ConnectWise: استمرار الهجمات على ScreenConnect في البيئات المحلية غير المحدّثة



أنهت ConnectWise تحقيقها في الوصول غير المصرّح به إلى بيئات ScreenConnect لدى الشركاء، وتنصح باستخدام عميل الفني بالإصدار 26.6.5 أو أحدث. ولا تزال تُبلَّغ هجمات على البيئات المحلية التي تفعّل إضافات خارجية محددة.

- أعلنت ConnectWise إتمام تحقيقها في الوصول غير المصرّح به إلى بيئات ScreenConnect لدى الشركاء.
- توصي العملاء بالتأكد من تشغيل عميل الفني بالإصدار 26.6.5 أو أحدث.
- لا يزال يُبلَّغ عن نشاط يستهدف البيئات المحلية.
- يتعلق النشاط المبلّغ عنه ببيئات ما زالت الإضافات الخارجية المحددة مفعّلة فيها.
- يربط عنوان المصدر استمرار الهجمات بأداة SCKit التي تستهدف الأنظمة غير المحدّثة.

أفادت ConnectWise بأنها أنهت تحقيقها في الوصول غير المصرّح به الذي استهدف بيئات ScreenConnect الخاصة بشركائها. وضمن إرشاداتها، توصي الشركة العملاء بالتأكد من أن عميل الفني لديهم يعمل بالإصدار 26.6.5 أو أحدث.

ما الذي لا يزال يحدث

وفق التقرير، لا تزال ConnectWise تتلقى بلاغات عن نشاط إضافي يستهدف بيئات ScreenConnect المحلية. وتتعلق هذه البلاغات بالنشرات التي ما زالت الإضافات الخارجية المحددة مفعّلة فيها. كما يربط عنوان المصدر استمرار الهجمات بأداة SCKit التي توصف بأنها تستهدف الأنظمة غير المحدّثة.

ولا يتضمن المقتطف المتاح لنا تفاصيل تقنية إضافية، مثل أسماء الإضافات أو معرّفات الثغرات أو عدد الجهات المتأثرة، ولذلك لا نفترض شيئًا بشأنها.

لماذا يهم ذلك

تمنح أدوات الدعم والوصول عن بعد صلاحيات واسعة على الأجهزة والخوادم المُدارة. وبالنسبة للجهات المنظَّمة التي تستخدم ScreenConnect مباشرة أو عبر مزوّد خدمات، فإن وجود نسخة غير محدّثة أو مكشوفة خطر يستحق المراجعة العاجلة حتى دون رصد حادثة.

النهج المقترح

تأكدوا من استخدام ScreenConnect في بيئتكم، بما في ذلك لدى الموردين ومزوّدي الخدمات المُدارة. قارنوا الإصدارات المثبتة بإرشادات الشركة، وراجعوا الإضافات المفعّلة، واطلعوا على إشعار ConnectWise الأصلي للاطلاع على المكونات المتأثرة قبل اتخاذ القرار.

ما يجب فعله الآن

1. حصر جميع نسخ ScreenConnect، بما فيها التي يديرها الموردون ومزوّدو الخدمات المُدارة.
2. التحقق من أن عميل الفني بالإصدار 26.6.5 أو أحدث، والتحديث عند الحاجة.
3. مراجعة الإضافات الخارجية المفعّلة على الخوادم المحلية وتعطيل غير الضروري منها وفق إرشادات ConnectWise.
4. فحص سجلات الوصول والنشاط على خوادم ScreenConnect بحثًا عن جلسات أو تغييرات غير متوقعة.
5. مطالبة مزوّدي الخدمات بتأكيد حالة التحديث لديهم كتابيًا.