Railway تبلّغ عن احتمال وصول غير مصرح به إلى متغيرات البيئة الخاصة بعملائها وتدعو إلى تدوير بيانات الاعتماد



أعلنت Railway رصد نشاط غير معتاد في أنظمة تخزّن متغيرات البيئة لعملائها، وقد يكون طرف غير مصرح له وصل إلى قيم مشفّرة وفك تشفيرها في بعض الحالات، ويقتصر الأثر على فئة من المستخدمين.

- أعلنت Railway، مزوّد منصة كخدمة (PaaS)، عن نشاط غير معتاد مرتبط بأنظمة تخزّن متغيرات البيئة لدى العملاء.
- أظهر التحقيق أن طرفًا غير مصرح له ربما وصل إلى متغيرات بيئة مشفّرة.
- في بعض الحالات ربما حصل هذا الطرف على المحتوى بعد فك تشفيره.
- تقول الشركة إن الأثر يقتصر على فئة من المستخدمين.

- تحثّ Railway العملاء المتأثرين على تدوير بيانات الاعتماد.

أعلنت Railway، وهي مزوّد منصة كخدمة (PaaS)، عن رصد نشاط غير معتاد في أنظمة تخزّن متغيرات البيئة الخاصة بعملائها. وبعد مزيد من التحقيق، خلصت الشركة إلى أن طرفًا غير مصرح له ربما وصل إلى متغيرات بيئة مشفّرة، وحصل في بعض الحالات على محتواها بعد فك تشفيره.

وتفيد Railway بأن الأثر يقتصر على فئة من المستخدمين، وتحثّ العملاء على تدوير بيانات الاعتماد. ولا يتضمن المقتطف المتاح تفاصيل إضافية عن السبب أو الجدول الزمني أو عدد الحسابات المتأثرة.

أهمية الخبر

غالبًا ما تحتوي متغيرات البيئة على **أسرار** مثل مفاتيح واجهات البرمجة وكلمات مرور قواعد البيانات والرموز. وإذا انكشفت هذه القيم فقد تتيح الوصول إلى أنظمة أخرى يتصل بها التطبيق المستضاف، حتى بعد تأمين المنصة نفسها.

الخطوات التالية

على الجهات التي تستضيف أي أحمال أو بيئات اختبار على Railway التعامل مع الحدث بمنطق الاحتياط أولاً. يُنصح بتدوير الأسرار المخزنة على المنصة دون انتظار تأكيد ما إذا كان حسابكم ضمن الفئة المتأثرة، ثم مراجعة سجلات الخدمات المرتبطة بحثًا عن استخدام غير معتاد لتلك البيانات. وإذا كانت بيانات شخصية قابلة للوصول عبر أي بيان اعتماد منكشف، فأشركوا وظيفة حماية البيانات مبكرًا لتقييم أي التزام بالإبلاغ.

ما يجب فعله الآن

1. حصر جميع التطبيقات والبيئات والفرق التي تستخدم Railway، بما فيها المشاريع غير الرسمية أو التجريبية.
2. تدوير جميع الأسرار المخزنة كمتغيرات بيئة على Railway، مثل مفاتيح واجهات البرمجة وكلمات مرور قواعد البيانات والرموز.
3. مراجعة سجلات الخدمات المرتبطة بحثًا عن مصادقة أو وصول غير معتاد باستخدام تلك البيانات.
4. نقل الأسرار إلى منظومة مُدارة لحفظ الأسرار بأقل صلاحيات ممكنة وفترات تدوير محددة متى أمكن.
5. تقييم ما إذا كانت بيانات شخصية قابلة للوصول عبر بيانات اعتماد منكشفة، ومراجعة التزامات الإبلاغ بموجب نظام حماية البيانات الشخصية (PDPL).
6. تسجيل الحدث في سجلات مخاطر الأطراف الثالثة والحوادث وطلب تفاصيل إضافية من Railway.