استغلال ثغرة CVE-2026-132165 في نواة Drupal فعلياً مع توفر التحديثات



ثغرة CVE-2026-132165 في نواة Drupal تتيح تنفيذ الشيفرة عن بُعد عبر المثبّت، وتُستغل فعلياً. أضافتها CISA إلى كتالوج KEV، والتحديثات متاحة، أما الفروع المنتهية الدعم فلن تُصلَّح.

- تؤثر الثغرة CVE-2026-132165 في المثبّت المرفق مع نواة Drupal، وقد تتيح لمهاجم غير مصادق، في ظروف معينة، السيطرة على الموقع أو تنفيذ شيفرة عن بُعد.
- صدر التصحيح في 18 نوفمبر، وأفادت Drupal برصد استغلال على مواقع فعلية منذ 19 نوفمبر.
- الإصدارات المصححة هي Drupal 11.4.13 و11.3.22 و10.6.22، ولن تحصل الفروع المنتهية الدعم على إصلاح.
- أضافت CISA الثغرة إلى كتالوج KEV في 24 نوفمبر، ورفعت Drupal تصنيفها إلى «حرجة للغاية».
- يحدّ من بعض مسارات الاستغلال، لا كلها، منع خادم الويب من الكتابة على settings.php أو تغيير صلاحياته.

تُستغل فعلياً ثغرة حُدّثت حديثاً في نواة Drupal، ورقمها CVE-2026-132165، بحسب وكالة CISA ومطوري Drupal. وقد تؤدي الثغرة إلى تنفيذ شيفرة عن بُعد.

ما الذي حدث

تكمن المشكلة في المثبّت المرفق مع نواة Drupal، وهو المستخدم لإعداد موقع جديد. وفي ظروف معينة يمكن لمهاجم غير مصادق إساءة استخدامه لإعادة تثبيت Drupal، مما قد يمنحه السيطرة على الموقع أو تنفيذ شيفرة اعتباطية.

صدر الإصلاح في 18 نوفمبر. وذكر فريق الأمن في Drupal أنه تلقى بلاغاً عن استغلال على مواقع فعلية منذ الساعة 19:00 بالتوقيت العالمي في 19 نوفمبر، ثم رفع التصنيف إلى «حرجة للغاية». وأضافت CISA الثغرة إلى كتالوج الثغرات المستغلة المعروفة (KEV) في 24 نوفمبر. ويُنسب اكتشاف الثغرة إلى OSS Scanner من Anthropic، وهي خدمة مجانية اختيارية تفحص مشاريع المصادر المفتوحة المسجّلة فيها.

لا تتوفر معلومات علنية عن الهجمات، ولا يزال عدد المواقع المتأثرة غير واضح.

من عليه التحرك

على كل جهة تشغّل Drupal 10 أو 11 التعامل مع الأمر على وجه الاستعجال. التحديثات متاحة في Drupal 11.4.13 و11.3.22 و10.6.22. أما الفروع المنتهية الدعم فلن تُصلَّح، لذا تحتاج المواقع عليها إلى الترحيل أو ضوابط تعويضية.

وتشير Drupal إلى أن بعض مسارات الاستغلال، لا كلها، يُحدّ منها عندما لا يستطيع خادم الويب الكتابة على settings.php أو تغيير صلاحياته. وتوصي بالترقية وبتأمين المثبّت بعد التثبيت.

وهذه ثالث ثغرة في Drupal يُبلَّغ عن استغلالها هذا العام، بعد ثغرة تجاوز الصلاحيات في وحدة Commerce Core في أكتوبر وأخرى في مايو.

ما يجب فعله الآن

1. حصر جميع مواقع Drupal، بما فيها المواجهة للإنترنت والمستضافة لدى أطراف ثالثة، وتوثيق إصداراتها.
2. الترقية إلى Drupal 11.4.13 أو 11.3.22 أو 10.6.22 بحسب الفرع، مع إعطاء الأولوية للمواقع المنشورة للعموم.
3. وضع خطة ترحيل أو ضوابط تعويضية للمواقع على فروع Drupal المنتهية الدعم التي لن تُصلَّح.
4. تأمين المثبّت بعد التثبيت ومنع خادم الويب من الكتابة على settings.php أو تغيير صلاحياته.
5. مراجعة سجلات خادم الويب والتطبيق منذ 18 نوفمبر بحثاً عن نشاط إعادة تثبيت أو تغييرات غير متوقعة، والتصعيد عبر الاستجابة للحوادث عند الاشتباه.