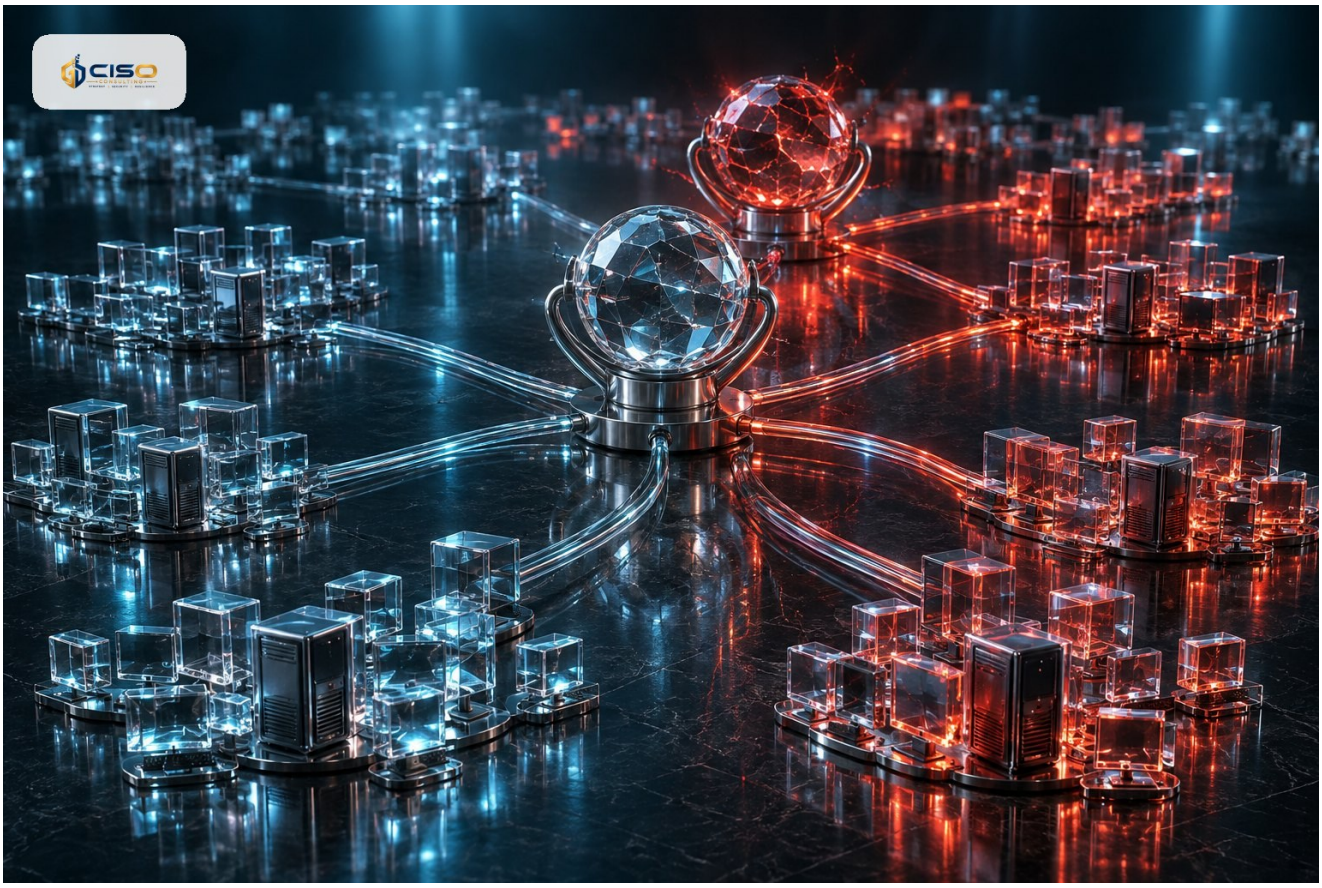
حملة على ScreenConnect تخترق مزودي الخدمات المُدارة وتنشر عملاء وصول عن بُعد غير مصرّح بهم لدى العملاء



تفيد ConnectWise وHuntress بحملة نشطة تسيء استخدام ScreenConnect لدى مزودي الخدمات المُدارة لتثبيت عملاء وصول عن بُعد غير مصرّح بهم على أجهزة العملاء. وتحصي Huntress ستة مزودين وأكثر من 286 جهازًا في 47 جهة، والأعداد في ازدياد.

