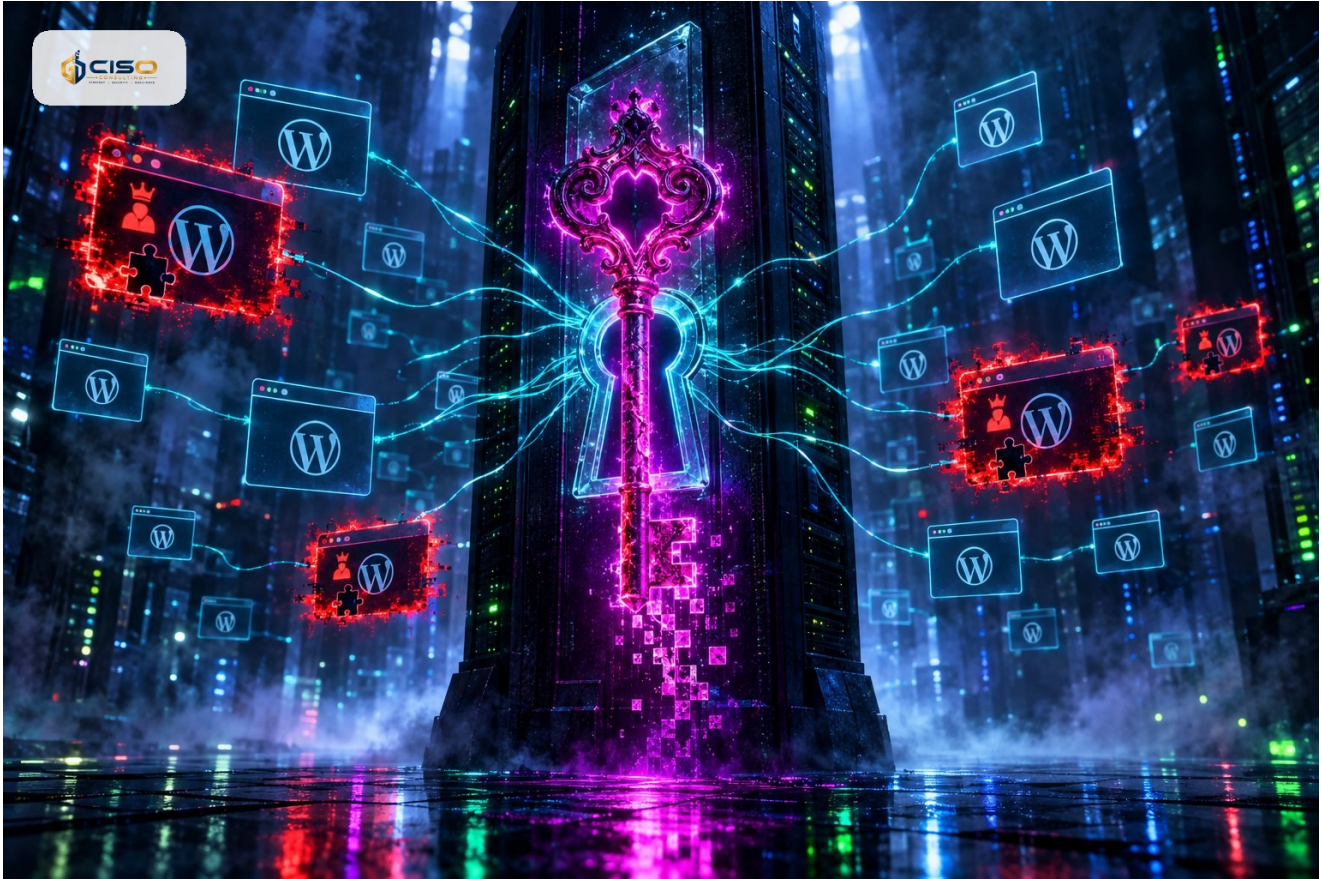


اختراق TeamUpdraft: مفاتيح UpdraftCentral المسروقة تُستخدم لزراعة أبواب خلفية في مواقع WordPress



أعلنت TeamUpdraft عن وصول غير مصرح به إلى موقعها في 17 و18 أكتوبر. ويُقال إن المهاجمين يستخدمون مفاتيح UpdraftCentral المسروقة لتثبيت إضافات خبيثة وإنشاء حسابات مدير على مواقع WordPress المرتبطة.

