الخليج

اقتصاد, تقنية وسيارات

14 ديسمبر 2021 12:45 مساء

أخطر هجوم إلكتروني يستهدف 40% من شركات العالم

ثغرة خطيرة في أداة برمجية مستخدمة على نطاق واسع، سرعان ما تم استغلالها بواسطة لعبة «ماين كرافت» على الشبكة العنكبوتية، لتتحول لاحقاً إلى تهديد رئيسي للمؤسسات والشركات على المستوى العالمي.

وقالت شركة Check Point للأمن السيبراني إن عيباً في كود الكمبيوتر المستخدم على نطاق واسع يدفع إلى 100 محاولة قرصنة جديدة كل دقيقة.

وقالت «تشيك بوينت» إنها شهدت محاولات لاستغلال الثغرة الأمنية في أكثر من 40% من شبكات الشركات على مستوى العالم.

وأضافت أن الخلل الأمني «لوج فور شيل Log4shell» يشكل «خطراً جسيماً»، حيث حذرت الشركات من أنه يتم استخدامه بنشاط من قبل الجماعات الإجرامية، خصوصاً أن التطبيقات الشعبية والخدمات السحابية قد تأثرت.

الكود الذي يحتوي على الخلل مكتوب بلغة «جافا»، وتستخدمه ملايين أجهزة الكمبيوتر التي تشغل خدمات عبر الإنترنت.

وقال بريان فوكس من شركة سوناتايب الأمنية، إنه تم تنزيله في الأشهر الأربعة الماضية 84 مليون مرة من أكبر مستودع عام لمكونات جافا مفتوحة المصدر.

وما يميز الهجوم الحالي غير المسبوق على الأقل منذ عقد من الزمن السهولة التي يمكن للقراصنة من خلالها استغلال الثغرة الأمنية.

حرج، طارئ، تافه

غالباً ما يتم التلاعب بكلمات مثل «حرج» و«طارئ» من قبل أفراد الأمن السيبراني عند اكتشاف عيب كبير. لكن في هذه الأزمة، تم تعليق كلمة أخرى «تافه».

غالباً عندما يتم العثور على ثغرة أمنية في نظام الكمبيوتر، يكون هناك القليل من الوقت لإصلاحها.

ويتعين على مجرمي الإنترنت إيجاد طريقة للهجوم، وعادة ما لا يتمكن سوى أذكى الأطقم من القيام بذلك في الساعات القليلة الأولى. لكن في هذه الحالة، يبدو أنه سهل للغاية.

ولا يعرف حتى الآن عدد محاولات الهجمات الناجحة ـ لكن هذه الحادثة قد تكون مكلفة للغاية بالنسبة للشركات التي تصبح ضحايا. أما بالنسبة للشخص العادي، فليس هناك الكثير مما يمكننا القيام به، سوى التأكد من تحديث التطبيقات والبرامج.

وبحسب «بي بي سي»، فقد اكتشف باحثون في شركة التكنولوجيا الصينية «علي بابا» الخلل الشهر الماضي. لكنها اكتسبت اهتماماً عاماً واسع النطاق بعد اكتشاف تأثيرها في بعض المواقع التي تستضيف إصدارات «فاين كرافت» باستخدام لغة «جافا».

خطر شديد

Log4j التي تشرف على كود Apache Software Foundation وقبل الإعلان عن الخلل، أصدرت مؤسسة إصلاحاً للمشكلة، وصنفت المشكلة ضمن الفئة 10 وهو أعلى مستوى من الجدية.

وشددت جين إيسترلي، مدير وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية، على إلحاح الموقف وكتبت: «لكي نكون واضحين، فإن هذا الضعف يشكل خطراً شديداً»، تم استغلاله على نطاق واسع من قبل المتسللين و«يمثل تحدياً عاجلاً للمدافعين عن الشبكة نظراً لاستخدامه الواسع».

من أجل، تثبيت برامج ضارة تستخرج العملات Log4shell وقال باحثو مايكروسوفت إنهم رأوا متسللين يستخدمون المشفرة، وسرقة كلمات المرور وتسجيلات الدخول، واستخراج البيانات من الأنظمة المخترقة.