ثغرة متبقية بعد تحديث مثبّت Drupal يستغلها المهاجمون حاليًا



أعلنت Drupal أن إصلاح المثبّت السابق لم يحمِ جميع المواقع، وأن الثغرة CVE-2026-136716 تُستغل للسيطرة على مواقع في حالات تثبيت غير مكتملة. التحديثات متاحة ويلزم تشغيل update hook بعد الترقية.

- CVE-2026-136716 ثغرة تجاوز صلاحيات قد تؤدي إلى الاستيلاء على الموقع، أُعلن عنها في 25 نوفمبر بتقييم CMSS قدره 21/25.
- تأتي بعد النشرة SA-CORE-2026-017 الصادرة في 18 نوفمبر لمعالجة ثغرة المثبّت CVE-2026-132165، وقد أضافتها CISA إلى كتالوج KEV في 24 نوفمبر.
- قد تبقى المواقع ذات حالات التثبيت غير المعتادة أو غير المكتملة، ومنها مواقع الإنتاج، عرضة للخطر، ولا تُظهر واجهة المستخدم هذه الحالة.
- الإصدارات المصححة هي 11.4.14 و11.3.23 و10.6.23، ويجب على مواقع الإنتاج تشغيل update

hook بعد الترقية.

- لم تنشر Drupal تفاصيل عن الهجمات أو الجهة المسؤولة، وتنصح بمراجعة السجلات بحثًا عن مؤشرات اختراق.

كشفت Drupal أن التحديث الذي أصدرته في 18 نوفمبر لمعالجة ثغرة في المثبّت لم يحمِ جميع المواقع. وتُستغل الآن ثغرة لاحقة، هي CVE-2026-136716، فعليًا لاختراق المواقع التي ما زالت عرضة للخطر.

ما الذي حدث

عالجت النشرة الأصلية SA-CORE-2026-017 الثغرة CVE-2026-132165 في المثبّت المرفق مع نواة Drupal، وهو الأداة المستخدمة لإعداد المواقع الجديدة. وعلمت Drupal بالاستغلال الفعلي بعد وقت قصير، وأضافت CISA تلك الثغرة إلى كتالوج KEV في 24 نوفمبر.

وفي 25 نوفمبر أعلنت Drupal عن CVE-2026-136716، وهي ثغرة تجاوز صلاحيات قد تؤدي إلى الاستيلاء على الموقع، بتقييم CMSS قدره 21/25. وبحسب Drupal، بقيت المواقع ذات حالات التثبيت غير المعتادة أو غير المكتملة، ومنها مواقع الإنتاج، معرضة للخطر بعد النشرة الأولى. ولا تُظهر واجهة المستخدم ما إذا كان الموقع في هذه الحالة، وقد لا يبدو الموقع المخترق فعلاً عرضة للثغرة.

من المتأثر

المواقع التي سبق تأمين المثبّت فيها غير معرضة للهجمات. أما أي موقع ترك المثبّت متاحًا عن بُعد بعد SA-CORE-2026-017 فقد يكون تعرض للاختراق. ولم تنشر Drupal تفاصيل عن الهجمات، والجهة المنفذة غير معروفة.

ما المطلوب

الإصلاحات متوفرة في الإصدارات 11.4.14 و11.3.23 و10.6.23. ويجب على مواقع الإنتاج تشغيل update hook بعد الترقية لمعالجة الثغرة بالكامل. وبما أن الاستغلال جارٍ، فقد لا يكفي التحديث وحده، ولذلك ينبغي مراجعة السجلات بحثًا عن مؤشرات اختراق.

ما يجب فعله الآن

1. حصر جميع مواقع Drupal، بما فيها الإنتاج والاختبار وأي نسخ غير مكتملة التثبيت، وتوثيق إصداراتها.
2. الترقية إلى 11.4.14 أو 11.3.23 أو 10.6.23 بحسب الحالة، ثم تشغيل update hook على مواقع الإنتاج.
3. التأكد من عدم إمكانية الوصول إلى المثبّت عن بُعد في أي موقع، وتقييد الوصول إليه.
4. مراجعة سجلات خادم الويب والتطبيق منذ 18 نوفمبر بحثًا عن مؤشرات اختراق، وبدء معالجة الحادثة عند اكتشاف أي منها.
5. اعتبار المواقع التي كان المثبّت فيها متاحًا مخترقة محتملاً حتى بعد التحديث، والتحقق من سلامتها.
6. توثيق التعرض والاستجابة ضمن إجراءات إدارة الثغرات والحوادث.