- تتابع Huntress ستة مزودين خدمات مُدارة مخترقين وأكثر من 286 جهازًا في 47 جهة، والأعداد لا تزال في ارتفاع.
- يستخدم المهاجمون ميزة Run Command في ScreenConnect لتثبيت عملاء ScreenConnect غير مصرّح بهم خارج بيئة مزود الخدمة نفسه.
- تصف Huntress النشاط بأنه إساءة استخدام لوظائف مشروعة وليس استغلال ثغرة، وتشير بيانات الرصد إلى بيانات اعتماد مخترقة أو جلسات مشغّلين مختطفة.

- عطّلت ConnectWise خمس إضافات من جهات خارجية في نحو 400 بيئة سحابية لشركائها، ويجب على عملاء النسخ المحلية تعطيلها يدويًا.
- قد تتعرض محطات عمل الفنيين للاختراق عند بدء جلسات تفاعلية مع أجهزة مصابة، وما زالت ConnectWise تتحقق من هذه البلاغات.

تحقق ConnectWise في حملة نشطة يستخدم فيها المهاجمون بيئات ScreenConnect المخترقة لدى مزودي الخدمات المُدارة (MSPs) لزرع عملاء وصول عن بُعد غير مصرّح بهم على أجهزة العملاء. وكانت Huntress أول من رصد النشاط، وتفيد بوجود ستة مزودين مخترقين وأكثر من 286 جهازًا في 47 جهة، مع استمرار ارتفاع الأعداد.

ما الذي يحدث

وفق Huntress، يستخدم المهاجمون وظيفة Run Command في ScreenConnect لتثبيت عملاء ScreenConnect غير مصرّح بهم على الأجهزة المُدارة، ما يمنحهم وصولاً عن بُعد خارج بيئة المزود الشرعي. وتحذّر Huntress كذلك من أسلوب أخطر، وهو اختراق محطة عمل الفني عندما يبدأ جلسة مع جهاز عميل مصاب. وتقول ConnectWise إن هذه البلاغات لا تزال قيد التأكيد، ولم تُشرح علنًا آلية الانتقال.

وتصف Huntress النشاط بأنه إساءة استخدام لوظائف مشروعة وليس استغلالاً لثغرة. ولم تحدد كيف يدخل المهاجمون إلى بيئات المزودين، لكن بيانات الرصد لديها تشير إلى بيانات اعتماد مخترقة أو جلسات مشغّلين مختطفة. كما توحي وسوم متسلسلة يستخدمها المهاجمون بأن مزودين آخرين ربما اختُرقوا في وقت سابق.

استجابة ConnectWise

أكدت ConnectWise وجود وصول غير مصرّح به إلى حسابات شركاء ScreenConnect. وعطّلت احترازيًا خمس إضافات من جهات خارجية (Labtech Plus وRMM Plus وRMM+ Link وRMM Plus Password وRMM+ Password) في نحو 400 بيئة لشركائها. وتؤكد أن وجود الإضافات لا يثبت الاختراق، وأن تعطيلها لا يزيل البرمجيات أو الوصول القائم أصلاً. أما عملاء النسخ المحلية فعليهم تعطيلها بأنفسهم وعدم إعادة تفعيلها قبل صدور إرشادات جديدة.

الدلالات

ينبغي لكل جهة تعتمد على مزود خدمات مُدارة أن تتعامل مع الحادثة بوصفها حدث مخاطر أطراف ثالثة. وقد نشرت Huntress مؤشرات اختراق، منها معرّفات العملاء غير المصرّح بهم وبنية المهاجمين التحتية، يمكن لفرق الأمن استخدامها في الاستقصاء.

ما يجب فعله الآن

1. اطلب كتابيًا من مزودي الخدمات المُدارة لديك بيان ما إذا كانوا يستخدمون ScreenConnect وهل ثُبّتت أي من الإضافات الخمس، مع تأكيد حالة تحقيقهم.
2. إذا كنت تشغّل ScreenConnect محليًا، فعطّل الإضافات الخمس يدويًا ولا تعد تفعيلها حتى تصدر ConnectWise إرشادات جديدة.
3. راجع سجلات المصادقة وسجلات تثبيت الإضافات والنشاط الإداري وسجل Run Command وسجلات

Toolbox، حتى لو لم تصدر تنبيهات.

4. ابحث عن مؤشرات الاختراق المنشورة (معرّفات العملاء غير المصرّح بهم والنطاقات وعناوين IP وأسماء الملفات) في الأجهزة وسجلات الشبكة.
5. تجنّب الجلسات التفاعلية عبر ScreenConnect مع الأجهزة المشتبه باختراقها، وافحصها بأدوات أمنية منفصلة.
6. أعد تعيين بيانات اعتماد حسابات ScreenConnect وراجع جلسات المشغّلين النشطة، وتأكد من فرض المصادقة متعددة العوامل على وصول مزودي الخدمة.