pCloud Pass يؤكد تعرضه لهجوم سيبراني بعد بلاغات عن أجهزة غير معروفة في الحسابات



أكدت شركة pCloud السويسرية أن مدير كلمات المرور pCloud Pass تعرض لهجوم سيبراني قالت إن فريقها احتواه، وذلك بعد بلاغات من مستخدمين عن أجهزة غير معروفة مرتبطة بحساباتهم.

- pCloud Pass مدير كلمات مرور متعدد المنصات تقدمه شركة سويسرية.
- أبلغ مستخدمون، ومنهم من نشر على Reddit، عن ظهور أجهزة غير معروفة مرتبطة بحساباتهم.
- أكدت الشركة وقوع هجوم وقالت إن فريقها احتواه سريعاً.
- ذكرت أن عدداً قليلًا من المستخدمين تأثرت عناوين بريدهم الإلكتروني، والنص المتاح ينقطع عند هذه النقطة.
- لا يحدد المصدر نطاق التعرض بما يتجاوز ذلك ولا سبب الهجوم.

ما الذي أُعلن

أقرت الشركة السويسرية المطورة لـ pCloud Pass بأن مدير كلمات المرور متعدد المنصات كان هدفاً لهجوم سيبراني. وجاء الإقرار بعد منشورات على Reddit أفاد فيها مستخدمون بظهور أجهزة غير معروفة مرتبطة بحساباتهم.

وقالت الشركة في ردها إن فريقها احتوى الهجوم سريعاً، وإن عدداً قليلًا من المستخدمين تأثرت عناوين بريدهم الإلكتروني. وينتهي النص المتاح عند هذه النقطة، ولذلك لا تتوافر تفاصيل إضافية عن بقية ما تعرض للكشف، أو كيفية دخول المهاجمين، أو عدد الحسابات المعنية.

الدلالة للمنشآت

يحتفظ مدير كلمات المرور ببيانات الدخول إلى أنظمة كثيرة أخرى، لذا يستحق أي حادث يتعلق به الانتباه حتى لو وصفه المزود بأنه تحت السيطرة. أما العَرَض المبلّغ عنه، وهو ظهور أجهزة غير مألوفة في الحسابات، فيمكن للمستخدمين وفرق الأمن التحقق منه مباشرة.

ينبغي ألا تُبنى استنتاجات تتجاوز ما صرّح به المزود. والنهج المناسب هو معرفة ما إذا كان الموظفون يستخدمون المنتج، والتأكد من حالة الحسابات، ومتابعة أي إشعارات لاحقة من المزود.

النهج المقترح

يُعامل الأمر كمراجعة احترازية لا كحالة طوارئ: يُحدَّد التعرض أولًا، ثم تُشدَّد ممارسات حماية الحسابات حيث يُستخدم pCloud Pass، وتُوثَّق الفحوص تحسباً لأي استفسار من الجهات التنظيمية أو المدققين.

ما يجب فعله الآن

1. تحديد ما إذا كان الموظفون أو الإدارات يستخدمون pCloud Pass، بما في ذلك الاستخدام الشخصي لبيانات دخول العمل.
2. مطالبة المستخدمين بمراجعة قائمة الأجهزة المتصلة بحساباتهم في pCloud Pass وإزالة أي جهاز لا يعرفونه.
3. توجيه المستخدمين المتأثرين إلى تغيير كلمة المرور الرئيسية وتفعيل المصادقة متعددة العوامل إن توافرت.
4. تنبيه الموظفين إلى احتمال استغلال عناوين البريد في رسائل التصيّد، والإبلاغ عن أي رسالة مشبوهة.
5. متابعة إشعارات المزود، وتقييم التزامات الإشعار بموجب نظام حماية البيانات الشخصية إذا تأكد تأثر بيانات شخصية للعملاء أو الموظفين.
6. توثيق المراجعة ونتائجها لأغراض التدقيق وإدارة مخاطر الأطراف الثالثة.