CISA تحذّر من ثغرة في مثبّت Drupal Core (CVE-2026-136716) تتيح السيطرة على الموقع عن بُعد



أدرجت CISA الثغرة CVE-2026-136716 في Drupal Core، وتتيح لمهاجم عن بُعد دون مصادقة السيطرة على الموقع عبر المثبّت المكشوف عندما يكون التثبيت في حالة غير مكتملة أو غير معتادة.

- الثغرة ناتجة عن فحص غير سليم للحالات الاستثنائية أو غير المعتادة في Drupal Core.
- يمكن لمهاجم عن بُعد دون مصادقة السيطرة على الموقع عبر مثبّت Drupal المكشوف.
- تنطبق الثغرة فقط عندما يكون الموقع في إحدى حالات التثبيت غير المعتادة أو غير المكتملة المتأثرة.
- تشترط CISA تطبيق إجراءات التخفيف وفق تعليمات المورّد وإرشادات BOD 26-04 ومتطلبات Forensics Triage.
- الموعد النهائي للجهات الفيدرالية الأمريكية هو 30-11-2026.

أدرجت CISA الثغرة CVE-2026-136716 في Drupal Core، وهي مصنّفة على أنها فحص غير سليم للحالات الاستثنائية أو غير المعتادة. ووفق الإدراج، يستطيع مهاجم عن بُعد دون مصادقة السيطرة على الموقع عبر مثبّت Drupal إذا كان مكشوفاً وكان الموقع في إحدى حالات التثبيت غير المعتادة أو غير المكتملة المتأثرة.

ما الذي تقوله النشرة

ترتبط المشكلة بالمثبّت لا بالتشغيل الاعتيادي للموقع. أما الحالات التي تجعل الموقع عرضة للخطر فهي حالات تثبيت محددة لا يصفها المصدر إلا بصورة عامة، لكن النتيجة هي سيطرة كاملة على الموقع دون أي بيانات اعتماد.

تطلب CISA تطبيق إجراءات التخفيف وفق تعليمات المورّد، مع الالتزام بإرشادات BOD 26-04 بشأن ترتيب أولويات التحديثات الأمنية بحسب المخاطر، ومتطلبات Forensics Triage. وفي الخدمات السحابية تُتَّبع إرشادات BOD 26-04 المعنية، وإذا تعذّرت إجراءات التخفيف فينبغي التوقف عن استخدام المنتج. والموعد النهائي للجهات الفيدرالية هو 30-11-2026، وتقع على كل جهة مسؤولية تقييم تعرّض أصولها للإنترنت.

الأثر على الجهات في المملكة

تسري BOD 26-04 على الجهات الفيدرالية الأمريكية لا على الجهات السعودية، لكنها مرجع عملي مفيد. وعلى المؤسسات التي تشغّل Drupal للبوابات العامة أو مواقع العملاء أو الشبكات الداخلية أن تتحقق من وجود نسخ متاحة عبر الإنترنت، ومن إمكانية الوصول إلى المثبّت أو وجود تثبيت لم يكتمل. ويُنصح بالبدء بإرشادات المورّد، وإجراء فحص جنائي للمواقع التي ربما تعرّضت للكشف.

ما يجب فعله الآن

1. حصر جميع نسخ Drupal Core وتحديد المتاح منها عبر الإنترنت.
2. فحص المواقع ذات حالات التثبيت غير المكتملة أو غير المعتادة والتأكد من عدم إمكانية الوصول إلى المثبّت من الخارج.
3. تطبيق إجراءات التخفيف الصادرة عن المورّد للثغرة CVE-2026-136716 في أقرب وقت.
4. مراجعة المواقع المتأثرة بحثاً عن مؤشرات اختراق وفق نهج فحص جنائي أولي مماثل لما تصفه CISA.
5. تقييد الوصول إلى أي موقع تتعذّر له إجراءات التخفيف أو إيقافه إلى حين توفر إصلاح.
6. توثيق الإجراءات ضمن عملية إدارة الثغرات لأغراض التقارير المتوافقة مع ضوابط NCA ECC.