ثغرة CVE-2026-132165 في Drupal Core: خلل في المثبّت قد يتيح الاستيلاء على الموقع أو تنفيذ تعليمات برمجية



أدرجت CISA الثغرة CVE-2026-132165 في Drupal Core، وتتيح لمهاجم غير مصادق عليه إساءة استخدام install.php في ظروف معينة للاستيلاء على الموقع أو تنفيذ تعليمات برمجية. يُنصح بتطبيق إجراءات المعالجة الصادرة عن المورّد.

- تؤثر CVE-2026-132165 في Drupal Core، وتوصف بأنها خلل في الفشل الآمن.
- قد يستولي مهاجم غير مصادق عليه على موقع قائم أو ينفّذ تعليمات برمجية عبر مثبّت Drupal.
- في ظروف معينة يمكن للمهاجم استخدام install.php لمحاولة إعادة تثبيت Drupal على الموقع.
- تشترط CISA تطبيق إجراءات المعالجة وفق تعليمات المورّد وتوجيه BOD 26-04 ومتطلبات الفرز الجنائي، وموعد الجهات الفيدرالية الأمريكية 27-11-2026.

- إذا لم تتوفر إجراءات معالجة فتوصي CISA بالتوقف عن استخدام المنتج.

أضافت CISA الثغرة CVE-2026-132165 إلى قائمتها للثغرات. وتتعلق بـ Drupal Core، وتوصف بأنها خلل في الفشل الآمن داخل مثبّت Drupal.

ما الذي تتيحه الثغرة

وفق ما ورد في الإدراج، قد يتمكن مهاجم غير مصادق عليه من الاستيلاء على موقع قائم أو تنفيذ تعليمات برمجية. وفي ظروف معينة يستطيع المهاجم استخدام install.php لمحاولة إعادة تثبيت Drupal على موقع يعمل بالفعل. ولا يحدد المصدر الإصدارات المتأثرة ولا طبيعة الظروف المطلوبة، لذا ينبغي الرجوع إلى تعليمات المورّد لمعرفة التفاصيل.

ما تشترطه CISA

تتمثل الإجراءات المطلوبة في تطبيق إجراءات المعالجة وفق تعليمات المورّد، مع اتباع توجيه BOD 26-04 بشأن ترتيب أولوية التحديثات الأمنية بحسب المخاطر، ومتطلبات الفرز الجنائي (Forensics Triage Requirements). وبالنسبة للخدمات السحابية يُتَّبع التوجيه المعمول به ضمن BOD 26-04. وإذا لم تتوفر إجراءات معالجة فتوصي CISA بالتوقف عن استخدام المنتج. كما تقع على الجهات مسؤولية تقييم تعرّض كل أصل للإنترنت. وموعد الجهات الفيدرالية الأمريكية هو 27-11-2026؛ وهو ملزم لتلك الجهات، لكنه مرجع مفيد للتخطيط.

قراءة عملية للمؤسسات في المملكة

على المؤسسات التي تشغّل Drupal في مواقع عامة أو بوابات أو خدمات موجهة للعملاء أن تعدّ ذلك دافعًا للتأكد من تعرضها وتطبيق إجراءات المعالجة الصادرة عن المورّد دون انتظار الموعد المرجعي.

ما يجب فعله الآن

1. حصر جميع نسخ Drupal Core، بما فيها بيئات الاختبار والمواقع المنسية، وتحديد المكشوف منها على الإنترنت.
2. تطبيق إجراءات المعالجة الصادرة عن المورّد للثغرة CVE-2026-132165 وفق تعليماته.
3. التحقق من إمكانية الوصول إلى install.php من الإنترنت في كل نسخة، وتقييد الوصول بما يتوافق مع إرشادات المورّد.
4. مراجعة سجلات خادم الويب والتطبيق بحثًا عن طلبات غير متوقعة إلى المثبّت أو مؤشرات على إعادة تثبيت أو تغييرات غير مصرح بها.
5. إذا لم تتوفر إجراءات معالجة لأصل معين، فالتخطيط لإخراجه من الخدمة كما توصي CISA.
6. توثيق تقييم التعرض وإجراءات المعالجة ضمن عملية إدارة الثغرات.