HIGH · مرتفع — تأثير مهم، يستوجب الترقيع العاجل.

SECURITY ADVISORY · نشرة تحذيرية

ثغرة XSS قبل المصادقة في WordPress قد تؤدي إلى تنفيذ شيفرة PHP

المعرّف	CVSS	المنتج المتأثر	تاريخ الاكتشاف
CVE-2026-64638	CVSS: 8.9 — High	WordPress Core	2026-08-06

١. الملخص التنفيذي

يرصد المركز الوطني للأمن السيبراني ثغرة جديدة تم الإفصاح عنها بمسؤولية في صفحة تسجيل الدخول لنظام WordPress Core (CVE-2026-64638)، تسمح بتنفيذ XSS دون مصادقة وتؤثر على جميع الإصدارات بدءاً من الفرع 4.7. حتى تاريخ إصدار هذه النشرة، لم تسجَّل المصادر المتابَعة أي استغلال فعلي أو إثبات مفهوم (PoC) علني لهذه الثغرة؛ إذ أبلغ الباحثون WordPress بها بشكل مسؤول قبل نشر الإصلاح. وفي حال توافر شروط إضافية تشمل جلسة إدارية نشطة وتفعيل ميزة Application Passwords وتفاعل المستخدم الإداري مع رابط ضار، يمكن تصعيد الثغرة إلى تنفيذ شيفرة PHP على الخادم. ونظراً لانتشار WordPress في المواقع الحكومية والخدمية العراقية، يوصي المركز بالتحديث الفوري إلى الإصدار 7.0.3 أو أحدث إصدار أمني متاح للفرع المستخدم، والتحقق من نجاح التحديثات التلقائية، إضافةً إلى مراجعة سجلات المصادقة بحثاً عن مؤشرات استغلال أو تغييرات غير مبررة.

٢. الأنظمة المتأثرة

- WordPress Core: الأنظمة التي لم تُطبق عليها الإصلاحات الأمنية المنشورة لمعالجة CVE-2026-64638.
- WordPress 7.0.3 يتضمن الإصلاح الأمني للثغرة.
- أعلنت WordPress عن توفير تحديثات أمنية للفروع المؤهلة للدعم و يجب تطبيق أحدث إصدار أمني متاح للفرع المستخدم.

٣. التأثير

قد يسمح استغلال الثغرة بتنفيذ JavaScript ضمن سياق متصفح الضحية عند تحقق شروط الاستغلال. وفي حال استهداف مستخدم ذي صلاحيات إدارية وتوافر الشروط الإضافية اللازمة لسلسلة الهجوم، قد يتصاعد الأثر إلى تنفيذ شيفرة PHP على الخادم، بما قد يعرّض سرية وسلامة الموقع والبيانات والحسابات الإدارية للخطر.

٤. التوصيات

1. تحديث WordPress إلى الإصدار 7.0.3 أو إلى أحدث إصدار أمني متاح للفرع المستخدم، والتحقق من نجاح تطبيق التحديث.
2. حصر مواقع WordPress المكشوفة للإنترنت وإعطاء الأولوية للمواقع الحكومية والخدمية والحسابات ذات الصلاحيات الإدارية.
3. تجنب اعتماد إجراءات WAF أو تقييد الوصول كبديل دائم عن تطبيق الإصلاح الأمني الرسمي.
4. مراجعة سجلات المصادقة والنشاط الإداري لرصد أي سلوك غير اعتيادي، خصوصاً إنشاء بيانات اعتماد أو تغييرات إدارية غير متوقعة.
5. توعية مسؤولي WordPress بعدم فتح روابط غير موثوقة أثناء وجود جلسة إدارية فعالة إلى حين استكمال التحديث.

٥. مؤشرات الاختراق (IOCs)

- حتى تاريخ إصدار هذه النشرة، لم تشر المصادر التي تمت مراجعتها إلى رصد استغلال فعلي للثغرة في هجمات واقعية، فيما أصبحت تفاصيل فنية حول آلية الاستغلال متاحة علناً.

٦. المراجع

- https://wordpress.org/news/2026/08/wordpress-7-0-3-release/
- https://thehackernews.com/2026/08/new-wordpress-pre-auth-xss-could-lead.html
- https://nvd.nist.gov/vuln/detail/CVE-2026-64638