مايكروسوفت تحذر الآلاف من عملاء السحابة بسبب ثغرة

الجمعة 27 أغسطس 2021 06:21 م

حذرت شركة مايكروسوفت الآلاف من عملائها في مجال الحوسبة السحابية، بما في ذلك بعض أكبر الشركات في العالم، من الثغرة الأمنية التي تركت بياناتهم مكشوفة خلال العامين الماضيين.

وتوجد الثغرة الأمنية في قاعدة بيانات Cosmos المركزية في Microsoft Azure، مما أثر في أكثر من 3300 عميل.

واكتشف فريق بحثي في شركة الأمان Wiz أنه كان قادرًا على الوصول إلى المفاتيح التي تتحكم في الوصول إلى قواعد البيانات التي تحتفظ بها آلاف الشركات.

وبالنظر إلى أن الشركة لا يمكنها تغيير هذه المفاتيح بمفردها، فقد راسلت العملاء عبر البريد الإلكتروني لإخبارهم بإنشاء مفاتيح جديدة.

ووافقت عملاقة البرمجيات على دفع مبلغ 40 ألف دولار لـ Wiz للعثور على الخلل والإبلاغ عنه. وشكرت الباحثين الأمنيين على العمل في ظل الكشف المنسق عن الثغرات الأمنية.

وقال بريد الشركة الإلكتروني للعملاء إنها أصلحت الثغرة الأمنية على الفور للحفاظ على سلامة وحماية العملاء وإنه لا يوجد دليل على أنه تم استغلال الخلل.

وأضاف: ليس لدينا ما يشير إلى أن الكيانات الخارجية خارج الباحث Wiz لديها حق الوصول إلى مفتاح القراءة والكتابة الأساسي.

وقالت Wiz: هذه هي أسوأ ثغرة في السحابة يمكنك تخيلها. هذه هي قاعدة البيانات المركزية لـ Azure، وتمكنا من الوصول إلى أي قاعدة بيانات عملاء أردناها.

وأوضحت Wiz أنها اكتشف المشكلة، التي يطلق عليها اسم ChaosDB، في 9 أغسطس وأبلغت مايكروسوفت في 12 أغسطس.

مايكروسوفت تحذر الآلاف من عملاء السحابة بسبب ثغرة

كان الخلل في أداة تسمى Jupyter Notebook، التي كانت متاحة منذ سنوات. ولكن تم تمكينها افتراضيًا في Cosmos بدءًا من شهر فبراير.

ويأتي هذا الكشف بعد شهور من الأخبار الأمنية السيئة لشركة مايكروسوفت. إذ تم اختراق الشركة من قبل نفس قراصنة الحكومة الروسية المشتبه بهم الذين تسللوا إلى SolarWinds. والذين سرقوا تعليمات برمجية مصدرية من عملاقة البرمجيات.

واحتاجت الشركة إلى إعادة إصلاح عيب في خدمة الطابعة ضمن نظام تشغيلها أتاح عمليات الاستحواذ على الحاسب بشكل متكرر بامتيازات على مستوى النظام.

وأدى عيب في البريد الإلكتروني في Exchange إلى تحذير الحكومة الأمريكية العاجل من أن العملاء بحاجة إلى تثبيت تصحيحات تم إصدارها منذ أشهر لأن عصابات برامج الفدية تستغلها الآن.

وتعد مشاكل Azure مزعجة، وذلك لأن الشركة كانت تدفع الشركات للتخلي عن معظم بنيتها التحتية والاعتماد على السحابة لمزيد من

الأمان. ولكن بالرغم من ندرة الهجمات السحابية، إلا أنها قد تكون أكثر تدميراً عند حدوثها. علاوة على ذلك لا يتم الإعلان عن بعضها أبدًا.