استغلال الثغرة الحرجة CVE-2026-132165 في Drupal للسيطرة على المواقع



أكد فريق Drupal استغلال الثغرة الحرجة CVE-2026-132165 في مثبّت النظام، وهي تتيح السيطرة على الموقع أو تنفيذ تعليمات عن بُعد. وأضافتها CISA إلى كتالوج KEV. يُنصح بالترقية أو حجب ملف التثبيت.

- تتيح الثغرة CVE-2026-132165 لمستخدم مجهول إساءة استخدام مثبّت Drupal للسيطرة على الموقع أو تنفيذ تعليمات عن بُعد.
- أفادت Drupal بأن الاستغلال على مواقع فعلية بدأ منذ 19-11-2026 الساعة 19:00 بالتوقيت العالمي المنسق.
- المعالجة بالترقية إلى أحدث إصدار من Drupal، وعملاء خدمة Drupal Steward WAF محميون من أساليب الهجوم المعروفة.
- إن تعذرت الترقية فيُحجب الوصول إلى /core/install.php في إعدادات الخادم أو ملف .htaccess.

- أضافت CISA الثغرة إلى كتالوج KEV وحددت 27 نوفمبر موعدًا لمعالجتها في الجهات الاتحادية الأمريكية.

أكد فريق أمن Drupal أن ثغرة حرجة في نواة النظام تُستغل حاليًا ضد المواقع التي لم تُحدَّث. الثغرة مسجلة برقم CVE-2026-132165، واكتشفتها أداة OSS Scanner التابعة لشركة Anthropic.

ما الذي يتأثر

تتضمن نواة Drupal ملف install.php المخصص لتثبيت النظام. وفي ظروف معينة يستطيع المهاجم استخدامه لمحاولة إعادة التثبيت، مما قد يؤدي إلى السيطرة على الموقع أو تنفيذ تعليمات عن بُعد، ولا يتطلب ذلك مصادقة. وتشير Drupal إلى أن بعض مسارات الاستغلال تتعطل إذا لم يكن لخادم الويب صلاحية الكتابة على settings.php أو تغيير صلاحياته.

لم تُصنَّف الثغرة في البداية على أنها مستغَلة، ثم حدّثت Drupal تنبيهها لتفيد بوقوع هجمات على مواقع فعلية منذ 19-11-2026 الساعة 19:00 بالتوقيت العالمي المنسق. وأضافت CISA الثغرة يوم الثلاثاء إلى كتالوج الثغرات المستغلة KEV، وألزمت الجهات الاتحادية الأمريكية بالمعالجة قبل الجمعة 27 نوفمبر، وشجعت جميع المنظمات على إعطاء أولوية للثغرات المدرجة فيه ضمن إدارة ثغرات قائمة على المخاطر.

خيارات الحماية

المعالجة الأساسية هي الترقية إلى أحدث إصدار متاح من Drupal. والمواقع المحمية بخدمة Drupal Steward WAF المدفوعة محمية من أساليب الهجوم المعروفة، لكن Drupal توصي بالترقية تحسبًا لظهور أساليب أخرى. وإذا تعذرت الترقية الفورية فيجب حجب الوصول إلى /core/install.php في إعدادات خادم الويب أو في ملف .htaccess بالمجلد الجذر.

أهمية الأمر

يُستخدم Drupal على نطاق واسع في الجهات الحكومية والجامعات والشركات والمؤسسات الإعلامية. وقد صنفت CISA خمس ثغرات في Drupal على أنها مستغَلة منذ نوفمبر 2021، منها اثنتان استغلتهما أيضًا جماعات فدية. لذا ينبغي لكل جهة تشغّل موقع Drupal عامًا التعامل مع الأمر كتعرض فعلي يستدعي سرعة التحرك.

ما يجب فعله الآن

1. حصر جميع مواقع Drupal، العامة والداخلية والمستضافة لدى أطراف ثالثة، والتحقق من إصداراتها.
2. ترقية المواقع المتأثرة إلى أحدث إصدار من Drupal بشكل عاجل.
3. عند تأخر الترقية، حجب /core/install.php في إعدادات خادم الويب أو ملف .htaccess.
4. التأكد من أن خادم الويب لا يملك صلاحية الكتابة على settings.php أو تغيير صلاحياته.
5. مراجعة سجلات الويب منذ 19-11-2026 بحثًا عن طلبات إلى المثبّت أو تغييرات غير متوقعة في ملفات الموقع وإعداداته.
6. توثيق التعرض والمعالجة ضمن عملية إدارة الثغرات وفق متطلبات الضوابط الأساسية للأمن السيبراني

(NCA ECC) وإطار SAMA CSF.