استغلال فعلي لثغرتين في GeoServer وتحذيرات من سلاسل تنفيذ أوامر عن بُعد دون مصادقة



أفادت watchTowr بأن مهاجمين يستغلون فعليًا ثغرتين حديثتي الإصلاح في GeoServer هما CVE-2026-120705 وCVE-2026-129243، مع تحذير من سلاسل تنفيذ أوامر عن بُعد دون مصادقة.

- تفيد watchTowr بأن جهات تهديد تستغل فعليًا ثغرتين حديثتي الإصلاح في GeoServer.
- الثغرتان هما CVE-2026-120705 وCVE-2026-129243.
- تبلغ درجة CVSS للثغرة CVE-2026-120705 8.6، وهي ثغرة قراءة ملفات اعتباطية.
- قد تتيح الوصول إلى الملفات النصية المحلية التي تستطيع عملية GeoServer قراءتها.
- يحذّر الباحثون من إمكانية استخدام الثغرات ضمن سلاسل تنفيذ أوامر عن بُعد دون مصادقة.

ما الذي ورد في التقرير

وفق watchTowr، يستغل مهاجمون حاليًا ثغرتين تم إصلاحهما حديثًا في GeoServer، وهما CVE-2026-120705 وCVE-2026-129243. كما يحذّر الباحثون من إمكانية الجمع بين هذه الثغرات في سلاسل تنفيذ أوامر عن بُعد دون مصادقة.

ما المعروف عن الثغرتين

تبلغ درجة CVSS للثغرة CVE-2026-120705 8.6، وهي ثغرة **قراءة ملفات اعتباطية** قد تتيح للمهاجم الوصول إلى الملفات النصية المحلية التي تستطيع عملية GeoServer قراءتها. المقتطف المتاح من المصدر غير مكتمل، ولذلك لا يتضمن تفاصيل الثغرة الثانية ولا سلاسل الاستغلال الكاملة. ننصح بالرجوع مباشرة إلى نشرات المورّد وwatchTowr للاطلاع على التفاصيل التقنية.

لماذا يهم ذلك

بما أن الاستغلال يُذكر بوصفه فعليًا وأن الإصلاحات متوفرة، فإن الفترة بين صدور التحديث وبدء الهجمات قصيرة. وينبغي التعامل مع أي نسخة GeoServer يمكن الوصول إليها من شبكات غير موثوقة ولم تُحدَّث بعد بوصفها أولوية عاجلة.

على الجهات التي تستخدم GeoServer في الخرائط أو الخدمات الجيومكانية، بما في ذلك التطبيقات الداخلية، تحديد أماكن تشغيله والإصدار المثبّت.

ما يجب فعله الآن

1. حصر جميع نسخ GeoServer، بما فيها البيئات الداخلية والاختبارية، وتوثيق إصداراتها.
2. تطبيق تحديثات المورّد الخاصة بالثغرتين CVE-2026-120705 وCVE-2026-129243 على سبيل الأولوية.
3. تقييد تعرّض واجهات الإدارة والخدمة في GeoServer للإنترنت إلى حين اكتمال التحديث.
4. مراجعة سجلات الويب والتطبيقات بحثًا عن طلبات قراءة ملفات غير معتادة أو نشاط غير متوقع للعمليات.
5. تغيير بيانات الاعتماد أو الأسرار المخزنة في ملفات يمكن لعملية GeoServer قراءتها عند الاشتباه بوقوع اختراق.