

ثغرة حرجية لتضمين الملفات عن بُعد في نواة ووردبريس



ثغرة حرجية لتضمين الملفات عن بُعد في نواة ووردبريس تتيح للمهاجمين غير المصادق عليهم تنفيذ أكواد عشوائية من خلال إجبار نظام القوالب على تضمين ملفات PHP محلية خارج مجلدات القوالب.

- نواة ووردبريس تحتوي على ثغرة تضمين ملفات عن بُعد مسجلة برقم CVE-2026-87902
- المهاجمون غير المصادق عليهم يمكنهم استغلال آلية تحليل القوالب لتضمين ملفات PHP محلية عشوائية
- الاستغلال الناجح يؤدي إلى تنفيذ أكواد عن بُعد على منصات ووردبريس المعرضة للخطر
- يجب على المؤسسات تطبيق تدابير الحماية الصادرة عن المورد فوراً أو إيقاف استخدام المنتج
- الأصول الرقمية لووردبريس المتصلة بالإنترنت تتطلب تقييماً وتصحيحاً فورياً

نظرة عامة على الثغرة

أعلنت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية عن **CVE-2026-87902**، وهي ثغرة حرجية لتضمين الملفات عن بُعد تؤثر على نواة ووردبريس. تتيح هذه الثغرة للمهاجمين غير المصادق عليهم التلاعب بآلية تحليل قوالب الصفحات في المنصة، مما يجبرها على تضمين ملفات PHP محلية قابلة للقراءة موجودة خارج مجلدات القوالب النشطة. يؤدي الاستغلال الناجح إلى **تنفيذ أكواد عن بُعد**، مما يمنح المهاجمين سيطرة كاملة على منصات ووردبريس المعرضة للخطر.

لا تتطلب الثغرة أي مصادقة، مما يخفض بشكل كبير حاجز الاستغلال ويوسع سطح الهجوم المحتمل للمؤسسات الخاضعة للرقابة التي تشغل بوابات عامة أو منصات تفاعل مع العملاء أو أنظمة إدارة محتوى داخلية قائمة على ووردبريس.

المخاطر على المؤسسات السعودية

تشغل منصة ووردبريس جزءاً كبيراً من البنية التحتية للويب عالمياً، بما في ذلك العديد من المواقع الإلكترونية للشركات والبوابات الإلكترونية للعملاء ومنصات الخدمات الرقمية التي تديرها المؤسسات المالية ومقدمو الرعاية الصحية والجهات الحكومية في المملكة. نظراً لطبيعة الثغرة التي لا تتطلب مصادقة، تشكل منصات ووردبريس المتصلة بالإنترنت خطراً فورياً. يمكن للمهاجمين الذين يحصلون على قدرات تنفيذ الأكواد استخراج البيانات الحساسة أو نشر برامج الفدية أو إنشاء وصول دائم أو التحرك نحو الشبكات الداخلية.

يجب على المؤسسات الخاضعة لإشراف الهيئة الوطنية للأمن السيبراني ومؤسسة النقد العربي السعودي التعامل مع هذه الثغرة بصفة عاجلة، خاصة حيث تعالج منصات ووردبريس أو تخزن بيانات خاضعة للتنظيم بموجب نظام حماية البيانات الشخصية أو تتعامل مع خدمات موجهة للعملاء.

إرشادات التخفيف

يجب على المؤسسات تطبيق التحديثات الأمنية الصادرة عن المورد فوراً لجميع منصات نواة ووردبريس. في حال عدم توفر التصحيحات بعد، ينبغي على المؤسسات تنفيذ ضوابط تعويضية تشمل تقييد الوصول الشبكي أو نشر قواعد جدار حماية تطبيقات الويب أو إيقاف الأنظمة المعرضة للخطر مؤقتاً. تتطلب خدمات ووردبريس المستضافة سحابةً التنسيق مع مزودي الخدمة لتأكيد حالة التصحيح والجداول الزمنية.

ما يجب فعله الآن

1. إجراء جرد فوري لجميع منصات نواة ووردبريس عبر البيئات المتصلة بالإنترنت والداخلية
2. تطبيق التصحيحات الأمنية الصادرة عن المورد لـ CVE-2026-87902 على جميع منصات ووردبريس دون تأخير
3. للأنظمة التي لا تتوفر لها تصحيحات، تنفيذ ضوابط تعويضية تشمل تجزئة الشبكة أو قواعد WAF أو تعليق الخدمة مؤقتاً
4. التحقق من حالة التصحيح مع مزودي الخدمات السحابية لمنصات ووردبريس المستضافة خارجياً
5. مراجعة سجلات الوصول وإجراء فرز جنائي على جميع أنظمة ووردبريس لتحديد مؤشرات الاستغلال المحتملة

6. توثيق أنشطة المعالجة والجداول الزمنية لإعداد تقارير الامتثال للهيئة الوطنية للأمن السيبراني أو ساما حسب الاقتضاء