Drupal تحذّر من ثغرة حرجة للغاية في النواة قيد الاستغلال الفعلي



كشفت Drupal عن ثغرة حرجة للغاية في نواتها برقم CVE-2026-136716، وأفادت باستغلالها فعليًا. وترتبط بثغرة Fail2Install السابقة وتعالج حالات تثبيت ظلّت عرضة للاستغلال.

- تصنّف Drupal الثغرة الجديدة في النواة على أنها حرجة للغاية وتفيد باستغلالها فعليًا.
- تحمل الثغرة الرقم CVE-2026-136716 ولا يذكر المصدر درجة CVSS لها.
- يوصف الخلل بأنه فحص غير سليم للحالات الاستثنائية أو غير المعتادة.
- ترتبط بالثغرة Fail2Install (CVE-2026-132165) وتعالج حالات تثبيت بقيت قابلة للاستغلال.

أصدرت Drupal تحذيرًا بشأن ثغرة أمنية جديدة في نواة Drupal صنّفتها على أنها «حرجة للغاية». ووفق ما ورد، فإن الثغرة تُستغل بالفعل في الواقع، ويصفها عنوان الخبر بأنها تتيح الاستيلاء على الموقع.

ما المعروف حتى الآن

تحمل الثغرة الرقم **CVE-2026-136716**، ولا يتوفر في المصدر تقييم CVSS لها. ويُوصف الخلل بأنه فحص غير سليم للحالات الاستثنائية أو غير المعتادة.

وترتبط هذه الثغرة بالثغرة **CVE-2026-132165** المعروفة باسم Fail2Install، إذ تعالج حالات تثبيت ظلّت عرضة للاستغلال بعد تلك الثغرة السابقة. ولا يقدّم المصدر تفاصيل تقنية إضافية ولا نطاق الإصدارات المتأثرة ولا معلومات التحديث، لذا ينبغي التحقق منها مباشرة من إشعار Drupal الرسمي.

الخطوات التالية

نظرًا إلى الإبلاغ عن استغلال فعلي، على الجهات التي تستخدم Drupal التعامل مع الأمر بأولوية عالية وعدم انتظار نافذة الصيانة الدورية. تبدأ الخطوة الأولى بحصر مواضع استخدام Drupal، بما في ذلك البوابات العامة والخدمات المقدمة للعملاء وأي نسخ تجريبية أو منسية. ثم الاطلاع على الإشعار الأمني الرسمي وتطبيق الإصدار المصحَّح الذي يحدده.

وينبغي كذلك مراجعة ما إذا كانت أي إجراءات تثبيت أو إعداد متاحة من الإنترنت، نظرًا لارتباط الثغرة بحالات التثبيت، وفحص السجلات بحثًا عن نشاط غير معتاد. وأي مؤشرات على اختراق تُعالج وفق إجراءات الاستجابة للحوادث المعتمدة لدى الجهة.

ما يجب فعله الآن

1. حصر جميع نسخ Drupal بما فيها المواقع العامة والتجريبية والقديمة.
2. الاطلاع على إشعار Drupal الرسمي للثغرة CVE-2026-136716 وتطبيق الإصدار المصحَّح المحدد كتغيير طارئ.
3. التأكد من عدم إتاحة إجراءات التثبيت أو الإعداد من الإنترنت.
4. مراجعة سجلات خادم الويب والتطبيق بحثًا عن طلبات غير معتادة أو تغييرات غير متوقعة منذ الإبلاغ عن الاستغلال.
5. تصعيد أي مؤشر على اختراق عبر مسار الاستجابة للحوادث وإبلاغ الجهة التنظيمية المعنية عند الاقتضاء.