

نسخ من إضافة Rank Math PRO تحمل باباً خلفياً في هجوم على سلسلة التوريد



احتوت بعض تنزيلات Rank Math PRO بالإصدار 3.0.123 من موقع المطور على برمجية خبيثة خلال نحو 11 ساعة. يجب التعامل مع المواقع التي فُعلتها كمخرقة وتنظيفها، لا تحديثها فقط.

- قد تحتوي النسخة 3.0.123 من Rank Math PRO، المنزلة من الموقع الرسمي بين 15 أكتوبر (20:02) بالتوقيت العالمي) و16 أكتوبر (07:12)، على برمجية خبيثة.
- لم تتأثر النسخة المجانية Rank Math SEO من WordPress.org.
- تحافظ البرمجية على وصول دائم، وتتصل بالنطاق rank1cdn[.]com، وتعيد إنشاء الأبواب الخلفية عند زيارة الموقع.
- قد تنكشف بيانات اعتماد قواعد البيانات ومفاتيح API وأسرار أخرى يصل إليها خادم الويب.
- التحديث أو إلغاء التفعيل لا يزيل التهديد؛ والإصدار السليم هو 3.0.124.

أعلن مطوّر Rank Math PRO، وهي إضافة مدفوعة لتحسين محركات البحث في WordPress، أن عدداً محدوداً من المستخدمين الذين نزلوا الإصدار 3.0.123 من موقعه الرسمي حصلوا على نسخة مفخخة. امتدت الفترة من 15 أكتوبر الساعة 20:02 إلى 16 أكتوبر الساعة 07:12 بالتوقيت العالمي، أي نحو 11 ساعة. وقد أزال المطوّر الملفات المتأثرة وأصدر نسخة سليمة هي 3.0.124.

ما الذي تفعله البرمجية

وفق المطوّر، تُنشئ البرمجية وصلاً دائماً، وتتصل بالنطاق rank1cdn[.]com، وتعيد بناء أبواب خلفية كلما زار أحدهم الموقع المصاب. ويجب اعتبار الأسرار التي يصل إليها خادم الويب، مثل بيانات اعتماد قواعد البيانات ومفاتيح API، مكشوفة.

كما عثر BleepingComputer على عينة PHP في VirusTotal تشترك في مؤشرات الاختراق مع تنبيه المطوّر، منها إنشاء حسابات مديرين ببادئة '_wpsupport'. ويبدو أنها نص نشر أولي قادر على تنفيذ أوامر وتعديل قواعد بيانات WordPress وسرقة بيانات اعتماد السحابة ومفاتيح SSH. ولم يتمكن الموقع من تأكيد توزيعها عبر الإضافة. ولم يرّد المطوّر على أسئلة حول عدد المواقع المتأثرة وطريقة الاختراق الأولى.

إرشادات التنظيف

يجب التعامل مع المواقع التي ثبتت النسخة المتأثرة وفعلتها كمخرقة. والمسار الموصى به هو استعادة الملفات وقاعدة البيانات من نسخة احتياطية سليمة، وإجراء الفحص، وتغيير جميع كلمات المرور والمفاتيح والـ salts. وإن لم تتوفر نسخة آمنة فيلزم تنظيف يدوي: حذف مجلد الإضافة بالكامل والمدخلات الخبيثة في قاعدة البيانات، ثم البحث عن أبواب خلفية أخرى وحسابات مديرين غير مصرح بها وملفات معدّلة ومهام مجدولة وتغييرات خارج WordPress. كما يُنصح بحظر الاتصالات الصادرة إلى rank1cdn[.]com.

أما إذا ثبتت الإضافة دون تفعيل، فتُحذف ثم تُنزل النسخة 3.0.124 ويُفحص الموقع.

ما يجب فعله الآن

1. تحقق مما إذا كان أي موقع، بما فيها المواقع التي تديرها وكالات أو مورّدون، يستخدم Rank Math PRO، وأي إصدار نُزل بين 15 و16 أكتوبر.
2. اعتبر أي موقع فعّل الإصدار 3.0.123 مخترقاً: استعد من نسخة احتياطية سليمة أو نظّف يدوياً وفق إرشادات المطوّر، ولا تكثف بالتحديث.
3. غيّر بيانات اعتماد قواعد البيانات ومفاتيح API ومفاتيح السحابة وSSH وكلمات المرور و salts الخاصة بـ WordPress التي يصل إليها الخادم المتأثر.
4. راجع حسابات المديرين (مثل أسماء المستخدمين ببادئة '_wpsupport') والمهام المجدولة والملفات المعدّلة، واحظر الاتصالات الصادرة إلى rank1cdn[.]com.
5. وثّق الحادثة ضمن إجراءات إدارة الحوادث ومخاطر الأطراف الخارجية، واحذف الإضافة واستبدلها بالنسخة 3.0.124 حيث ثبتت دون تفعيل.