اختراق حزمة LiteLLM البرمجية في هجوم على سلسلة التوريد



أفادت تقارير باختراق الإصدار 1.107.0 من LiteLLM الموزَّع عبر PyPI وصور Docker، وتضمّن أداة لسرقة بيانات الاعتماد وباباً خلفياً. وقد حُجرت الحزمة في PyPI.

- الإصدار المتأثر هو LiteLLM 1.107.0.
- جرى توزيعه عبر حزم wheels في PyPI وصور Docker.
- تضمّن الحمل الخبيث أداة لسرقة بيانات الاعتماد وباباً خلفياً.
- أبلغت عن الحادثة SafeDep وSocket وStepSecurity وUpwind.
- حُجرت الحزمة في PyPI.

ما الذي ورد في التقارير

أفاد باحثون في SafeDep وSocket وStepSecurity وUpwind بأن حزمة LiteLLM الشائعة في بيئة Python تعرضت للاختراق ضمن هجوم على سلسلة التوريد البرمجية. والإصدار المتأثر هو 1.107.0 الذي وُزّع عبر حزم wheels في PyPI وكذلك عبر صور Docker. وبحسب التقارير، فقد حمل أداة لسرقة بيانات الاعتماد إلى جانب باب خلفي.

وقد حُجرت الحزمة في فهرس حزم Python (PyPI). ولا يتضمن المقتطف المتاح تفاصيل تقنية إضافية، مثل كيفية وقوع الاختراق أو النطاق الكامل للتعرض أو البيانات المستهدفة.

لماذا يهم ذلك

قد يمنح وجود أداة سرقة بيانات اعتماد وباب خلفي في إحدى التبعيات المهاجمَ وصولًا إلى الأسرار المخزنة في البيئات التي تعمل فيها الحزمة، ومنفذاً دائماً إليها. ولأن الإصدار وصل عبر قناتي الحزم والحاويات، ينبغي للمنشآت فحص تبعيات تطبيقاتها والصور المبنية لديها على حد سواء.

النهج المقترح

يُعدّ أي بيئة ثبّتت الإصدار 1.107.0 أو شغّلته معرّضة للخطر إلى أن يثبت خلاف ذلك. وتكون الأولوية لتحديد أماكن وجود هذا الإصدار، ثم الاحتواء وتدوير بيانات الاعتماد احترازياً. ومن المناسب متابعة نشرات الجهات الموردة والباحثين للاطلاع على مؤشرات الاختراق والإصدارات المصححة، نظراً لمحدودية المعلومات المتاحة حالياً.

ما يجب فعله الآن

1. البحث في مستودعات الشيفرة وملفات القفل وخطوط CI وسجلات الحاويات عن LiteLLM 1.107.0.
2. عزل أي خادم أو حاوية ثبّتت هذا الإصدار أو شغّلته والتحقيق في احتمال اختراقها.
3. تدوير مفاتيح API والرموز وسائر بيانات الاعتماد التي يمكن الوصول إليها من البيئات المتأثرة.
4. تثبيت إصدارات التبعيات واعتماد مرآة داخلية للحزم مع مراجعة الإصدارات الجديدة قبل اعتمادها.
5. متابعة نشرات الباحثين للحصول على مؤشرات الاختراق والإصدارات المصححة، وتوثيق الحادثة ضمن عملية إدارة مخاطر البرمجيات الخارجية.