1Password تكشف عن اختراق طال سجلات عملاء وشيفرة مصدرية دون المساس بالخزائن



أعلنت 1Password أن مهاجمًا استخدم حساب GitHub لأحد موظفيها بعد اختراقه للحصول على سجلات عملاء وشيفرة مصدرية. وتفيد بعدم وجود دليل على الوصول إلى الخزائن المشفرة، والتحقيق مستمر.

- بدأ التحقيق في 19 نوفمبر بعد الاشتباه باختراق حساب GitHub المؤسسي لأحد الموظفين.
- شملت السجلات المكشوفة الأسماء وعناوين البريد وهويات الحسابات والمفاتيح العامة ومعاملات المصادقة وأوقات النشاط وبيانات وصفية غير سرية.
- استولى المهاجم أيضًا على شيفرة مصدرية من مستودعات خاصة ووصل إلى نظام CI/CD، ما قد يكشف بيانات اعتماد للبنية التحتية.
- لا يوجد دليل على تنزيل الخزائن المشفرة أو الوصول إليها، ولم تتأثر تطبيقات العملاء وإضافات المتصفح ومفاتيح الاسترداد.

- لا يزال عدد المتضررين وطريقة الدخول الأولى غير معروفين.

كشفت 1Password، المتخصصة في إدارة كلمات المرور وأمن الهوية، أن مهاجمًا سرق بيانات عملاء وشيفرة مصدرية خاصة بها. وبدأت الشركة التحقيق في 19 نوفمبر بعد الاشتباه باختراق حساب GitHub المؤسسي لأحد موظفيها.

ما الذي تأثر

وفق التقرير، استخدم المهاجم الحساب لنشر شيفرة خبيثة في خدمات الواجهة الخلفية واستخراج سجلات العملاء. وتتضمن هذه السجلات الأسماء وعناوين البريد الإلكتروني وهويات الحسابات والمفاتيح التشفيرية العامة ومعاملات المصادقة وأوقات نشاط الحساب وبيانات وصفية غير سرية. كما حصل المهاجم على شيفرة مصدرية من مستودعات خاصة ووصل إلى نظام CI/CD، ما قد يعرّض بيانات اعتماد البنية التحتية للكشف. وسُرقت كذلك رموز (tokens) من رسائل الدعوة والتهيئة والاسترداد. وأُبلغ عدد صغير من الأشخاص كانوا في مرحلة التهيئة أو الاسترداد وقت الاختراق. وتؤكد الشركة أن هذه الرموز لا تُستغل منفردة، ولا يوجد دليل على الاستيلاء على حسابات.

وشملت بيانات المصادقة المسروقة مُحققات Secure Remote Password. وتقول الشركة إنها لا تصلح للمصادقة المباشرة، وإن تخمين كلمات المرور يتطلب Secret Keys التي لا تخزنها 1Password.

الاستجابة والأسئلة المفتوحة

تفيد الشركة بأن خزائن العملاء والمفاتيح التي تحميها لم تُمس، ولا دليل على الوصول إلى الخزائن المشفرة. ولم تتأثر تطبيقات العملاء وإضافات المتصفح ومفاتيح استرداد الحساب. وعطّلت الشركة الحساب المخترق وأبطلت رمزًا مسروقًا واستبدلت بيانات اعتماد البنية التحتية المحتمل كشفها واستعادت نسخًا سليمة من الخدمات المتأثرة. ولا يزال التحقيق جاريًا بمشاركة خبراء مستقلين.

لا يزال عدد المستخدمين المتضررين وكيفية الدخول الأولى إلى حساب GitHub غير واضحين. وتفيد الشركة بأنه لا يلزم العملاء اتخاذ إجراء، مع الحذر من رسائل التصيد التي تستغل الخبر.

ما يجب فعله الآن

1. تأكد مما إذا كانت جهتكم تستخدم 1Password، وتابعوا مستجدات الشركة مع تقدم التحقيق.
2. نبّهوا الموظفين والمسؤولين إلى رسائل التصيد التي تستغل هذه الحادثة، وأحيلوا الرسائل المشبوهة إلى فريق الأمن.
3. راجعوا حسابات المطورين لديكم: فعّلوا المصادقة متعددة العوامل على GitHub ومنصات مماثلة، ودققوا الوصول إلى المستودعات الخاصة وأنظمة CI/CD.
4. تحققوا من إمكانية تدوير أسرار ورموز CI/CD بسرعة، واختبروا هذه العملية.
5. سجّلوا الحادثة في سجل مخاطر الأطراف الثالثة واطلبوا من المورّد إفادة خطية بشأن الأثر، وفق متطلبات ضوابط الهيئة الوطنية للأمن السيبراني (ECC) وإطار الأمن السيبراني للبنك المركزي السعودي.