CISA تضيف ثغرة تعارض التوقيت في نواة WordPress إلى كتالوج الثغرات المستغلة



أضافت CISA الثغرة CVE-2026-119977 في نواة WordPress إلى كتالوج KEV بسبب رصد استغلال فعلي لها. وهي ثغرة عالية الخطورة قد تتيح تنفيذ تعليمات برمجية دون قيود.

- أضافت CISA ثغرة في نواة WordPress إلى كتالوج الثغرات المستغلة المعروفة (KEV).
- تحمل الثغرة الرمز CVE-2026-119977 وتقييم CVSS بدرجة 8.1، أي خطورة عالية.
- هي من نوع تعارض التوقيت بين الفحص والاستخدام (TOCTOU).
- يمكن استغلالها لتنفيذ تعليمات برمجية دون قيود.
- استندت CISA في الإضافة إلى أدلة على استغلال فعلي.

أضافت الوكالة الأمريكية للأمن السيبراني وأمن البنية التحتية (CISA) ثغرة في نواة WordPress إلى كتالوج الثغرات

المستغلة المعروفة (KEV)، مشيرة إلى وجود أدلة على استغلالها فعلياً.

ما المعروف حتى الآن

تحمل الثغرة الرمز **CVE-2026-119977** وتقييم CVSS بدرجة 8.1، أي ضمن فئة الخطورة العالية. وهي من نوع تعارض التوقيت بين الفحص والاستخدام (TOCTOU)، وبحسب التقرير يمكن استغلالها لتنفيذ تعليمات برمجية دون قيود.

التقرير المصدر موجز، ولا يوضح في الجزء المتاح لنا النسخ المتأثرة ولا الإصدارات المصححة ولا شروط الاستغلال بدقة ولا الجهة التي تقف خلف الهجمات. لذلك ينبغي اعتماد إشعار الأمان الرسمي من WordPress مرجعاً لهذه التفاصيل.

أهمية الخبر

إدراج الثغرة في كتالوج KEV يعني أن الاستغلال واقع فعلًا وليس نظرياً. وبالنسبة للجهات التي تشغّل WordPress للمواقع العامة أو بوابات العملاء أو صفحات المستثمرين والإعلام، فإن ثغرة تنفيذ تعليمات برمجية في النواة قد تعرّض بيئة الاستضافة والبيانات التي يمكن الوصول إليها منها.

النهج المقترح

يُنصح بداية بحصر مواضع استخدام WordPress، بما في ذلك المواقع التي تديرها فرق التسويق أو وكالات خارجية. ثم الرجوع إلى إرشادات الأمان الرسمية لمعرفة الإصدار المصحح وجدولة التحديث عبر إدارة التغيير المعتمدة، مع إعطاء الأولوية للمواقع المكشوفة على الإنترنت. ومن الاحتياطات المناسبة أثناء التحديث مراقبة تغيّرات الملفات غير المعتادة أو النشاط الإداري غير المتوقع.

ما يجب فعله الآن

1. حصر جميع نسخ WordPress، بما فيها التي تديرها وكالات خارجية أو وحدات أعمال.
2. مراجعة إشعار الأمان الرسمي من WordPress بخصوص CVE-2026-119977 وتحديد الإصدار المصحح.
3. تحديث المواقع المكشوفة على الإنترنت أولًا عبر إجراءات إدارة التغيير.
4. فحص سجلات خادم الويب وWordPress بحثاً عن تغيّرات ملفات أو نشاط إداري غير متوقع.
5. تسجيل CVE-2026-119977 في سجل إدارة الثغرات مع موعد نهائي للمعالجة.