pCloud تؤكد تعرض مدير كلمات المرور Pass لهجوم دون استبعاد الوصول إلى الخزائن المشفرة



أكدت pCloud أن هجوماً على pCloud Pass كشف عدداً محدوداً من عناوين البريد وأدى إلى محاولات دخول. وتقول إن البيانات المخزنة تبقى مشفرة، دون توضيح ما إذا جرى الوصول إلى الخزائن المشفرة.

- تلقى مستخدمون تنبيهات عن اتصال جهاز جديد باسم "pd" بحساباتهم في pCloud Pass، بعضهم كان مفعّلًا للمصادقة الثنائية.
- تقول pCloud إن الهجوم جرى احتواؤه وانحصر في مدير كلمات المرور دون التأثير على خدمة التخزين السحابي.
- أفادت الشركة بكشف عدد محدود من عناوين البريد ووقوع محاولات دخول.
- تقول الشركة إن بيانات الخزائن مشفرة على أجهزة المستخدمين وتتطلب كلمة المرور الرئيسية، لكنها لم توضح ما إذا جرى الوصول إلى خزائن مشفرة أو سرقتها.
- أشار قارئ إلى أن رابط الإعدادات في رسائل التنبيه يشير إلى اسم مضيف يبدو بيئة اختبار جودة.

أكدت pCloud أن مدير كلمات المرور التابع لها، pCloud Pass، تعرض لهجوم سيبراني. وظهرت الحادثة حين تلقى عملاء رسائل تفيد باتصال جهاز غير معروف باسم "pd" بحساباتهم. وذكر بعضهم أن المصادقة الثنائية كانت مفعّلة، فيما لم يجد آخرون أي جهاز غريب عند مراجعة حساباتهم. كما وصلت التنبيهات إلى أشخاص لم يستخدموا مدير كلمات المرور أصلًا.

ما تقوله pCloud

تفيد الشركة بأنها احتوت الهجوم سريعاً وأنه انحصر في مدير كلمات المرور دون أن يطال خدمة التخزين السحابي. وتقول إن عدداً محدوداً من عناوين البريد الإلكتروني كُشف، وإن محاولات دخول وقعت، وإن التنبيهات أُرسلت تلقائياً إلى هذه العناوين. وتؤكد أن كلمات المرور والملاحظات وسائر العناصر المخزنة لم تتعرض للاختراق، لأنها مشفرة على أجهزة العملاء ولا تُفك إلا بكلمة المرور الرئيسية.

ما لم يتضح بعد

لم توضح pCloud ما إذا جرى الوصول إلى خزائن مشفرة أو سرقتها. وهذا مهم لأن من يملك خزائن مشفرة قد يحاول كسرها دون اتصال، متجاوزاً حدود محاولات الدخول والمصادقة الثنائية. ويذكّر المصدر باختراق LastPass عام 2022، إذ رُبطت نسخ الخزائن المسروقة لاحقاً بسرقات عملات رقمية يُعتقد أنها تمت عبر كسر كلمات مرور رئيسية ضعيفة أو مكررة.

وأشار قارئ إلى أن رابط "Open settings" في رسالة التنبيه يشير إلى اسم مضيف يبدو بيئة اختبار جودة لا بيئة الإنتاج، وأكد BleepingComputer ذلك من نسخة من الرسالة. وحذرت pCloud العملاء من التصيد، مؤكدة أنها لا تطلب كلمات المرور الرئيسية أو كلمات الاسترداد عبر البريد أو الهاتف أو المحادثة.

وتأتي الحادثة بعد وقائع أخرى طالت مديري كلمات المرور هذا الشهر، منها mSecure و1Password، بحسب المصدر.

ما يجب فعله الآن

1. حصر الموظفين والإدارات التي تستخدم pCloud Pass أو مديري كلمات مرور استهلاكيين مشابهين، والتأكد مما إذا كانت بيانات اعتماد المؤسسة مخزنة فيها.
2. توجيه المستخدمين المتأثرين إلى تغيير كلمة المرور الرئيسية إلى عبارة طويلة وفريدة، وتدوير بيانات الاعتماد عالية الأهمية المخزنة في الخزنة.
3. عدم الاكتفاء ببيان pCloud، وطلب توضيح من المزود حول ما إذا جرى الوصول إلى خزائن مشفرة.
4. تنبيه الموظفين بأن pCloud تقول إنها لا تطلب كلمات المرور الرئيسية أو كلمات الاسترداد، وبأن رسائل التنبيه قد تُستغل في التصيد، والتحقق من الروابط قبل فتحها.
5. مراجعة تقييم مخاطر الأطراف الثالثة وشروط الإبلاغ عن الحوادث لمديري كلمات المرور المستخدمين، بما يتوافق مع متطلبات الأطراف الخارجية في ضوابط NCA ECC وإطار SAMA CSF.