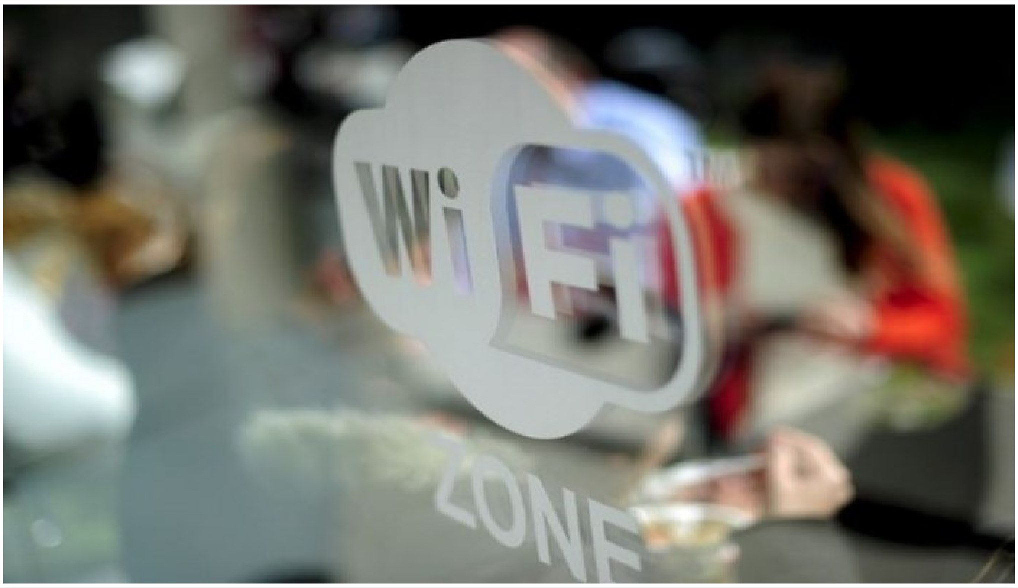
اكتشاف خلل أمني خطير في شبكات الـ "واي فاي" يسهّل القرصنة



الثلاثاء 17 أكتوبر 2017 06:10 م

كشف باحثون ومختصون في مجال أمن التكنولوجيا احتمالية أن تكون شبكات الـ "واي فاي" عُرضة لخلل أمني غير مسبوق يسمح للقراصنة بالتطفل على حركة الإنترنت.

وبحسب خبر نشرته صحيفة "ديلي تلغراف" البريطانية الاثنين، فإن هذا الخلل يعد الأول في تقنيات التشفير الحديثة التي تم استخدامها لتأمين شبكات "واي فاي" على مدى السنوات الـ 14 الماضية.

ويُسمح نظريا -بحسب الصحفية- للمهاجم داخل نطاق الـ"واي فاي" بإدخال فيروسات الكمبيوتر إلى شبكات الإنترنت، وقراءة البيانات مثل كلمات السر وأرقام بطاقات الائتمان والصور المرسلة عبر الشبكة العنكبوتية.

ويصف الخبراء "هجوم الكراك" بأنه "خلل أساسي" في تقنيات الأمن اللاسلكي، حيث أصبحت أنظمة تشغيل "أبل" و"أندرويد" و"ويندوز" معرضة لهذه المشاكل، والتي لن يتم إصلاحها عن طريق تغيير كلمات مرور شبكة الـ"واي فاي"، وبإمكان شركات التكنولوجيا فقط إصدار أو تطوير تحديثات لإصلاح هذا الخلل.

ويقول البروفيسور "ألان وودوارد" من مركز أمن الانترنت التابع لجامعة ساري البريطانية: "يبدو أن هذا الخلل يؤثر على جميع شبكات الـ"واي فاي"، وهو عيب أساسي في البروتوكول الأساسي".

وتابع وودوارد: "حتى لو كنت قد فعلت كل شيء بشكل صحيح فإن أمن جهازك سيبقى معرضًا للخطر، وهذا يعني أنه لا يمكنك الوثوق في الشبكة الخاصة بك، كما لا يمكنك افتراض أن ما يحدث بين جهاز الكمبيوتر الخاص بك وجهاز توزيع الإنترنت آمن".

يوجد لدى شبكات الـ "واي فاي" ما يطلق عليه المختصون "حركة مرور" مشفرة ببروتوكول يعرف باسم "Wpa" أو "Wpa-2"، وهو موجود منذ العام 2003 وإلى الآن لم يتم كسره من قبل القراصنة.

ويحمي هذا البروتوكول البيانات، لأنها تنتقل من جهاز كمبيوتر أو الهاتف الذكي إلى جهاز توزيع الإنترنت، مما يمنع المتسللين من تتبع الشبكات أو إدخال التعليمات البرمجية الخبيثة في عمليات النقل.

ومن ناحية أخرى، فإن الاتصال الآمن بأي شبكة ينطوي على اتصال رباعي الاتجاهات بين الجهاز المستخدم وجهاز توزيع الإنترنت لضمان عدم تمكن أي شخص آخر من فك تشفير حركة المرور.

ووجد الباحث "ماثي فانهوف" من جامعة لوفين في بلجيكا وسيلة لتثبيت "مفتاح" جديد يستخدم لتشفير الاتصالات على الشبكة، مما يسمح للقراصنة بالوصول إلى البيانات، ويتضمن ذلك كلمات المرور وأرقام بطاقات الائتمان والصور والرسائل المرسلة عبر شبكة ما لكي يتم سرقتها، أو هجمات إلكترونية يتم إدراجها في حركة المرور.

ولا يمكن تنفيذ الهجوم عن بعد، فالمهاجم يجب أن يكون في نطاق شبكة "واي فاي" يتصل فيها "الضحية" ليتمكن من تنفيذ الهجوم، بالإضافة إلى أن ذلك لن يعمل على مواقع الويب المضمونة - تلك التي تستخدم "https" في بداية عنوان الويب بدلًا من "http".

ويرى البروفيسور وودوارد أن الطريقة الوحيدة لإصلاح الخلل "يكون بالاستبدال يدويًا أو تصحيح كل جهاز موزع للإنترنت في المنازل"، مضيفا: "بالرغم من أن الهجوم ليس سهلًا من الناحية الفنية، إلا أن الأدوات ستنشأ قريبًا مما يسمح للمجرمين بتنفيذ الهجوم".