اختراق OpenCode يكشف مفاتيح API المستخدمة مع مزوّدين خارجيين



أبلغ مشروع OpenCode المفتوح المصدر لبرمجة الذكاء الاصطناعي عددًا محدودًا من المستخدمين بأن مفاتيح API التي استخدموها مع مزوّدين خارجيين تعرّضت للكشف إثر اختراق أمني.

- OpenCode مشروع مفتوح المصدر لبرمجة الذكاء الاصطناعي.
- أبلغ المشروع عددًا محدودًا من المستخدمين بوقوع اختراق أمني.
- البيانات المكشوفة هي مفاتيح API المستخدمة مع مزوّدين خارجيين.
- يربط المصدر الحادثة بسياق هجمات التقطير (distillation) على الذكاء الاصطناعي.
- لم يتوفر من التقرير سوى مقدمته، لذا لم تتأكد تفاصيل أخرى.

ما الذي أُعلن

أبلغ مشروع OpenCode، وهو مشروع مفتوح المصدر لبرمجة الذكاء الاصطناعي، عددًا محدودًا من مستخدميه بأن مفاتيح API التي استخدموها مع مزوّدين خارجيين تعرّضت للكشف نتيجة اختراق أمني. ويورد موقع BleepingComputer الحادثة في سياق هجمات التقطير (distillation) المتواصلة على الذكاء الاصطناعي.

ما لم يتضح بعد

لا يتضمن الجزء المتاح لنا من التقرير كيفية وقوع الاختراق ولا توقيته ولا المزوّدين المعنيين ولا ما إذا أُسيء استخدام المفاتيح. لذلك لم نذكر أيًا من هذه التفاصيل. وننصح بمراجعة التقرير الأصلي وأي إشعار صادر عن المشروع للاطلاع على المستجدات.

أهمية الأمر للجهات المنظَّمة

يربط المطورون أدوات البرمجة بالذكاء الاصطناعي بمزوّدي النماذج الخارجيين عبر مفاتيح API بشكل متزايد. وقد يتيح المفتاح المكشوف عبر أداة طرف ثالث للغير استهلاك الخدمات على حساب الجهة، وقد يكشف حدود ما يُسمح للحساب بالوصول إليه. وحتى لو اقتصر الأثر على عدد محدود من المستخدمين، فعلى أي فريق استخدم هذه الأداة مع مفاتيح مزوّدين أن يتعامل مع احتمال الكشف بجدية.

والاستجابة العملية واضحة: التحقق من استخدام الأداة داخل الجهة، وتدوير أي مفاتيح أُعدّت فيها، ومراجعة سجلات الاستخدام لدى المزوّدين بحثًا عن نشاط غير مفسَّر.

ما يجب فعله الآن

1. التحقق مما إذا كان مطورو الجهة أو فرقها يستخدمون OpenCode.
2. تدوير أي مفاتيح API لمزوّدين كانت مُعدّة في OpenCode دون انتظار تأكيد إساءة استخدامها.
3. مراجعة سجلات الاستخدام والفوترة لدى كل مزوّد بحثًا عن نشاط غير مفسَّر.
4. تضييق صلاحيات المفاتيح وتحديد حدود للإنفاق متى أتاح المزوّد ذلك.
5. نقل مفاتيح API إلى مخزن أسرار مُدار، وإدراج أدوات البرمجة بالذكاء الاصطناعي ضمن سجل الأطراف الثالثة والبرمجيات المعتمدة.