حملة SCKit تستغل ثغرة مصححة في ScreenConnect وتزيد المخاطر على مزودي الخدمات المُدارة



أفادت Blackpoint Cyber بأن حملة SCKit ضد ConnectWise ScreenConnect تستغل الثغرة (CVSS 9.9) CVE-2026-84869 وهي ثغرة حرجة مصححة وليست جديدة.

- الحملة الجارية تستهدف نشرات ConnectWise ScreenConnect.
- تستغل الحملة الثغرة CVE-2026-84869 بدرجة CVSS تبلغ 9.9، وهي ثغرة حرجة سبق إصلاحها.
- استعادت مجموعة Adversary Pursuit Group التابعة لـ Blackpoint Cyber أدوات المهاجمين وشاركت التفاصيل مع The Hacker News.
- النشاط لا يعتمد على ثغرة جديدة، ما يجعل الأنظمة غير المحدّثة موضع التعرض.
- قد تتحول جلسات الدعم عن بُعد إلى مسارات هجوم نحو بيئات مزودي الخدمات المُدارة.

ما الذي ورد في التقرير

وصفت مجموعة Adversary Pursuit Group (APG) التابعة لـ Blackpoint Cyber حملة جارية تستهدف ConnectWise ScreenConnect، وهو برنامج وصول عن بُعد يُستخدم في جلسات الدعم الفني. ووفق التقرير تعتمد الحملة على أدوات استعادها الباحثون يُشار إليها باسم SCKit.

والتوضيح الأهم أن الحملة لا تقوم على ثغرة جديدة، بل تستغل الثغرة CVE-2026-84869 وهي ثغرة حرجة بدرجة CVSS تبلغ 9.9 وقد جرى إصلاحها بالفعل.

أهمية الأمر

بما أن الثغرة مصححة، فإن التعرض يقع أساساً في النشرات التي لم تطبق الإصلاح. وتحتل أدوات الدعم عن بُعد موقعاً موثوقاً لأنها تربط مقدمي الخدمة ببيئات العملاء. ويشير طرح التقرير إلى أن جلسات الدعم قد تكون مساراً للوصول إلى بيئات مزودي الخدمات المُدارة (MSP) ومنها إلى الجهات التي يخدمونها.

لا يتضمن المقتطف المتاح تفاصيل تقنية إضافية مثل الإصدارات المتأثرة أو مؤشرات الاختراق أو حجم النشاط، ولذلك ينبغي التحقق منها لدى المورّد وفي البحث الأصلي.

قراءة عملية

على الجهات التي تشغّل ScreenConnect بنفسها، أو تعتمد على مزودين يستخدمونه، أن تتعامل مع الأمر كمهمة تحقق من التحديثات وضمان لأمن الأطراف الثالثة، لا كحالة طارئة تتطلب تقنيات جديدة.

ما يجب فعله الآن

1. تأكد من استخدام ScreenConnect في بيئتكم وتحقق من تطبيق إصلاح الثغرة CVE-2026-84869.
2. اسألوا مزودي الخدمات المُدارة والدعم كتابةً عما إذا كانوا يشغّلون ScreenConnect وقد أصلحوا هذه الثغرة.
3. راجعوا سجلات الوصول وتاريخ الجلسات في ScreenConnect بحثاً عن نشاط غير متوقع أو غير مصرح به.
4. قلّصوا تعرض خوادم الدعم عن بُعد للإنترنت واشترطوا مصادقة قوية لوصول الفنيين.
5. أدرجوا أدوات الوصول عن بُعد ضمن إدارة الثغرات ومراجعات مخاطر الأطراف الثالثة في برامج الالتزام بضوابط NCA ECC وإطار SAMA CSF.