

منصة Langflow للذكاء الاصطناعي تواجه استغلالاً نشطاً لثغرة حرجية في تنفيذ الأوامر عن بُعد



ثغرة حرجية في تنفيذ الأوامر عن بُعد تتطلب مصادقة في منصة Langflow مفتوحة المصدر لتطبيقات الذكاء الاصطناعي تعرضت لأكثر من 1400 محاولة استغلال سجلتها أنظمة الفخاخ الأمنية.

- الثغرة CVE-2026-105740 هي ثغرة حرجية في تنفيذ الأوامر عن بُعد تتطلب مصادقة في Langflow بدرجة خطورة 9.9 على مقياس CVSS
- سجل باحثو الأمن السيبراني في Previdian 1423 محاولة استغلال ضد أنظمة الفخاخ الأمنية
- Langflow منصة مفتوحة المصدر لبناء تطبيقات الذكاء الاصطناعي وسير العمل الوكيل
- استحوذت IBM على شركة DataStax الأم لـ Langflow في فبراير 2025
- الجهات التهديدية تستهدف الثغرة بشكل نشط في البيئات الحقيقية

تفاصيل الثغرة الأمنية

تم اكتشاف ثغرة أمنية حرجة تحمل الرمز **CVE-2026-105740** في منصة Langflow مفتوحة المصدر التي يستخدمها المطورون لبناء تطبيقات الذكاء الاصطناعي وسير العمل الوكيل. تحمل الثغرة درجة خطورة 9.9 على مقياس CVSS، مما يشير إلى مخاطر عالية للغاية. تتيح الثغرة تنفيذ الأوامر عن بُعد للمستخدمين المصادق عليهم، مما يسمح للجهات التهديدية التي حصلت على بيانات اعتماد صالحة بتنفيذ أوامر برمجية عشوائية على الأنظمة المتأثرة. أصدر باحثو الأمن السيبراني في Previdian تنبيهاً يؤكد أن الثغرة تتعرض للاستغلال النشط. سجلت أنظمة الفخاخ الأمنية لديهم 1423 محاولة استغلال متميزة، مما يدل على اهتمام مستمر من المهاجمين بهذه الثغرة.

سياق المنصة

تُدار منصة Langflow من قبل شركة DataStax التي استحوذت عليها IBM في فبراير 2025. بصفتها منصة مفتوحة المصدر، يتم نشر Langflow عبر بيئات متنوعة حيث تقوم المؤسسات بتطوير تطبيقات مدفوعة بالذكاء الاصطناعي وسير عمل آلي. يزيد الانتشار الواسع للمنصة في مجتمع تطوير الذكاء الاصطناعي من سطح الهجوم المحتمل لهذه الثغرة.

مشهد التهديدات

يشير الاستغلال النشط الذي رصدته Previdian إلى أن الجهات التهديدية طورت أدوات استغلال فعالة وتقوم بمسح منهجي للبحث عن نسخ Langflow الضعيفة. تشير طبيعة الثغرة التي تتطلب مصادقة إلى أن المهاجمين قد يجمعون بين تقنيات اختراق بيانات الاعتماد وثغرة تنفيذ الأوامر عن بُعد للحصول على وصول أعمق إلى الأنظمة المستهدفة.

يجب على المؤسسات التي تدير نسخ Langflow أن تتعامل مع هذا الأمر كمسألة أمنية عاجلة تتطلب اهتماماً ومعالجة فورية.

ما يجب فعله الآن

1. إجراء جرد فوري لجميع نسخ Langflow المنشورة عبر بيئات التطوير والاختبار والإنتاج
2. تطبيق التحديثات الأمنية الصادرة من DataStax للثغرة CVE-2026-105740 دون تأخير
3. مراجعة وتعزيز آليات المصادقة لجميع نسخ Langflow مع تطبيق المصادقة متعددة العوامل حيثما أمكن
4. مراجعة سجلات الوصول لأنظمة Langflow لتحديد أي نشاط مشبوه في المصادقة أو تنفيذ الأوامر منذ الإفصاح عن الثغرة
5. عزل نسخ Langflow غير المحدثة عن شبكات الإنتاج حتى اكتمال المعالجة
6. التنسيق مع فرق تطوير التطبيقات لتقييم التأثير المحتمل على مشاريع سير عمل الذكاء الاصطناعي وإنشاء ممارسات نشر آمنة