ثغرة حرجة في Apache Roller قيد الاستغلال الفعلي تتيح تنفيذ الأوامر عن بُعد دون مصادقة



أفادت Apache Software Foundation باستغلال الثغرة (CVSS 9.8) CVE-2026-129448 في Apache Roller، وهي تقع في نقطة XML-RPC وقد تتيح تنفيذ الأوامر عن بُعد دون مصادقة.

- Apache Roller منصة تدوين مفتوحة المصدر مبنية على Java.
- تحمل الثغرة الرقم CVE-2026-129448 وبدرجة CVSS تبلغ 9.8.
- تتمثل في فك تسلسل بيانات غير موثوقة دون مصادقة في نقطة XML-RPC.
- قد يؤدي الاستغلال الناجح إلى تنفيذ الأوامر عن بُعد.
- تفيد Apache Software Foundation بأن الثغرة مستغلة فعلياً.

ما الذي أُعلن

أشارت Apache Software Foundation (ASF) إلى أن ثغرة حرجة في Apache Roller يجري استغلالها فعلياً. وApache Roller منصة تدوين مفتوحة المصدر مكتوبة بلغة Java.

تحمل الثغرة الرقم CVE-2026-129448 وبدرجة CVSS تبلغ 9.8. وهي ضعف في فك تسلسل بيانات غير موثوقة دون مصادقة في نقطة XML-RPC، وقد يتيح للمهاجم تنفيذ شيفرة عن بُعد على الخادم المتأثر.

أهمية الأمر

لأن الاستغلال لا يتطلب مصادقة، فإن أي نسخة من Roller يمكن الوصول فيها إلى النقطة المتأثرة هدف محتمل. ويعني الاستغلال الفعلي أن المهلة بين الإفصاح والهجوم قد انتهت. ولا يذكر المقتطف المتاح الإصدارات المتأثرة أو الإصدارات المصححة، لذا ينبغي الرجوع إلى نشرة ASF الرسمية لمعرفتها.

النهج المقترح

على الجهات أن تحدد أولًا ما إذا كان Apache Roller مستخدماً في بيئتها، بما في ذلك بوابات المعرفة الداخلية والمواقع التسويقية والأنظمة التي يديرها أطراف ثالثة. وعند العثور عليه، يُقلَّل انكشاف نقطة XML-RPC بينما تُراجع إرشادات المورّد وتُطبَّق.

وإذا كانت النسخة متاحة من الإنترنت، فتُعامل على أنها قد تكون مخترقة إلى أن تثبت المراجعة خلاف ذلك، مع حفظ السجلات للتحقيق.

ما يجب فعله الآن

1. حصر جميع نسخ Apache Roller بما فيها التي يديرها الموردون أو وحدات الأعمال.
2. مراجعة نشرة ASF الرسمية لمعرفة الإصدارات المتأثرة والمصححة وتطبيق التحديث.
3. تقييد الوصول من الإنترنت إلى نقطة XML-RPC أو حجبه إلى حين التصحيح.
4. فحص سجلات الويب والتطبيق بحثاً عن طلبات XML-RPC مشبوهة وحفظها.
5. التعامل مع النسخ المكشوفة للإنترنت على أنها قد تكون مخترقة وبدء الفرز الأولي للحادث.
6. إبلاغ الجهة التنظيمية القطاعية عن الحوادث المؤكدة عبر القنوات المطلوبة.