# Drupal تحذّر من ثغرة ثانية للاستيلاء على المواقع قيد الاستغلال الفعلي




أعلنت Drupal أن ثغرة حرجة ثانية، CVE-2026-136716، تُستغل للاستيلاء على مواقع غير محدّثة، وتشمل حالات تثبيت بقيت مكشوفة بعد إصلاح Fail2Install. يُنصح بالترقية أو حجب المثبّت.

- صدر إصلاح CVE-2026-136716 بعد أسبوع من Fail2Install (CVE-2026-132165)، وتؤكد Drupal أنه يُستغل فعلياً.
- بقيت مواقع في حالات تثبيت غير مكتملة أو غير معتادة، ومنها مواقع إنتاج، عرضة للاستيلاء بعد SA-CORE-2026-017.
- لا تظهر الحالة الضعيفة في واجهة المستخدم، وقد لا تظهر في المواقع التي سبق اختراقها.
- الإصدارات المصحّحة هي Drupal 10.6.23 و11.3.23 و11.4.14.
- إن تعذّرت الترقية الفورية يجب حجب الوصول إلى /core/install.php.

حذّر فريق الأمن في Drupal من أن مهاجمين يستغلون ثغرة حرجة ثانية تتيح لهم الاستيلاء على مواقع لم تُحدَّث.

## ما الذي حدث

أصلحت Drupal الأسبوع الماضي ثغرة تنفيذ شيفرة عن بُعد برقم CVE-2026-132165 وتُعرف باسم Fail2Install، وكانت تتيح لمستخدمين مجهولين السيطرة على المواقع عبر إساءة استخدام المثبّت. وذكر تحديث لاحق للنشرة أن الاستغلال بدأ بعد يوم واحد من صدور الإصلاحات.

أما الثغرة الجديدة CVE-2026-136716 فقد صدر إصلاحها بعد أسبوع، وهي تعالج مسارات هجوم تُركت دون إصلاح. وتوضح Drupal أن مواقع في حالات تثبيت غير معتادة أو غير مكتملة، ومنها مواقع إنتاج، بقيت معرضة بعد SA-CORE-2026-017. ولا تظهر هذه الحالة في واجهة المستخدم، وقد لا يكون الموقع المخترق أصلًا في الحالة الضعيفة. ولم تنشر Drupal حتى الآن تفاصيل إضافية عن الهجمات.

## الخطوات التي توصي بها Drupal

أي موقع ترك المثبّت متاحاً عن بُعد قد يكون تعرّض للاختراق. على المسؤولين التأكد من أن البريد الإلكتروني للمستخدم رقم 1 يخضع لسيطرتهم والنظر في إعادة تعيينه، ومراجعة السجلات بحثاً عن وصول غير مصرّح به، وخصوصاً التغييرات غير المتوقعة على حساب المستخدم 1 أو منه، واتباع إرشادات Drupal عند الاشتباه بالاختراق.

الإصدارات المصحّحة هي Drupal 10.6.23 و11.3.23 و11.4.14. وعلى الفرق التي لا تستطيع الترقية فوراً حجب الوصول إلى /core/install.php في جميع المواقع الجديدة والقائمة، عبر إعدادات خادم الويب أو ملف .htaccess في الجذر.

## لماذا يهم ذلك

لأن التحديث وحده قد لا يكشف اختراقاً سابقاً، ينبغي للجهات التي تشغّل Drupal أن تقرن الترقية بمراجعة بحثاً عن مؤشرات اختراق.

## ما يجب فعله الآن

1. حصر جميع مواقع Drupal بما فيها التطوير والاختبار، وتحديد ما يعمل بإصدار أقدم من 10.6.23 أو 11.3.23 أو 11.4.14.
2. الترقية إلى إصدار مصحّح، أو حجب /core/install.php في إعدادات خادم الويب أو ملف .htaccess إلى حين الترقية.
3. التحقق من أن البريد الإلكتروني للمستخدم رقم 1 تحت سيطرة فريقكم والنظر في إعادة تعيينه.
4. مراجعة السجلات بحثاً عن تغييرات غير متوقعة على حساب المستخدم 1 أو منه، وأي وصول غير مصرّح به.
5. عند الاشتباه بالاختراق، اتباع إرشادات Drupal وتفعيل خطة الاستجابة للحوادث بما فيها الإبلاغ للجهة التنظيمية.