GitHub تضيف مهلة انتهاء مدتها 48 ساعة لإعدادات النشر الموثوق غير المُتحقَّق منها في npm



باتت GitHub تُنهي صلاحية إعدادات النشر الموثوق في npm غير المُتحقَّق منها بعد 48 ساعة من إنشائها، عقب بحث بيّن إمكانية نشر إصدارات جديدة لحزمة مستخدم آخر دون سرقة بيانات اعتماده.

- تُنهي GitHub صلاحية إعدادات النشر الموثوق في npm غير المُتحقَّق منها بعد 48 ساعة من إنشائها.
- وجد باحثون أن بإمكان مهاجم نشر إصدارات جديدة من حزمة مستخدم آخر دون سرقة بيانات اعتماده.
- يصبح الإعداد مُتحقَّقًا منه ومعفى من الانتهاء بعد أول عملية نشر ناجحة.
- يشير عنوان الخبر إلى أن أكثر من 1,500 حزمة كانت عرضة للاختطاف.

غيّرت GitHub طريقة عمل النشر الموثوق في npm بعد أن أظهر باحثون وجود خلل يتيح لمهاجم نشر إصدارات

جديدة من حزمة تعود لمستخدم آخر، دون الحاجة إلى سرقة بيانات اعتماد ذلك المستخدم.

ما الذي تغيّر

بموجب القاعدة الجديدة، تنتهي صلاحية إعداد النشر الموثوق الذي لم يُتحقَّق منه بعد 48 ساعة من إنشائه. وتوضح GitHub أن الإعداد يصبح مُتحقَّقًا منه ومعفى من الانتهاء بمجرد نجاح أول عملية نشر. ويذكر عنوان الخبر أن أكثر من 1,500 حزمة كانت عرضة للاختطاف بسبب هذا الخلل.

أهمية الخبر

يهدف النشر الموثوق إلى الاستغناء عن الرموز طويلة الأمد في مسارات الإصدار. ولذلك فإن أي ضعف في هذه الآلية مهم، إذ قد يصل إصدار خبيث إلى المستخدمين عبر تحديث اعتيادي دون وجود سرقة بيانات اعتماد يمكن رصدها. وترث الجهات التي تعتمد على حزم npm، مباشرة أو عبر مورّديها، هذا التعرض.

لا يوضح المقتطف المتاح من المصدر كيفية استغلال الخلل، ولا ما إذا كان قد استُغل فعليًا، ولا أسماء الحزم المتأثرة. لذا ينبغي عدم افتراض أي من ذلك، والتحقق بدلاً منه من الإعدادات والاعتماديات الخاصة بكل جهة.

نظرة عملية

يضيّق انتهاء الصلاحية بعد 48 ساعة النافذة التي قد يُساء فيها استخدام إعداد معلّق غير مُتحقَّق منه، لكنه لا يغني عن مراجعة الإعدادات القائمة. وعلى مسؤولي الحزم التأكد من أن كل إعداد نشر موثوق مقصود وأنه أتمّ أول عملية نشر مشروعة.

ما يجب فعله الآن

1. مراجعة جميع إعدادات النشر الموثوق في npm للحزم التي تنشرها جهتكم، وإزالة أي إعداد غير معروف.
2. التأكد من أن كل إعداد أتمّ أول عملية نشر مشروعة وأنه ما زال مطلوبًا.
3. فحص الإصدارات الأخيرة للحزم التي تنشرونها بحثًا عن إصدارات لم يعدّها أو يعتمدها فريقكم.
4. الاستفسار من مورّدي البرمجيات والفرق الداخلية عن استخدامهم للنشر الموثوق في npm وكيفية تعاملهم مع الخبر.
5. تثبيت إصدارات الاعتماديات ومراجعة التغييرات في ملفات القفل قبل نقل التحديثات إلى بيئة الإنتاج.