تثبيت SHA وحده لا يحمي من هجمات سلسلة توريد GitHub Actions



يفيد تقرير بأن المهاجمين وجدوا طريقة لتجاوز تثبيت SHA في GitHub Actions. ففي مارس 2026 زرع من اختطفوا ماسح Trivy شيفرة خبيثة بدت كأنها من أداة checkout الرسمية من GitHub.

- يُستخدم تثبيت SHA على نطاق واسع بوصفه دفاعاً رئيسياً ضد هجمات سلسلة توريد البرمجيات.
- يذكر المصدر أن المهاجمين وجدوا بالفعل طريقة لتجاوزه.
- في مارس 2026 زرع مختطفو ماسح Trivy مفتوح المصدر شيفرة خبيثة.
- صُممت الشيفرة لتبدو كأنها صادرة عن أداة checkout الرسمية من GitHub.
- المصدر مادة ترويجية لندوة، لذا فالتفاصيل التقنية فيه محدودة.

ما الذي ورد في التقرير

أصبح تثبيت GitHub Actions على نسخة محددة من الشيفرة، المعروف بتثبيت SHA، دفاعاً شائعاً ضد هجمات سلسلة توريد البرمجيات. وبحسب The Hacker News، فقد وجد المهاجمون بالفعل طريقة لتجاوزه.

ويستشهد التقرير بحالة وقعت في مارس 2026، حين زرع من اختطفوا Trivy، وهو ماسح أمني مفتوح المصدر واسع الاستخدام، شيفرة خبيثة بدت كأنها صادرة عن أداة checkout الرسمية من GitHub.

لماذا يهم ذلك

تعتبر فرق كثيرة أن المرجع المثبّت دليل على موثوقية الشيفرة. ويشير التقرير إلى أن هذا الافتراض ناقص، فالتثبيت يحدد نسخة بعينها لكنه لا يثبت وحده أن الشيفرة خلفه هي ما تبدو عليه. كما أن أدوات الأمن، ومنها الماسحات، تعمل بصلاحيات داخل بيئات البناء، فتصبح هدفاً جذاباً.

المصدر مادة قصيرة للترويج لندوة ولا يشرح الأسلوب بالتفصيل، لذا ينبغي تجنب استنتاجات تتجاوز ما ذُكر.

الخطوة التالية

يُنصح بالنظر إلى تثبيت SHA بوصفه ضابطاً واحداً ضمن ضوابط عدة، ومراجعة كيفية إشارة خطوط البناء إلى الإجراءات الخارجية، ومن يملك تعديلها، وما الصلاحيات الممنوحة لها. وفيما يلي نقطة انطلاق عملية.

ما يجب فعله الآن

1. حصر جميع إجراءات GitHub Actions والماسحات الخارجية المستخدمة في خطوط البناء، ومنها Trivy وخطوات checkout.
2. التحقق مما إذا كان Trivy مستخدماً في خطوط البناء لديكم حوالي مارس 2026 ومراجعة سجلات البناء ذات الصلة.
3. حصر صلاحيات رموز الوصول والأسرار في كل مهمة بالحد الأدنى اللازم.
4. إضافة مراجعة واعتماد لأي تغيير في ملفات سير العمل ومراجع الإجراءات.
5. إدراج مخاطر سلسلة توريد CI/CD ضمن تقييم مخاطر الأطراف الثالثة والتطوير الآمن.