اختراق TeamUpdraft يكشف مفاتيح UpdraftCentral المستخدمة لزرع أبواب خلفية في مواقع ووردبريس

اخترق مهاجمون مجهولون موقع TeamUpdraft وربما وصلوا إلى مفاتيح الربط الخاصة بعملائه لخدمات UpdraftCentral وUpdraftVault وUpdraftClone، واستخدموها لزرع أبواب خلفية في مواقع ووردبريس.

- اخترق مهاجمون مجهولون موقع TeamUpdraft، الجهة المطورة لإضافة النسخ الاحتياطي UpdraftPlus.
- ربما جرى الوصول إلى مفاتيح الربط الخاصة بالعملاء لخدمات UpdraftCentral وUpdraftVault وUpdraftClone.
- وذُكر أن المفاتيح استُخدمت لزرع أبواب خلفية في مواقع ووردبريس.
- تتجاوز عمليات التثبيت النشطة لـ UpdraftPlus أربعة ملايين، ما يوسّع نطاق التعرض المحتمل.
- لا يوضح المقتطف المتاح تفاصيل الباب الخلفي ولا عدد المواقع المتأثرة.

اخترق مهاجمون مجهولون موقع TeamUpdraft، الجهة المطورة لإضافة UpdraftPlus الشائعة للنسخ الاحتياطي في ووردبريس، والتي تتجاوز عمليات تثبيتها النشطة أربعة ملايين. ووفق التقرير، ربما حصل المهاجمون على مفاتيح الربط الخاصة بالعملاء لخدمات UpdraftCentral وUpdraftVault وUpdraftClone، واستخدموها لزرع أبواب خلفية في مواقع ووردبريس.

لماذا يهم ذلك

تعمل مفاتيح الربط كبيانات اعتماد تصل الموقع بخدمات الإدارة عن بُعد والنسخ الاحتياطي. وعند انكشاف المفتاح قد يتمكن المهاجم من التحرك عبر هذه القناة الموثوقة دون الحاجة إلى بيانات دخول الموقع نفسه. وبالنسبة إلى الجهات التي تعتمد على UpdraftPlus أو خدماته المرافقة، يشمل القلق احتمال اختراق الموقع والنسخ الاحتياطية المرتبطة به.

المقتطف المتاح من المصدر محدود؛ فهو لا يشرح آلية عمل الأبواب الخلفية، ولا عدد المواقع المتأثرة، ولا الإجراءات التي أصدرتها TeamUpdraft للمعالجة. وينبغي الرجوع إلى إعلانات المورّد الرسمية لمعرفة هذه التفاصيل وعدم افتراضها.

الخطوات التالية

على الجهات التي تشغّل ووردبريس أن تحدد أولًا ما إذا كانت تستخدم UpdraftPlus أو UpdraftCentral أو

UpdraftVault أو UpdraftClone، بما في ذلك المواقع التي تديرها وكالات أو أطراف ثالثة. وفي حال الاستخدام، يُعامل مفتاح الربط على أنه معرّض للانكشاف، وتُراجع المواقع بحثاً عن تغييرات غير متوقعة، وفق إجراءات الاستجابة للحوادث وإدارة مخاطر الأطراف الثالثة لدى الجهة.

ما يجب فعله الآن

1. حصر جميع مواقع ووردبريس، بما فيها التي تديرها وكالات خارجية، وتحديد ما يستخدم UpdraftPlus أو UpdraftCentral أو UpdraftVault أو UpdraftClone.
2. إلغاء مفاتيح الربط الخاصة بـ UpdraftCentral وUpdraftVault وUpdraftClone وإعادة إنشائها للمواقع المعنية.
3. مراجعة المواقع بحثاً عن مستخدمين إداريين غير متوقعين أو ملفات معدلة أو غير مألوفة أو تغييرات غير معتادة في الإضافات والقوالب.
4. التحقق من سلامة النسخ الاحتياطية المخزنة عبر UpdraftVault أو الخدمات المرتبطة ومن سجلات الوصول إليها.
5. متابعة إشعارات TeamUpdraft الرسمية وتطبيق أي إصلاحات أو إرشادات تصدرها.
6. فتح سجل حادثة وإبلاغ مسؤولي مخاطر الأطراف الثالثة عند الاشتباه بوجود اختراق.