Cursor تربط إضافة Claude Code المخترقة بمفتاح وصول انكشف في اختراق Fireworks AI



أفادت Cursor بأن اختراق إضافة Claude Code من Anthropic في سوقها جاء عبر مفتاح وصول منحته لشركة Fireworks AI وانكشف بعد اختراقها، واستخدمه المهاجم لنسخ بيانات من مصدر للقراءة فقط.

- تقول Cursor إن إضافة Claude Code المزروع فيها برمجيات خبيثة في سوقها نتجت عن سرقة مفتاح وصول.
- كانت Cursor قد أصدرت المفتاح لشركة Fireworks AI.
- بحسب Cursor، انكشف المفتاح لدى Fireworks AI بعد اختراق استهدفها.
- استخدم المهاجم المفتاح لنسخ بيانات من مورد للقراءة فقط.
- المقتطف المتاح من المصدر جزئي ولا يتضمن تفاصيل تقنية إضافية.

أوضحت Cursor كيف جرى اختراق إضافة Claude Code الرسمية من Anthropic في سوق الإضافات التابع لها. وذكرت الشركة في تحديث لها أن مهاجماً حصل على مفتاح وصول كانت قد أصدرته لشركة Fireworks AI.

ما يقوله المصدر

بحسب Cursor، انكشف المفتاح لدى Fireworks AI بعد اختراق استهدف هذه الشركة، ثم استخدمه المهاجم لنسخ بيانات من مورد للقراءة فقط. ويتوقف المقتطف المتاح من المصدر عند هذا الحد، فلا يبيّن نوع البيانات، ولا كيف استُخدمت لتعديل الإضافة، ولا عدد المستخدمين المتضررين.

أهمية الحادثة للجهات الخاضعة للتنظيم

تبيّن الحادثة كيف يمكن لبيانات اعتماد لدى طرف ثالث أن تصبح منفذاً إلى قناة توزيع موثوقة. وغالباً ما تعمل أدوات المطورين وإضافات بيئات التطوير بصلاحيات واسعة على الشيفرة المصدرية والأنظمة الداخلية، لذا تُعد الإضافة المعدّلة مصدر خطر على سلسلة التوريد حتى لو كان الضعف الأصلي لدى مورّد المورّد.

وينبغي ألا تُبنى استنتاجات تتجاوز ما نُشر؛ فقد تصدر Cursor والأطراف الأخرى تفاصيل إضافية، ويُستحسن متابعتها قبل اتخاذ إجراءات معالجة أوسع.

وفي الأثناء، يُنصح بمراجعة أدوات البرمجة بالذكاء الاصطناعي والإضافات المستخدمة، ومن أصدر بيانات الاعتماد التي تعتمد عليها، ومدى سرعة إبطالها إذا اختُرق أحد الشركاء.

ما يجب فعله الآن

1. حصر مساعدات البرمجة بالذكاء الاصطناعي وإضافات بيئات التطوير المستخدمة لدى فرق الهندسة، ومنها Cursor وClaude Code.
2. متابعة النشرات الصادرة عن الجهات المزودة وتطبيق أي خطوات معالجة تُعلنها بشأن الإضافة المتأثرة.
3. مراجعة المفاتيح والرموز الممنوحة لمزودي الذكاء الاصطناعي من الأطراف الثالثة، والتأكد من تقييد صلاحياتها بالحد الأدنى وإمكانية إبطالها بسرعة.
4. تدوير بيانات الاعتماد المشتركة مع الموردين عند إبلاغ أي مورد عن اختراق.
5. إدراج مصادر الإضافات وإصداراتها ضمن مراجعات مخاطر الأطراف الثالثة وفق ضوابط سلسلة التوريد في ضوابط NCA ECC وإطار SAMA CSF.