اختراق موقع TeamUpdraft يكشف مفاتيح UpdraftCentral ويُستغل لزرع أبواب خلفية في مواقع ووردبريس



اخترق مهاجمون مجهولون موقع TeamUpdraft وربما وصلوا إلى مفاتيح الاتصال الخاصة بالعملاء لمنتجات UpdraftCentral وUpdraftVault وUpdraftClone، واستخدموها لزرع أبواب خلفية في مواقع ووردبريس.

- مهاجمون مجهولون اخترقوا موقع TeamUpdraft، الجهة المطورة لإضافة UpdraftPlus.
- احتمال وصولهم إلى مفاتيح الاتصال الخاصة بالعملاء لمنتجات UpdraftCentral وUpdraftVault وUpdraftClone.
- استُخدمت المفاتيح لزرع أبواب خلفية في مواقع ووردبريس.
- إضافة UpdraftPlus نسخ احتياطي واسعة الانتشار تتجاوز تثبيتاتها النشطة أربعة ملايين.

ما الذي حدث

اخترق مهاجمون مجهولون موقع شركة TeamUpdraft المطوِّرة لإضافة النسخ الاحتياطي UpdraftPlus لمنصة ووردبريس. وربما حصلوا على وصول غير مصرّح به إلى مفاتيح الاتصال الخاصة بعملاء UpdraftCentral وUpdraftVault وUpdraftClone، ثم استخدموها لزرع أبواب خلفية في مواقع ووردبريس.

تتجاوز تثبيتات UpdraftPlus النشطة أربعة ملايين تثبيت. وتقدّم الشركة أيضاً UpdraftCentral، وهو منتج للإدارة عن بُعد لمواقع ووردبريس. ولا يتضمن المقتطف المتاح تفاصيل إضافية عن نطاق الاختراق أو عدد المواقع المتأثرة أو الأسلوب التقني للأبواب الخلفية.

لماذا يهم ذلك

تعمل مفاتيح الاتصال كبيانات اعتماد موثوقة بين الموقع وخدمة الإدارة أو التخزين. وإذا انكشفت فقد يتمكن المهاجم من التصرف في الموقع دون استغلال ثغرة فيه. لذا ينبغي للجهات التي تستخدم هذه المنتجات في مواقع ووردبريس المؤسسية أو العامة اعتبار المفاتيح مكشوفة محتملًا إلى أن يرد توجيه مغاير من المطوّر.

الخطوات التالية

تحقق مما إذا كانت جهتك، أو أي جهة أو مقاول يدير مواقعك الإلكترونية، يستخدم UpdraftPlus أو UpdraftCentral أو UpdraftVault أو UpdraftClone. وإن كان الأمر كذلك، فراجع الإشعار الرسمي للمطوّر، وبدّل مفاتيح الاتصال، وابحث عن أي تغييرات غير مصرّح بها في المواقع المعنية.

ما يجب فعله الآن

1. حصر جميع مواقع ووردبريس التي تستخدم UpdraftPlus أو UpdraftCentral أو UpdraftVault أو UpdraftClone، بما فيها المواقع التي تديرها وكالات أو مقاولون.
2. تدوير مفاتيح الاتصال الخاصة بهذه المنتجات أو إعادة إنشائها وإلغاء المفاتيح القديمة.
3. مراجعة إشعار المطوّر الرسمي واتباع خطوات المعالجة الواردة فيه.
4. فحص المواقع المتأثرة بحثاً عن مستخدمين إداريين غير معروفين وملفات معدّلة وإضافات غير مألوفة وأي مؤشرات على أبواب خلفية.
5. مراجعة سجلات الوصول إلى التخزين الاحتياطي والإدارة عن بُعد بحثاً عن نشاط غير متوقع.
6. إبلاغ فريق الأمن بأي حادثة مؤكدة، وإبلاغ الجهة المختصة عند اشتراط ذلك في التزامات الإبلاغ عن الحوادث.