واتساب يطلق إنذار أمني بسبب خلل خطير... تعرف على التفاصيل

تلقى ملايين مستخدمي تطبيق واتساب تنبيها مثيرا للقلق يطالبهم بـ"التحقق من الإعدادات على الفور" أو أنهم سيخاطرون بسرقة رسائلهم النصية.

وسيؤثر هذا على المستخدمين الذين يستخدمون خدمة المراسلة الفورية على أجهزة الكمبيوتر الخاصة بهم.

وإذا كنت تستخدم إصدارًا أقدم من WhatsApp على جهاز كمبيوتر يعمل بنظام Windows، فقد تكون هذه الأخبار مفيدة لك.

وسيتعين على المستخدمين تحديث المنصة، وإلا فقد تتعرض البيانات الشخصية لخطر السرقة.

وتم تأكيد العثور على ثغرة أمنية داخل خدمة الدردشة العالمية والتي قد تسمح لمجرمي الإنترنت بتنفيذ ما يسمى بالرمز التعسفي.

ويتم إخفاء الهجوم الخبيث من المحتالين داخل مرفقات تبدو غير ضارة.

إذا نجح هجوم برمجي عشوائي، فقد يتمكن المتسللون من الوصول بشكل غير مصرح به إلى التفاصيل والمعلومات.

وفي الحالات السيئة بشكل خاص وأسوأ السيناريوهات، قد يتمكنون من الحصول على السيطرة الكاملة على الأجهزة.

وبحسب صحيفة Mirror The ، أوضحت واتساب:"كانت مشكلة التزييف في واتساب لنظام التشغيل ويندوز قبل إصدار قديم تعرض المرفقات وفقًا لنوع MIME الخاص بها ولكنها تحدد معالج فتح الملف بناءً على امتداد اسم ملف المرفق".

وقد يؤدي عدم التطابق المصمم بشكل ضار إلى دفع المتلقي عن غير قصد إلى تنفيذ تعليمات برمجية عشوائية بدلاً من عرض المرفق عند فتح المرفق يدويًا داخل واتساب.

وعلى الرغم من إصلاح خلل في التطبيق، فقد حذر التطبيق من أنه من الضروري لمستخدمي ويندوز الذين يرسلون رسائل عبر الخدمة تحديث برامجهم.

وحذرت من أن:"الناس بحاجة إلى التأكد من أن لديهم الإصدار الأحدث من التطبيق ، وبمجرد قيامهم بتثبيت الإصدار الأحدث مع التصحيح الجديد، ستكون ملفاتهم وبياناتهم آمنة".

وأكد آدم بيلتون، وهو مستشار أول للأمن السيبراني في شركة CyberSmart، أن:"عددا محددا فقط من المستخدمين معرضون للخطر".

وأوضح، من المهم حقًا التأكيد على أن هذه الثغرة الأمنية في واتساب تؤثر على مستخدمي أجهزة سطح المكتب بنظام ويندوز.

وسيكون معظم الأشخاص جزءًا من مجموعة واتساب حيث من الشائع مشاركة الصور وهذا هو المكان الذي تصبح فيه هذه الثغرة خطيرة.

لأنه إذا تمكن مجرم إلكتروني من مشاركة هذه الصورة إما في مجموعتك أو مع شخص تثق به والذي يقوم بعد ذلك بمشاركتها في مجموعتك، فإن أي شخص في تلك المجموعة قد يقوم دون علمه بتنفيذ الكود الخبيث المرتبط بالصورة المشتركة.

وسيستمر مجرمو الإنترنت في استغلال الثغرات الأمنية الموجودة في البرامج التي نستخدمها، وسيستمر مزودو البرامج في توفير التحديثات أو التصحيحات التي تحمينا من الهجمات التي يستخدمها مجرمو الإنترنت.

وأضاف:"لهذا السبب فإن إدارة الثغرات الأمنية، أو تطبيق التحديثات التى يصدرها مزودو البرامج، مهمة للغاية!".