تثبيت إصلاح ثغرة WordPress المستغلة قد يعرّض بعض المواقع للخطر لحظة التحديث



يفيد باحث في Picus Security بأن بعض مواقع WordPress تبقى عرضة للهجوم أثناء تثبيت إصلاح ثغرة مستغلة فعليًا، لأن التحديث يعمل بالشيفرة القديمة غير المحدّثة.

- الثغرة مستغلة فعليًا في هجمات قائمة.
- اكتشف الباحث Umut Bayram من Picus Security ضعف مرحلة التحديث.
- يفك التحديث ملفاته باستخدام شيفرة الموقع القديمة غير المحدّثة.
- المهاجم الذي يتحرك في اللحظة المناسبة قد يتمكن من تنفيذ شيفرة على الخادم.
- ينصح الباحث بحجب الوصول عبر الويب إلى موارد معينة، والنص المتاح ينقطع قبل تحديدها.

وصف الباحث Umut Bayram من Picus Security ضعفًا يتعلق بطريقة تطبيق الإصلاح الخاص بثغرة WordPress

مستغلة فعليًا. ووفق ما توصل إليه، فإن تثبيت التحديث لا يغلق الباب تمامًا لحظة التثبيت في بعض المواقع.

ما الذي توصل إليه الباحث

تفك عملية التحديث ملفاتها باستخدام شيفرة الموقع الحالية، وهي في تلك اللحظة ما تزال النسخة القديمة غير المحدّثة. وعليه، فإن مهاجمًا يتحرك في التوقيت المناسب أثناء التحديث قد يتمكن من تنفيذ شيفرة على الخادم، رغم أن الموقع في طور الإصلاح.

ينصح الباحث بحجب الوصول عبر الويب إلى عناصر معينة أثناء التحديث. غير أن النص المتاح لنا ينقطع قبل تحديدها، ولذلك لا نذكرها هنا. يُرجى الرجوع إلى التقرير الأصلي وإرشادات الجهة المطوِّرة للخطوات الدقيقة.

الدلالة للمؤسسات

الدرس العملي أن فترة التحديث نفسها تنطوي على مخاطر للمواقع المتأثرة. ولأن الثغرة الأساسية مستغلة بالفعل، فإن تأجيل التحديث ليس خيارًا آمنًا. والنهج المناسب هو التحديث السريع مع تقليل التعرض أثناء التنفيذ.

على الفرق التي تدير WordPress للبوابات العامة أو مواقع العملاء أو المواقع التسويقية التعامل مع الأمر كبند إدارة تغيير: جدولة التحديث، وتقييد الوصول أثناء تنفيذه، ثم فحص الموقع بعده بحثًا عن أي مؤشرات عبث.

ما يجب فعله الآن

1. حصر جميع مواقع WordPress، بما فيها التي تديرها فرق التسويق أو أطراف ثالثة.
2. مراجعة التقرير الأصلي وإرشادات الجهة المطوِّرة لمعرفة الوصول الذي يجب حجبه أثناء التحديث.
3. جدولة التحديث في نافذة مضبوطة وتقييد الوصول عبر الويب إلى الموقع أثناء تنفيذه.
4. بعد التحديث، فحص الموقع بحثًا عن ملفات غير متوقعة أو حسابات إدارية جديدة أو نشاط غير معتاد على الخادم.
5. توثيق التحديث ضمن إدارة التغيير والتأكد من تطبيق النسخة المحدّثة.