محاولات استغلال ثغرتي GeoServer رقم CVE-2026-120705 وCVE-2026-129243



رصدت WatchTowr محاولات فحص لثغرتين عاليتي الخطورة في GeoServer يمكن ربطهما لتنفيذ أوامر عن بُعد دون مصادقة. التحديثات متاحة: 3.0.2 أو 2.28.6 أو 2.27.7.

- رصدت WatchTowr محاولات استغلال للثغرتين CVE-2026-120705 وCVE-2026-129243، ويبدو أن هدفها تحديد الخوادم القابلة للاختراق.
- لم يُبلَّغ عن نجاح تنفيذ أوامر عن بُعد، ولم ترد تقارير أخرى عن الاستغلال وقت النشر.
- الثغرتان ضمن سلسلة من خمس ثغرات اكتشفها باحث في Rapid7، ونُشرت التفاصيل التقنية وشيفرة PoC هذا الأسبوع.
- أثبتت Eye Security إمكان تنفيذ أوامر عن بُعد دون مصادقة على Linux وWindows، ورصدت أكثر من 3000 نسخة متاحة عبر الإنترنت.
- الإصدارات المعالجة هي GeoServer 3.0.2 و2.28.6 و2.27.7.

يستهدف المهاجمون ثغرتين أُعلن عنهما حديثًا في GeoServer، ويمكن ربطهما بثغرات أخرى لتحقيق تنفيذ أوامر عن بُعد (RCE) دون مصادقة. وGeoServerg تطبيق مفتوح المصدر لنشر البيانات الجغرافية المكانية ومشاركتها، وتستخدمه على نطاق واسع جهات حكومية ومرافق خدمية.

ما الذي يحدث

رصدت WatchTowr محاولات استغلال للثغرتين CVE-2026-120705 وCVE-2026-129243، وكلتاهما عالية الخطورة. ويبدو أن الفحوصات تهدف إلى تحديد الخوادم المعرّضة، عبر طلبات قائمة على الأخطاء تنشئ استعلامات مخزّنة وتستدعيها. ولم تُبلغ WatchTowr عن نجاح أي تنفيذ أوامر عن بُعد، ولم يذكر المصدر تقارير أخرى عن الاستغلال وقت كتابته.

الثغرة CVE-2026-120705 هي حقن XML قد يتيح لمهاجم غير مصادَق قراءة ملفات حساسة أو تنفيذ هجمات تزوير الطلبات من جانب الخادم (SSRF). أما CVE-2026-129243 فتتيح تجاوز ضوابط الوصول وتنفيذ عمليات مخصصة عادةً للمسؤولين.

لماذا يهم ذلك

تنتمي الثغرتان إلى سلسلة من خمس ثغرات أبلغ عنها الباحث في Rapid7 جوناه بورغس مطوّري GeoServer في أوائل أغسطس. وتضم السلسلة أيضًا CVE-2026-129244 وCVE-2026-129245 وCVE-2026-129242، وتبيّن كيف يمكن للمهاجم الحصول على صلاحيات إدارية وتنفيذ أوامر بصلاحيات عملية GeoServer. ونُشرت التفاصيل التقنية وشيفرة PoC هذا الأسبوع. كما أثبتت Eye Security بصورة مستقلة تنفيذ أوامر عن بُعد دون مصادقة على Linux وWindows بدمج CVE-2026-120705 وCVE-2026-129245 وCVE-2026-120704، وحددت أكثر من 3000 نسخة متاحة عبر الإنترنت.

ما العمل

أصدرت GeoServer تحديثات قبل عدة أسابيع ونشرت نشرات أمنية في الأيام الأخيرة. ينبغي للمؤسسات الترقية إلى GeoServer 3.0.2 أو 2.28.6 أو 2.27.7. ومع توفر شيفرة PoC علنًا، يجب إعطاء الأولوية للنسخ المكشوفة على الإنترنت.

ما يجب فعله الآن

1. حصر جميع نسخ GeoServer، بما فيها التي تديرها الإدارات أو أطراف ثالثة، وتحديد المكشوف منها على الإنترنت.
2. الترقية إلى GeoServer 3.0.2 أو 2.28.6 أو 2.27.7 بدءًا بالنسخ المكشوفة على الإنترنت.
3. مراجعة سجلات الويب والتطبيق بحثًا عن طلبات قائمة على الأخطاء تنشئ استعلامات مخزّنة أو تستدعيها، وتصعيد أي مؤشرات إلى فريق الاستجابة للحوادث.
4. التحقق من عدم وجود تغييرات إدارية غير متوقعة في GeoServer ومن تشغيل الخدمة بأقل الصلاحيات.
5. إذا تعذّر التحديث الفوري، تقييد الوصول إلى GeoServer بالشبكات الموثوقة حتى اكتمال الترقية.