- رصدت TeamUpdraft وصولاً غير مصرح به خلال عطلة 17 و18 أكتوبر، وترجع أن قاعدة بيانات العملاء قد تم الاطلاع عليها.
- شملت البيانات تجزئات كلمات المرور وإعدادات المصادقة الثنائية ومفاتيح الاتصال لخدمات UpdraftCentral وUpdraftVault وUpdraftClone.
- أفادت Patchstack ببدء الهجمات في 18 أكتوبر الساعة 15:32 بالتوقيت العالمي المنسق لتنفيذ تعليمات برمجية وإضافة حسابات بصلاحيات مدير كاملة، وسُجّلت 99 إضافة خبيثة على الأقل.

بأسماء مختلفة.

- يُقدَّر أن نحو 10% من المواقع التي تستخدم UpdraftPlus لديها مفتاح UpdraftCentral أو Migrator، أي نحو 400,000 موقع.
- يُنصح بتحديث UpdraftPlus إلى 1.26.13 (المجاني) أو 2.26.13 (المدفوع) أو أحدث، وحذف مفاتيح UpdraftCentral الحالية.

أعلنت TeamUpdraft، مطوّرة إضافة النسخ الاحتياطي UpdraftPlus وأدوات WordPress المرتبطة بها، أنها اكتشفت وصولاً غير مصرح به إلى موقعها خلال عطلة 17 و18 أكتوبر. وقد أغلقت مسار الدخول، وأنهت جلسات جميع الحسابات، واستبدلت المفاتيح وبيانات الاعتماد التي ربما تأثرت.

ما الذي انكشف

ترجّح الشركة أن المهاجم وصل إلى قاعدة بيانات العملاء، وهي تضم بيانات العملاء والفوترة وسجل الطلبات وتجزئات كلمات المرور وإعدادات المصادقة الثنائية ومفاتيح الاتصال لخدمات UpdraftCentral وUpdraftVault وUpdraftClone. وتؤكد أنها لا تخزن بيانات الدفع، وأن ملفات UpdraftPlus وتنزيلاتها لم تتأثر، وأن نسخ UpdraftCentral المستضافة ذاتياً غير متأثرة.

استغلال فعلي

تفيد Patchstack بأن المهاجمين يستخدمون المفاتيح المسروقة ضد المواقع المرتبطة بـ UpdraftCentral، وقد بدأ النشاط في 18 أكتوبر. وتنقذ الهجمات تعليمات برمجية عشوائية وتضيف حسابات مدير. وسُجلت 99 إضافة خبيثة على الأقل متخفية في هيئة أدوات صيانة أو تحسين. ووثقت Nethemba هجمات على ثلاثة من مواقعها، نجح تثبيت إضافة خبيثة في اثنين منها، وأشارت إلى أن الأوامر وُقِّعت بمفاتيح صالحة دون استغلال ثغرة. كما ذكرت أن الإصدار الأول من الإصلاح 1.26.12/2.26.12 لم يحذف المفاتيح السحابية بسبب خطأ برمجي.

ويُقدَّر أن نحو 10% من مواقع UpdraftPlus لديها مفتاح UpdraftCentral أو Migrator، ما قد يعرّض نحو 400,000 موقع للخطر.

على الجهات التي تدير مواقع WordPress عبر UpdraftCentral اعتبار المفاتيح مخترقة والتحرك دون انتظار ظهور مؤشرات اختراق.

ما يجب فعله الآن

1. حصر جميع مواقع WordPress، بما فيها التي تديرها وكالات أو موردين، والتي تستخدم UpdraftPlus أو UpdraftCentral.
2. تحديث UpdraftPlus إلى 1.26.13 (المجاني) أو 2.26.13 (المدفوع) أو أحدث، ثم حذف مفاتيح اتصال UpdraftCentral الحالية من إعدادات كل موقع.
3. تدوير بيانات اعتماد التخزين وإعادة تفويض الاتصالات للمواقع التي جرى الوصول إليها عبر UpdraftCentral.
4. مراجعة السجلات والملفات بحثاً عن مؤشرات الاختراق التي نشرتها TeamUpdraft وPatchstack.

Nethembag، والتحقق من وجود إضافات غير معروفة أو حسابات مدير جديدة.

5. عند تأكيد الاختراق: الاستعادة من نسخ احتياطية نظيفة، وتغيير كلمة مرور حساب TeamUpdraft، وإلغاء جميع الجلسات، وإعادة تعيين وسيلة المصادقة الثنائية.

6. تقييم ما إذا كانت البيانات الشخصية على المواقع المتأثرة تستوجب معالجة الحادثة والإبلاغ وفق الإجراءات الداخلية ونظام حماية البيانات الشخصية.