سير عمل خبيث في GitHub Actions لسرقة بيانات الاعتماد يصل إلى أكثر من 340 مستودعًا عبر حسابات مشرفين مخترقة



يفيد باحثون بحملة مستمرة استخدمت حسابين مخترقين لمشرفين على مشاريع مفتوحة المصدر لدفع سير عمل يسرق بيانات الاعتماد إلى أكثر من 340 مستودعًا على GitHub.

- توصف الحملة بأنها مستمرة وتهدف إلى سرقة بيانات الاعتماد.
- اختُرق حسابان لمشرفين بارزين على مشاريع مفتوحة المصدر.
- دُفع سير عمل خبيث إلى أكثر من 340 مستودعًا.
- يعود أحد الحسابين إلى مؤلف محرك الألعاب pyxel الذي يحمل 18,400 نجمة، وشملت العملية 27 مستودعًا بدءًا من الساعة 13:20 بالتوقيت العالمي.
- تعود التفاصيل إلى الباحثين في StepSecurity.

كشف باحثون عن حملة مستمرة لسرقة بيانات الاعتماد تستغل GitHub Actions. وبحسب التقرير، اخترق المهاجمون حسابين لمشرفين بارزين على مشاريع مفتوحة المصدر، واستخدموهما لدفع سير عمل خبيث إلى أكثر من 340 مستودعًا.

ما الذي رُصد

ذكرت StepSecurity أن أحد الحسابين يعود إلى Takashi Kitao، مؤلف محرك الألعاب pyxel الذي يحمل 18,400 نجمة. ومن خلال هذا الحساب دفع المهاجم سير العمل الخبيث إلى 27 مستودعًا بدءًا من الساعة 13:20 بالتوقيت العالمي. ويهدف سير العمل إلى سرقة بيانات الاعتماد. ويشير عنوان المصدر إلى نطاق أوسع بكثير، بينما تتحدث التفاصيل المقتبسة عن أكثر من 340 مستودعًا، لذا ينبغي اعتبار حجم الحملة الكامل ما يزال قيد التكشف.

لماذا يهم ذلك

تعمل سير العمل داخل بيئة البناء الخاصة بالمستودع، وغالبًا ما تحتوي هذه البيئة على رموز وأسرار. وقد يبدو سير عمل أُضيف عبر حساب مشرف موثوق عاديًا عند المراجعة. وقد تتعرض الجهات التي تستنسخ المشاريع المتأثرة أو تعتمد عليها، أو تشغّل خطوط GitHub Actions الخاصة بها، للخطر إذا كانت الأسرار متاحة لتلك السير.

لا يسمّي المصدر ضحايا محددين غير حسابي المشرفين، ولا يورد مؤشرات اختراق في المقتطف المتاح. يُنصح بمتابعة منشور StepSecurity لمعرفة المستجدات.

ما يجب فعله الآن

1. ابحث في مستودعاتك والنسخ المتفرعة عن ملفات سير العمل المضافة أو المعدّلة حديثًا، خاصة من حسابات المشرفين، وراجعها بحثًا عن اتصالات شبكية غير متوقعة أو وصول إلى الأسرار.
2. بدّل الرموز والأسرار المخزنة في GitHub Actions لأي مستودع شغّل سير عمل مشبوهًا.
3. قيّد صلاحيات سير العمل إلى الحد الأدنى، واشترط مراجعة أي تغيير في مجلد workflows.
4. فعّل المصادقة متعددة العوامل وراجع صلاحيات حسابات المشرفين وحسابات الخدمة في GitHub الخاص بمؤسستك.
5. احصر المشاريع مفتوحة المصدر التي تعتمد عليها خطوط التطوير، وثبّت إجراءات الأطراف الثالثة على إصدارات تمت مراجعتها.
6. أبلغ عن أي تعرض مؤكد عبر عملية إدارة الحوادث لديك، وإلى الهيئة الوطنية للأمن السيبراني والجهة القطاعية المنظِّمة عند الاقتضاء.