Chainstack تكشف عن اختراق لأنظمة الإنتاج وتعرّض بيانات عملاء وتجزئات كلمات المرور



أعلنت Chainstack، مزوّدة البنية التحتية للبلوكتشين، أن جهة غير مصرح لها وصلت إلى أجزاء من بنيتها التحتية، وربطت الحادثة بحملة هجمات واسعة مدعومة بالذكاء الاصطناعي ظهرت الأسبوع الماضي.

- أعلنت Chainstack يوم الثلاثاء أن مهاجماً خارجياً وصل دون تصريح إلى جزء من بنيتها التحتية.
- يشير عنوان الخبر إلى تعرّض بيانات العملاء وتجزئات كلمات المرور.
- تُقيَّم الحادثة على أنها جزء من حملة هجمات واسعة مدعومة بالذكاء الاصطناعي ظهرت الأسبوع الماضي.
- المقتطف المتاح لا يوضح النطاق الكامل أو الجدول الزمني أو التفاصيل التقنية.

كشفت Chainstack، وهي مزوّد لبنية البلوكتشين التحتية، أنها تعرضت لهجوم سيبراني تمكنت خلاله جهة غير

مصرح لها من الوصول إلى بعض أجزاء بنيتها التحتية.

ما الذي أُعلن

وفق الخبر، تقول الشركة إن مهاجماً خارجياً وصل إلى جزء من أنظمتها. ويذكر العنوان أن أنظمة الإنتاج تأثرت وأن بيانات العملاء وتجزئات كلمات المرور تعرضت للانكشاف. وتُقيَّم الحادثة على أنها ضمن حملة هجمات واسعة النطاق تستخدم الذكاء الاصطناعي، وقد ظهرت الأسبوع الماضي.

الجزء المتاح لنا من المصدر موجز؛ فهو لا يبيّن عدد العملاء المتأثرين، ولا أنواع البيانات المعنية، ولا كيفية الوصول، ولا مدة بقاء المهاجم. لذلك لا نستنتج أكثر مما أعلنته الشركة.

الأهمية للجهات المنظَّمة

على الجهات في المملكة التي تستخدم خدمات البلوكتشين أو العقد (nodes)، أو تعتمد على منصات طرف ثالث تحتفظ ببيانات اعتماد، أن تعدّ هذا الخبر دافعاً لمراجعة تعرضها. فانكشاف تجزئات كلمات المرور لا يعني انكشاف كلمات المرور نفسها، لكنه قد يرفع المخاطر إذا كانت كلمات المرور ضعيفة أو مُعاد استخدامها في مواضع أخرى.

والخطوة العملية هي التحقق مما إذا كانت Chainstack ضمن سجل الموردين لديكم، وقراءة إشعار الشركة مباشرة، ثم تحديد الإجراءات الاحترازية بحسب ما يرد فيه. وإذا كانت بيانات شخصية معنية، فعلى الفريقين القانوني وفريق الخصوصية تقييم التزامات الإبلاغ بموجب نظام حماية البيانات الشخصية.

ما يجب فعله الآن

1. تحققوا مما إذا كانت جهتكم أو أي مورد حرج لديكم يستخدم Chainstack، وحدّدوا الحسابات ومفاتيح API المرتبطة بها.
2. اطلعوا على الإشعار الرسمي من Chainstack واتبعوا إرشاداتها بشأن إعادة تعيين بيانات الاعتماد وتدوير المفاتيح.
3. غيّروا كلمات المرور ومفاتيح API المرتبطة بالخدمة، وفعّلوا المصادقة متعددة العوامل متى توفرت.
4. تأكدوا من عدم إعادة استخدام كلمات المرور نفسها في أنظمة أخرى، وأعيدوا تعيينها إن حدث ذلك.
5. راقبوا السجلات بحثاً عن تسجيلات دخول أو نشاط API غير معتاد على الحسابات المعنية.
6. إذا كانت بيانات شخصية قد تأثرت، فكلّفوا الفريقين القانوني والخصوصية بتقييم التزامات الإبلاغ وفق نظام حماية البيانات الشخصية.