

ConnectWise تعيد ضبط بيانات الاعتماد مع استمرار توقف Cloud Backup بعد حادث أمني



أعلنت ConnectWise تعزيز حماية الوصول الإداري وإعادة ضبط الحسابات واستبدال بيانات اعتماد التطبيقات بعد وصول غير مصرح به إلى هويات تطبيقات مرتبطة بـ Cloud Backup، ولا تزال الخدمة متوقفة.

- تتعامل ConnectWise مع حادث أمني تضّمن وصولاً غير مصرح به إلى هويات تطبيقات مرتبطة بـ Cloud Backup.
- شملت إجراءات المعالجة تشديد حماية الوصول الإداري.
- أعادت الشركة ضبط الحسابات واستبدلت بيانات اعتماد التطبيقات.
- بحسب التقرير، لا تزال خدمة Cloud Backup متوقفة.
- لا يوضح المقتطف المتاح نطاق الحادث أو العملاء المتأثرين أو موعد استعادة الخدمة.

ذكرت ConnectWise أنها تواصل التعامل مع حادث أمني أدى إلى وصول غير مصرح به إلى هويات تطبيقات مرتبطة بخدمة Cloud Backup، وأن الخدمة ما زالت متوقفة.

ما أعلنته الشركة

وصفت الشركة يوم الاثنين إجراءات المعالجة المنفذة حتى الآن، ومنها تعزيز حماية الوصول الإداري، وإعادة ضبط الحسابات، واستبدال بيانات اعتماد التطبيقات. والنص المتاح من المصدر موجز ولا يسرد جميع الإجراءات المكتملة.

ما لم يتضح بعد

لا يبين المقتطف كيف جرى الوصول، ولا العملاء أو البيانات المتأثرة، ولا موعد عودة Cloud Backup. ينبغي للجهات عدم الافتراض والاعتماد على إفادات المورد المباشرة.

أهمية الأمر للجهات المنظمة

تحتفظ خدمات النسخ الاحتياطي بنسخ من بيانات حيوية، وهويات التطبيقات هي بيانات اعتماد تتيح للأنظمة التخابط فيما بينها. وأي حادث يمسها يثير تساؤلات حول تعرّض بيانات الاعتماد وجاهزية الاستعادة أثناء توقف الخدمة. على الجهات التي تستخدم ConnectWise Cloud Backup، مباشرة أو عبر مزود خدمات مُدارة، تأكيد وضعها والتحقق من توافر خيارات استعادة بديلة.

ما يجب فعله الآن

1. تأكد مما إذا كانت جهتكم أو أي مزود خدمات مُدارة لديكم يستخدم ConnectWise Cloud Backup.
2. اطلبوا كتابيًا من المورد أو المزود إيضاحًا حول أثر الحادث على بياناتكم والجدول المتوقع لاستعادة الخدمة.
3. تحققوا من وجود نسخ احتياطية حديثة ومُختبرة خارج الخدمة المتأثرة.
4. بدّلوا بيانات الاعتماد أو مفاتيح API التي أصدرتموها للتكامل مع الخدمة إن وُجدت.
5. راجعوا سجلات الوصول الخاصة بالتكامل بحثًا عن نشاط غير معتاد، ووثّقوا المراجعة ضمن ملفات مخاطر الأطراف الثالثة.