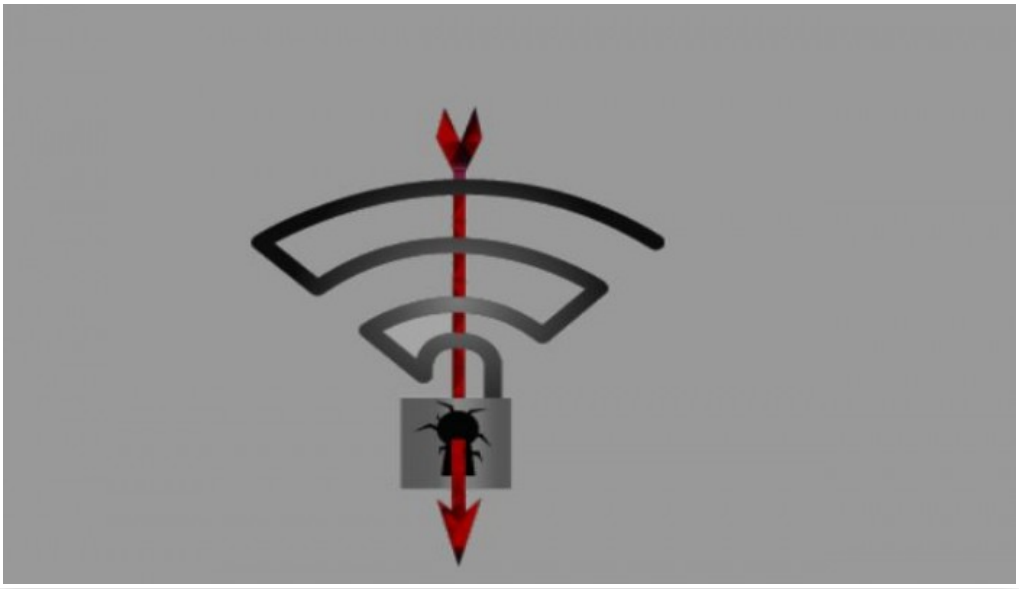
ثغرة خطيرة تصيب جميع شبكات واي فاي وأجهزة أندرويد هي الأكثر تأثرا



الاثنين 16 أكتوبر 2017 05:10 م

قال باحث أمني إن اكتشف ثغرة في بروتوكول الأمان المستخدم في حماية الغالبية العظمى من اتصالات واي فاي، مما يعرض حتمًا حركة الإنترنت اللاسلكية إلى لخطر التنصت الخبيث أو الهجمات الإلكترونية.

وأوضح ماثي فانهوف، وهو خبير أمني في الجامعة البلجيكية كو ليوفن، أن الثغرة موجودة في بروتوكول أمن الشبكات اللاسلكية المعروف اختصارًا باسم "دبليو بي أي 2" WPA2، ونشر تفاصيل الثغرة صباح اليوم الاثنين.

وقال فانهوف: "يمكن للمهاجمين استخدام تقنية الهجوم الجديد هذه لقراءة المعلومات التي كان من المفترض أن تُشفّر بأمان". وأضاف: "يمكن أن يُساء استخدام التقنية لسرقة المعلومات الحساسة مثل أرقام بطاقات الائتمان وكلمات السر ورسائل الدردشة ورسائل البريد الإلكتروني والصور وما شابه".

وأكد فانهوف أن "الهجوم يصيب جميع شبكات واي فاي المحمية الحديثة. ومن الممكن أيضًا، استنادًا إلى تكوين الشبكة، حقن والتلاعب بالبيانات. على سبيل المثال، قد يكون المهاجم قادرًا على حقن برمجية فدية خبيثة أو برمجية خبيثة أخرى في المواقع".

وأضاف فانهوف أن الثغرة تؤثر على عدد من أنظمة التشغيل والأجهزة، بما في ذلك أندرويد، ولينكس، وآبل، ووينـدوز، وأجهزة مثل ميدياتك ولينكسس، وغيرها. وتابع: "إذا كان جهازك يدعم واي فاي، فمن المرجح أن تتأثر، عمومًا، أي بيانات أو معلومات ينقلها الضحية يمكن فك تشفيرها ... بالإضافة إلى ذلك، يمكن أيضًا، استنادًا إلى الجهاز المستخدم وإعدادات الشبكة، فك تشفير البيانات المرسلة نحو الضحية (على سبيل المثال محتوى موقع على شبكة الانترنت)".

وقد حذرت فريق الاستعداد لطوارئ الحاسبات CERT في الولايات المتحدة الأمريكية من الثغرة، التي أطلق عليها باحثون الاسم الرمزي "كراك" KRACK، وهي اختصار لـ "هجوم إعادة تثبيت المفتاح" Key Reinstallation AttaCK.

وقال CERT: "إن تأثير استغلال هذه الثغرات الأمنية يشمل فك التشفير، وإعادة الرزم، واختطاف اتصال TCP، وحقن محتوى HTTP، وغير ذلك"، موضحًا بالتفصيل عددًا من الهجمات المحتملة. وأضاف أنه نظرًا لأن الثغرة في البروتوكول نفسه، فبدلًا من أي جهاز أو برنامج معين، "فإن معظم أو جميع التطبيقات الصحيحة للمعيار سوف تتأثر".

يُشار إلى أن الإعلان عن KRACK يعد تطورًا مهمًا لأن بروتوكول WPA2 هو الأكثر أمانًا في الاستخدام العام لتشفير اتصالات واي فاي. إذ إن البروتوكولات السابقة WPA1 و WEP قد أُخترقت في السابق.

ومع أن الثغرة قد تضر بالأجهزة المختلفة وأنظمة التشغيل بدرجات متفاوتة استنادًا إلى كيفية تنفيذ بروتوكول WPA2، إلا أن إصدار 6.0 "مارشميلو" وما قبله من نظام أندرويد هو الأكثر تضررًا ما يعني أن 41% من أجهزة أندرويد معرضة للخطر، إضافة إلى نظام لينكس. ويعد نظام آي أو إس الأقل تأثرًا بالثغرة.