تكنولوجيا

ميكروسوفت تصلح ثغرة خطيرة في ويندوز عمرها 17 عاما

الجمعة 17 يوليو 2020 11:37 ص

سيحصل مستخدمو "ميكروسوفت" أخيرًا على إصلاح لثغرة خطيرة عمرها 17 عامًا في برمجية الشركة، حيث تم تصحيح الخطأ في 14 يوليو / تموز، وتعتبر درجة خطورة هذه الثغرة 10 من 10، وفق تقييم نظام "CVSS".

وقالت "ميكروسوفت": "توجد ثغرة في تنفيذ الأكواد البرمجية عن بُعد في خوادم نظام Windows Domain Name System عندما تفشل في معالجة الطلبات بشكل صحيح. يمكن للمهاجم الذي نجح في استغلال الثغرة الأمنية تشغيل أكواد برمجية عشوائية، وخوادم ويندوز التي تمت تهيئتها كخوادم DNS معرضة لخطر هذه الثغرة".

ويشير DNS إلى "نظام أسماء النطاقات"، الذي يترجم عناوين "IP" إلى عناوين "URL" وهو ما يعادل دفتر هاتف على الإنترنت.

تؤثر الثغرة على جميع إصدارات خوادم "ويندوز"، من 2003 إلى 2019، وكان بإمكانها أن تنتشر عبر البرامج الخبيثة دون تفاعل المستخدم.

كما كان من الممكن أن تمنح الثغرة المتسللين القدرة على الوصول إلى جهاز واحد واستخدامه للوصول إلى أجهزة أخرى، على غرار ثغرة "واناكراي"، التي تم تصنيفه بـ 8.5 على مقياس CVSS"".

وإذا تمكن أحد القراصنة من الوصول إلى الشبكة المحلية، عبر واي فاي الشركة أو كابل إيثرنت، فقد يتمكن من الاستيلاء على الخادم.

من الممكن تحقيق مثل هذا الإجراء باستخدام بريد إلكتروني للتصيد الاحتيالي، وهو بريد إلكتروني يتظاهر بأنه من مصدر موثوق به لنشر الأكواد البرمجية الخبيثة.

وعندما ينقر المستخدم الساذج على هذا البريد الإلكتروني يمنح القرصان السيطرة الكاملة على خادم "DNS".

وقال مدير الأمن الرئيسي في شركة "ميكروسوفت""ميشيل جرون"،: "في حين أنه من غير المعروف حاليًا إن كانت هذه الثغرة الأمنية قد استخدمت في الهجمات النشطة، فمن الضروري أن يقوم العملاء بتطبيق تحديثات ويندوز لمعالجة هذه الثغرة الأمنية في أقرب وقت ممكن".

كان الباحث "ساغي تزيك"، الذي يعمل لدى شركة الأمن الإسرائيلية "تشيك بوينت"، هو من اكتشف هذه الثغرة، وسميت "SigRed".

وعلى الرغم من عدم وجود دليل على استغلال الثغرة، إلا إنه لا يمكن استبعاد الاحتمال، حيث قالت "تشيك بوينت": "نعتقد أن احتمال استغلال هذه الثغرة مرتفع".