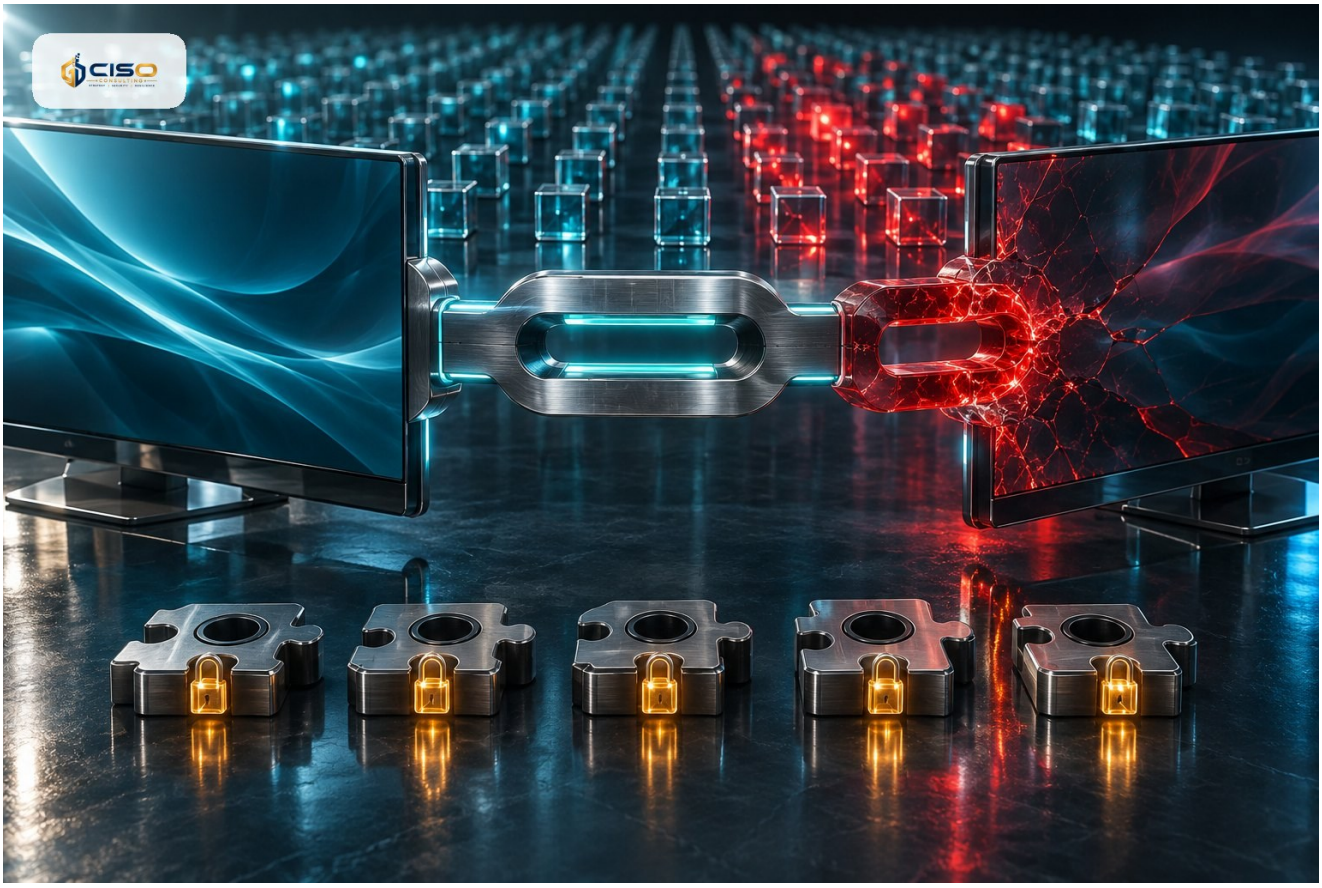
عملاء ScreenConnect غير مصرّح بهم على 288 جهازًا وConnectWise تعطّل خمس إضافات



تفيد التقارير بأن هجمات عبر عملاء ScreenConnect غير مصرّح بهم طالت 288 جهازًا على الأقل في 48 جهة. وعطّلت ConnectWise خمس إضافات من جهات خارجية في بيئات شركائها بعد بلاغات عن وصول غير مصرّح به.

- استُهدف ما لا يقل عن 288 جهازًا في 48 جهة بعملاء ScreenConnect غير مصرّح بهم.
- عطّلت ConnectWise خمس إضافات من جهات خارجية في بيئات الشركاء كإجراء احترازي.
- تقول الشركة إنه لا يوجد دليل على اختراق بنيتها التحتية أو على ثغرة في برنامج ScreenConnect.
- التقييم الأولي للشركة ما زال مبدئيًا، والمقتطف المتاح لا يتضمن تفاصيل تقنية إضافية.

عطّلت ConnectWise خمس إضافات من جهات خارجية في بيئات شركائها، بعد بلاغات عن وصول غير مصرّح به يتعلق بأداة الوصول عن بُعد ScreenConnect. وتشير التقارير إلى استخدام عملاء ScreenConnect غير مصرّح بهم

ضد 288 جهازًا على الأقل في 48 جهة.

ما تقوله الشركة

ذكرت ConnectWise في إشعار على موقعها أنه لا يوجد دليل على اختراق بنيتها التحتية أو على ثغرة في برنامج ScreenConnect. ووصفت تقييمها الأولي بأنه مبدئي، ولا يوضح المقتطف المتاح آلية النشاط ولا الإضافات المتأثرة.

أهمية الموضوع

أدوات الوصول عن بُعد موثوقة بطبيعتها، لذا قد يبدو العميل غير المصرّح به المثبّت على جهاز كنشاط إداري اعتيادي. وعلى الجهات التي تستخدم ScreenConnect مباشرة، أو تعتمد على مزوّدي خدمات مُدارة يستخدمونه، أن تتحقق مما هو مثبّت وممن يحق له الاتصال.

ولأن الشركة لم تشر إلى ثغرة برمجية، فقد لا يكفي التحديث وحده لمعالجة التعرّض. ينصب التركيز عمليًا على الجرد وضبط الوصول ومراقبة أدوات الوصول عن بُعد، مع متابعة إشعار ConnectWise لأي مستجدات.

ما يجب فعله الآن

1. حصر جميع نسخ وعملاء ScreenConnect، بما فيها ما يديره مزوّدو الخدمات المُدارة، وإزالة غير المعتمد منها.
2. مراجعة إشعار ConnectWise والتأكد مما إذا كانت أي من الإضافات الخمس المعطّلة مستخدمة في بيئتكم.
3. البحث عن عملاء وصول عن بُعد غير متوقعين على الأجهزة ومراجعة سجلات الجلسات الأخيرة بحثًا عن اتصالات غير مألوفة.
4. تقييد تثبيت أدوات الوصول عن بُعد عبر ضوابط التطبيقات وتحديد من يملك صلاحية الموافقة على الاتصالات.
5. مطالبة مزوّدي الخدمات المُدارة بتأكيد مدى تعرّضهم وإجراءات الاستجابة كتابيًا، وفق متطلبات الأطراف الخارجية في ضوابط الهيئة الوطنية للأمن السيبراني (NCA ECC).