إضافة ثغرة Fail2Install في نواة Drupal (CVE-2026-132165) إلى كتالوج CISA للثغرات المستغلة



أضافت CISA ثغرة تنفيذ الأوامر عن بُعد الحرجة CVE-2026-132165 المعروفة بـ Fail2Install (CVSS 9.8) في نواة Drupal إلى كتالوج KEV، وعلى الجهات الفيدرالية الأمريكية تطبيق الإصلاحات قبل 27 نوفمبر 2026.

- أضافت CISA ثغرة Drupal إلى كتالوج الثغرات المستغلة المعروفة (KEV).
- الثغرة مسجلة بالرقم CVE-2026-132165 ويُطلق عليها Fail2Install.
- تبلغ درجتها 9.8 وفق CVSS وتتيح تنفيذ أوامر عن بُعد في نواة Drupal.
- أمام الجهات الفيدرالية الأمريكية مهلة حتى 27 نوفمبر 2026 لتطبيق الإصلاحات.
- إدراجها في KEV يشير إلى استغلالها الفعلي.

أضافت الوكالة الأمريكية للأمن السيبراني وأمن البنية التحتية (CISA) ثغرة حرجة في Drupal إلى كتالوج الثغرات المستغلة المعروفة (KEV). والثغرة مسجلة بالرقم **CVE-2026-132165** ويُشار إليها أيضًا باسم **Fail2Install**.

ما هو معروف

تتعلق الثغرة بتنفيذ الأوامر عن بُعد (RCE) في نواة Drupal، وتبلغ درجتها 9.8 وفق CVSS. وقد طُلب من الجهات الفيدرالية الأمريكية تطبيق الإصلاحات قبل 27 نوفمبر 2026. ويعكس إدراجها في KEV أنها تتعرض لاستغلال فعلي، كما بدأت تفاصيل الاستغلال بالظهور.

لا يذكر المقتطف المتاح الإصدارات المتأثرة ولا إصدارات الإصلاح ولا شروط الاستغلال الدقيقة، لذا ينبغي التحقق منها من نشرة Drupal الأمنية الرسمية.

أهمية الخبر للمؤسسات في المملكة

يُستخدم Drupal على نطاق واسع كنظام لإدارة المحتوى، ويجب التعامل مع أي ثغرة RCE في نواته قيد الاستغلال بوصفها أولوية عاجلة، خاصة في المواقع المكشوفة على الإنترنت، بما فيها ما تديره وكالات ويب أو مزودو استضافة نيابة عن المؤسسة.

والأفضل اتباع استجابة هادئة ومنظمة: حصر مواضع استخدام Drupal، والتأكد من الإصدار، وتطبيق إصلاح المورد، ثم فحص مؤشرات الاختراق على الأنظمة التي كانت مكشوفة قبل التحديث.

ما يجب فعله الآن

1. حصر جميع نسخ Drupal، بما فيها التي تديرها أطراف ثالثة، وتسجيل إصداراتها.
2. مراجعة نشرة Drupal الأمنية الرسمية وتطبيق إصلاح CVE-2026-132165 بدءًا بالمواقع المكشوفة على الإنترنت.
3. فحص سجلات خادم الويب والتطبيق للنسخ المكشوفة بحثًا عن نشاط غير معتاد قبل التحديث.
4. مطالبة وكالات الويب ومزودي الاستضافة بتأكيد حالة التحديث كتابيًا.
5. إدراج CVE-2026-132165 في سجل متابعة الثغرات ورفع حالة المعالجة إلى مسؤول أمن المعلومات.