CISA تضيف ثلاث ثغرات مستغلة في GeoServer وDrupal إلى كتالوج الثغرات المستغلة المعروفة



أضافت CISA ثغرتين في OSGeo GeoServer وثغرة في Drupal Core إلى كتالوج KEV بناءً على أدلة استغلال فعلي. على الجهات التي تستخدم هذه المنتجات مراجعة تعرّضها وإعطاء المعالجة أولوية.

- أضافت CISA ثلاث ثغرات إلى كتالوج KEV استناداً إلى أدلة على استغلالها فعلياً.
- الثغرة CVE-2026-120705 حقن XML، والثغرة CVE-2026-129243 تفويض غير سليم، وكلتاهما في OSGeo GeoServer.
- الثغرة CVE-2026-136716 خلل في التحقق من الحالات الاستثنائية وغير المعتادة في Drupal Core.
- التوجيه BOD 26-04 ملزم للجهات المدنية الفيدرالية الأمريكية فقط، لكن CISA تشجع جميع المؤسسات على اعتماد إدارة ثغرات قائمة على المخاطر وإعطاء أولوية لثغرات KEV.

أضافت CISA ثلاث ثغرات إلى كتالوج الثغرات المستغلة المعروفة (KEV) بعد توفر أدلة على استغلالها فعلياً. وتشير الوكالة إلى أن هذا النوع من الثغرات يشكّل وسيلة هجوم متكررة لدى الجهات الخبيثة.

الثغرات المضافة

- **CVE-2026-120705**: ثغرة حقن XML في OSGeo GeoServer
- **CVE-2026-129243**: ثغرة تفويض غير سليم في OSGeo GeoServer
- **CVE-2026-136716**: خلل في التحقق من الحالات الاستثنائية وغير المعتادة في Drupal Core

لا يتضمن المصدر الإصدارات المتأثرة ولا تفاصيل التصحيح أو الجوانب التقنية، لذا ينبغي الرجوع إلى نشرات الجهات المطوّرة للحصول عليها.

أهمية الأمر خارج الجهات الأمريكية

يُلزم التوجيه التشغيلي الملزم BOD 26-04 الجهات المدنية الفيدرالية الأمريكية بالمعالجة السريعة للثغرات المدرجة في KEV على الأصول المكشوفة للإنترنت والتي تمنح سيطرة كاملة بعد الاستغلال، مع إرجاء الثغرات الأقل خطورة. كما يحدد توقعات أساسية للتحقق مما إذا كان النظام قد اختُرق قبل تطبيق التصحيح.

لا ينطبق التوجيه على الجهات خارج تلك الفئة، غير أن CISA تشجع جميع المؤسسات على اعتماد إدارة ثغرات قائمة على المخاطر وإعطاء الأولوية لثغرات KEV. وبالنسبة للمؤسسات في المملكة، يمثل الكتالوج مدخلًا عملياً قائماً على الأدلة لترتيب أولويات التصحيح، خاصة للأنظمة المكشوفة للإنترنت.

النهج المقترح

تأكدوا من استخدام GeoServer أو Drupal في بيئتكم، بما في ذلك لدى الأطراف الثالثة، ومن إمكانية الوصول إليها عبر الإنترنت. وحيثما وُجدت، فاجعلوا المعالجة أولوية وراجعوا السجلات بحثاً عن مؤشرات اختراق سابق.

ما يجب فعله الآن

1. حصر جميع نسخ GeoServer وDrupal، بما فيها التي يديرها الموردون أو مزوّدو الاستضافة.
2. تحديد النسخ المكشوفة للإنترنت وإعطاؤها أولوية المعالجة.
3. تطبيق إصلاحات الجهات المطوّرة أو إجراءات التخفيف للثغرات الثلاث وفق نشراتها.
4. مراجعة السجلات والأنظمة على النسخ المكشوفة بحثاً عن مؤشرات اختراق قبل التصحيح.
5. إدراج متابعة كتالوج KEV ضمن عملية إدارة الثغرات كمدخل لتحديد الأولويات.