اختراق إصدار LiteLLM 1.107.0 في هجوم على سلسلة التوريد لسرقة بيانات الاعتماد



اخترق مهاجمون مسار إصدار LiteLLM في 21 أكتوبر ونشروا النسخة 1.107.0 المحمّلة ببرمجية تسرق بيانات الاعتماد عبر PyPI وسجلات Docker. يُنصح بالرجوع إلى 1.106.2 وتدوير جميع الأسرار المكشوفة.

- اختُرق مسار إصدار LiteLLM في 21 أكتوبر ونُشرت النسخة 1.107.0 على PyPI وسجل Docker.
- تأثرت جميع حزم wheel السبع للنسخة 1.107.0 على Windows وLinux وmacOS، ويذكر المطوّر أن عملاء النسخة المؤسسية الخاصة لم يتأثروا.
- تستهدف البرمجية بيانات الاعتماد السحابية وأدوات الذكاء الاصطناعي والمطورين وCI/CD والمفاتيح الخاصة وبيانات المتصفح ومتغيرات البيئة.
- ثلاثة ملفات في مجلد مكتبات Python تعمل عند كل تشغيل لـ Python، حتى تشغيل Python أو pip للفحص يفعّل البرمجية.
- النسخة النظيفة الموصى بها هي 1.106.2، مع عزل الأنظمة المصابة وإعادة بنائها وتدوير الأسرار.

أفاد مطورو LiteLLM، وهي حزمة Python مفتوحة المصدر وبوابة للذكاء الاصطناعي تتيح للتطبيقات الوصول إلى نماذج من مزوّدين مختلفين عبر واجهة برمجية واحدة، بأن مسار الإصدار لديهم اختُرق في 21 أكتوبر. ونشر المهاجم النسخة 1.107.0 على PyPI وفي سجل Docker. ويصف المطوّر هذه النسخة بأنها تحتوي على برمجية خبيثة مجمّعة تسرق بيانات الاعتماد وتحمّل أدوات تنفيذ أوامر عن بُعد.

ما الذي تأثر

كانت جميع حزم wheel السبع للنسخة litellm 1.107.0 متاحة لنحو ساعتين في 21 أكتوبر (بالتوقيت العالمي). كما أشارت وسوم في Docker Hub وGHCR، منها v1.107.0 وlatest، إلى صور مخترقة خلال اليوم نفسه. ووفق الباحثين، لم يُعدَّل كود التطبيق نفسه، بل عُدّلت حزمة التثبيت فقط بإضافة ثلاثة ملفات (cook.pth وcook.py وsitecustomize.py) إلى مجلد مكتبات Python، وتعمل عند كل تشغيل لـ Python في تلك البيئة.

تستهدف البرمجية بيانات الاعتماد السحابية وبيانات النشر، وبيانات أدوات الذكاء الاصطناعي وإعدادات المزوّدين المخزنة، وأسرار المطورين مثل رموز Git وnpm وPyPI وCI/CD، ومفاتيح SSH وGPG وTLS، وبيانات المتصفح ومتغيرات البيئة. وتُشفَّر البيانات المسروقة قبل رفعها إلى عنوان خارجي. كما يشغّل أحد الملفات محمّلًا منفصلًا يتحقق كل ساعة من مؤشر مستضاف على GitHub ثم ينزّل شيفرة Python إضافية لتنفيذها على الجهاز.

إرشادات التعافي

أُزيلت الحزم الخبيثة. وعلى من يُحتمل أنه ثبّتها إيقاف الأنظمة المتأثرة وفحص البيئات دون تشغيل مفسّر Python، لأن تشغيل Python أو pip يفعّل الحمولة. ينبغي عزل الأنظمة المصابة وإعادة بنائها من نسخ احتياطية نظيفة وتدوير جميع الأسرار المكشوفة فورًا. وقد يترك حذف مجلد LiteLLM وحده ملفات تشغيل أو محمّلًا نشطًا. والنسخة الموصى بها للتعافي هي 1.106.2، آخر إصدار نظيف قبل الهجوم.

ما يجب فعله الآن

1. حدّدوا كل نظام وصورة حاوية ومهمة CI/CD ثبّتت أو سحبت LiteLLM 1.107.0 أو وسوم maing latest في 21 أكتوبر.
2. أوقفوا النشرات المتأثرة وافحصوها دون تشغيل Python أو pip، واعزلوا الأجهزة المصابة وأعيدوا بناءها من نسخ احتياطية نظيفة.
3. دوّروا جميع الأسرار المتاحة من البيئات المتأثرة: السحابة وKubernetes وDocker وGit وnpm وPyPI وCI/CD ومفاتيح SSH وGPG وTLS ومفاتيح مزوّدي الذكاء الاصطناعي.
4. ثبّتوا LiteLLM على النسخة 1.106.2، واعتمدوا تثبيت الإصدارات أو بصمات الصور للتبعيات والحاويات بدل الوسوم المتغيرة.
5. راجعوا حركة الشبكة الصادرة بحثًا عن اتصالات بـ litellm[.]dev، وأبلغوا عن أي كشف مؤكد وفق إجراءات الحوادث الداخلية ومتطلبات الهيئة الوطنية للأمن السيبراني والبنك المركزي السعودي ذات الصلة.