جهاز الفني الذي يتصل بالجلسة.
- تشمل الأهداف المبلغ عنها خوادم مزودي الخدمات المُدارة (MSP).
- صدر تصحيح للثغرة، ورُصد استغلالها فعليًا.
- يذكر المصدر حادثة رُصدت في 12 نوفمبر 2026.

يستغل مهاجمون ثغرة حرجة في ConnectWise ScreenConnect تحمل الرمز CVE-2026-84869 وتبلغ درجتها 9.9

وفق مقياس CVSS. وقد أصدرت الجهة المطورة تصحيحًا لها، إلا أنه رُصدت هجمات استهدفت بيئات مزودي الخدمات المُدارة.

آلية الهجوم

تكمن الثغرة في عميل ScreenConnect. فبإمكان الضيف، أي الطرف البعيد في جلسة الدعم، نقل حمولة خبيثة إلى جهاز الفني وتنفيذها عند اتصاله بالجلسة. وبذلك ينقلب اتجاه الخطر المعتاد، إذ يصبح جهاز مهندس الدعم هو الهدف وليس جهاز العميل.

ويشير المصدر إلى حادثة رُصدت في 12 نوفمبر 2026 تخص مزود خدمات مُدارة، دون تفاصيل إضافية في الجزء المتاح، لذا يبقى نطاق الحملة وهوية المهاجمين غير واضحين.

الأهمية للمؤسسات في المملكة

غالبًا ما تحتفظ أجهزة الفنيين بصلاحيات مرتفعة للوصول إلى بيئات عملاء عدة، وقد يتحول اختراقها إلى بوابة نحو جهات متعددة في آن واحد. ولذلك ينبغي للمؤسسات المنظمة التي تعتمد على مزودي خدمات مُدارة أو تشغّل ScreenConnect داخليًا أن تتعامل مع الأمر بوصفه مخاطر سلسلة إمداد وأطراف ثالثة، إضافة إلى كونه مسألة تحديث.

والاستجابة العملية هي التحقق من تثبيت الإصدار المُصحَّح، ومراجعة الجلسات الأخيرة، وطلب إفادة المزودين بشأن وضعهم.

ما يجب فعله الآن

1. تأكدوا من استخدام ScreenConnect داخليًا أو لدى مزودي الخدمات، وتحققوا من تثبيت الإصدار المُصحَّح للثغرة CVE-2026-84869.
2. اطلبوا كتابيًا من كل مزود خدمات مُدارة إفادةً بحالة التحديث ورصد أي جلسات ضيف مشبوهة.
3. راجعوا سجلات جلسات ScreenConnect الأخيرة بحثًا عن نقل ملفات أو تنفيذ غير متوقع على أجهزة الفنيين.
4. قيّدوا صلاحيات أجهزة الفنيين ووصولها الشبكي، وراقبوها بأدوات كشف واستجابة لنقاط النهاية.
5. سجلوا الموضوع في سجل مخاطر الأطراف الثالثة، وصعّدوا أي اشتباه باختراق عبر مسار الاستجابة للحوادث.