1Password تكشف عن اختراق عبر حساب GitHub لأحد موظفيها دون المساس بالخزائن



أعلنت 1Password أن مهاجمًا استخدم حساب GitHub مخترقًا لأحد موظفيها لحقن شيفرة سحبت سجلات حسابات العملاء. لم تتأثر الخزائن ولا مفاتيحها، ويبقى التصيد بالبيانات المسروقة الخطر الأبرز.

- بدأ التحقيق في 19 نوفمبر بعد مؤشرات على اختراق حساب GitHub لأحد الموظفين.
- حقن المهاجم شيفرة خبيثة في خدمات خلفية وحمّل سجلات حسابات العملاء.
- تشمل البيانات المكشوفة الأسماء والبريد الإلكتروني والمعرّفات والطوابع الزمنية والمفاتيح العامة ومعاملات SRP ورموز الدعوة أو الاسترداد.
- سُرقت شيفرة مصدرية داخلية وجرى الوصول إلى بيئة CI/CD، مما قد يكشف بيانات اعتماد للبنية التحتية.
- تأثر عدد محدود من المستخدمين، ولا يُطلب تغيير كلمات المرور أو Secret Keys.

كشفت 1Password عن حادثة أمنية سيطر فيها مهاجم على حساب GitHub المؤسسي لأحد موظفيها، ووصل إلى مستودعات الشيفرة المصدرية الخاصة، وأدخل شيفرة خبيثة في خدمات خلفية استُخدمت لتنزيل سجلات حسابات العملاء.

ما الذي تأثر

تؤكد الشركة أن خزائن كلمات المرور ومفاتيح التشفير التي تحميها لم تتعرض للاختراق. وتشمل السجلات المسروقة أسماء العملاء وعناوين بريدهم الإلكتروني، ومعرّفات الحسابات والمستخدمين، وطوابع وقت الإنشاء وآخر تسجيل دخول، والمفاتيح العامة، ومعاملات بروتوكول SRP (Secure Remote Password)، ورموز الدعوة والتهيئة واسترداد الحساب. كما سرق المهاجم شيفرة مصدرية داخلية ووصل إلى بيئة CI/CD، وهو ما قد يكشف بيانات اعتماد للبنية التحتية.

لا يمكن استخدام هذه الرموز وحدها، إذ يتطلب إكمال الدعوة أو الاسترداد مصادقة SSO أو رمزًا يُرسل إلى البريد المسجّل للمستخدم. وقد رفعت 1Password طول هذا الرمز من ستة أرقام إلى عشرة أحرف وأرقام احترازًا من هجمات التخمين. وأُبلغ المستخدمون المتأثرون، وهم عدد محدود، بشكل فردي.

الاستجابة والمخاطر المتبقية

عطّلت الشركة الحساب المخترق، وألغت الرمز المسروق، واستعادت نسخًا سليمة من الخدمات المتأثرة، وبدّلت أو ألغت بيانات الاعتماد المحتمل كشفها. ويتحقق خبراء مستقلون من المعالجة، وتفيد الشركة بعدم وجود دليل داخلي على الاستيلاء على حسابات. ولا تطلب من العملاء تغيير كلمات المرور أو Secret Keys.

يتمثل الخطر العملي في التصيّد. فالبيانات المسروقة تحدد مستخدمين حقيقيين لـ 1Password، وقد يرسل مهاجمون رسائل تنتحل صفة الشركة تدعو إلى تأمين الحساب أو إعادة تعيين كلمة المرور أو التحقق من البيانات. على المستخدمين فتح الموقع أو التطبيق مباشرة بدل الروابط في البريد، وعدم مشاركة كلمات المرور أو Secret Keys أو رموز التحقق مع أحد.

ما يجب فعله الآن

1. حدّد الجهات والموظفين الذين يستخدمون 1Password، ودوّن ذلك كتعرّض لطرف ثالث في سجل المخاطر.
2. نبّه المستخدمين إلى رسائل التصيّد التي تستغل هذه الحادثة، خاصة التي تطلب تأمين الحساب أو إعادة تعيين كلمة المرور أو التحقق من البيانات.
3. وجّه المستخدمين إلى الوصول لـ 1Password عبر موقعها أو تطبيقها فقط، وعدم مشاركة كلمات المرور أو Secret Keys أو رموز التحقق.
4. اطلب من فريق الأمن رصد رسائل الدعوة أو استرداد الحساب غير المتوقعة ومراجعة نشاط الدخول المرتبط.
5. اطلب من 1Password تأكيدًا خطيًا بحجم الأثر والمعالجة، وراجع التزامات الإشعار بموجب نظام حماية البيانات الشخصية (PDPL) واللوائح القطاعية إن تعلّقت الحادثة ببيانات شخصية لموظفيك.
6. راجع حماية حسابات GitHub وبيانات اعتماد CI/CD لديك: المصادقة متعددة العوامل ونطاق الرموز ودورة تدويرها.