GoDaddy يعاني من خرق يكشف بيانات مستخدمي ووردبريس

الخميس 25 نوفمبر 2021 04:05 م

أبلغت شركة GoDaddy العملاقة لاستضافة الويب المنظمين الماليين الأمريكيين عن حدوث خرق للبيانات، وتحذر من إمكانية الوصول إلى بيانات 1.2 مليون عميل.

وفي ملف مع لجنة الأوراق المالية والبورصات، قال كبير مسؤولي أمن المعلومات في GoDaddy، ديميتريوس كوميس، إن الشركة اكتشفت وصولًا غير مصرح به إلى أنظمتها حيث تستضيف وتدير خوادم ووردبريس لعملائها.

وتمثل ووردبريس عبارة عن نظام إدارة محتوى قائم على الويب يستخدمه الملايين لإعداد المدونات أو مواقع الويب. وتتيح GoDaddy للعملاء استضافة تثبيتات ووردبريس الخاصة بهم عبر خوادمهم.

وقالت الشركة، التي لديها أكثر من 20 مليون عميل حول العالم، إن الشخص غير المصرح له استخدم كلمة مرور مخترقة للوصول إلى أنظمتها في 6 سبتمبر تقريبًا.

وأضاف أنها اكتشفت الاختراق في الأسبوع الماضي في 17 نوفمبر. وليس من الواضح ما إذا كانت كلمة المرور المخترقة محمية عبر المصادقة الثنائية.

وقال الملف إن الخرق أثر في 1.2 مليون مستخدم ووردبريس مدار نشط وغير نشط. وتم الكشف عن عناوين بريدهم الإلكتروني وأرقام العملاء. وأوضحت الشركة أن هذا الخرق قد يعرض المستخدمين لخطر أكبر بشأن هجمات التصيد الاحتيالي.

وقال مضيف الويب أيضًا إن كلمة مرور مسؤول ووردبريس الأصلية التي تم إنشاؤها عندما تم تثبيت ووردبريس لأول مرة قد تم الكشف عنها أيضًا. ويمكن استخدام كلمة المرور هذه للوصول إلى خادم ووردبريس الخاص بالعميل.

وقالت الشركة: أصبحت بيانات العملاء النشطين الذين لديهم حسابات FTP لنقل الملفات مكشوفة في الخرق. إلى جانب أسماء المستخدمين وكلمات المرور لقواعد بيانات ووردبريس الخاصة بهم، التي تخزن كل محتوى المستخدم.

وفي بعض الحالات، تم الكشف عن المفتاح الخاص بالعميل في شهادة SSL. ويسمح هذا المفتاح الخاص في حالة إساءة استخدامه للمهاجم بانتحال هوية موقع الويب أو الخدمات الخاصة بالعميل.

قالت GoDaddy إنها تعيد تعيين كلمات مرور ووردبريس الخاصة بالعميل والمفاتيح الخاصة. كما أوضحت أنها بصدد استبدال شهادات SSL.

يذكر أن هذه ليست المرة الأولى التي يتم فيها اختراق GoDaddy في السنوات الأخيرة. وكشف خطأ AWS في عام 2018 البيانات الموجودة عبر خوادم GoDaddy.

كما تم في عام 2020 اختراق 28 ألف حساب مستخدم من قبل فرد غير مصرح له. وتمت الإشارة إلى GoDaddy في العام الماضي كجزء من عملية اختراق أدت إلى إزالة عدد من المواقع في مجال العملات المشفرة.