6 نصائح لحماية شبكة "wifi" من الاختراق

الجمعة 20 أكتوبر 2017 10:10 م

اكتشف خبير في أمن المعلومات ثغرة أمنية كبيرة في نظام الحماية الخاص بمستخدمي شبكة الإنترنت اللاسلكية (واي فاي) في الشركات والمنازل في أنحاء العالم، ما يسمح باختراقها وسرقة البيانات الشخصية.

هذه الثغرة، التي اكتشفها ماثي فانهوف، وهو خبير في جامعة "كو ليوفن" البلجيكية قبل أيام، تتعلق بنظام للتحقق يُستخدم على نطاق واسع لتأمين الاتصال بالشبكة اللاسلكية، يسمى "WPA2"، وهو بروتوكول مسؤول عن تشفير وإغلاق موزعات الإشارة، ويستخدم أيضًا في تأمين نسبة كبيرة جدًا من أجهزة "الراوتر".

**** معلومات خطيرة**

وأطلق الخبراء على تلك الثغرة اسم "كراك" (Krac)، وهو اختصار لـ"هجوم إعادة تثبيت المفتاح" (Key Reinstallation Attack)، ووصفوها بأنها "عيب أساسي" في تقنيات الأمن اللاسلكي.

وتسمح هذه الثغرة للقراصنة، الموجودون ضمن نطاق الشبكة، بالدخول إليها، دون علم المستخدم، والتجسس على جميع الملفات المتبادلة والبيانات، طالما أنها غير مشفرة، مثل قراءة الاتصالات وأرقام بطاقات الائتمان والصور المرسلة عبر الإنترنت، فضلاً عن إمكانية شن هجمات إلكترونية.

وتسمح تلك الثغرة للقراصنة بالحصول على معلومات المستخدمين، مثل أرقام البطاقات الائتمانية وكلمات المرور (السر) والمحادثات ورسائل البريد الإلكتروني والصور.

ومنذ عام 2003، يستخدم بروتوكول "WPA2" في الشبكات اللاسلكية ولم يتم اختراقه من قبل، حيث يحمي البيانات، التي تمر بين "الراوتر" وجهاز الكمبيوتر أو جهاز الهاتف، عبر وقف المتسللين والبرمجيات الخبيثة.

ويعتبر الخبراء أن الإعلان عن اختراق هذا البروتوكول يعد تطورًا مهمًا يبعث على القلق؛ لكونه الأكثر أمانًا في الاستخدام العام لتشفير اتصالات "واي فاي"، إذ إن البروتوكولات السابقة "WPA1" و"WEP" تم اختراقها في السابق، وهو ما يضع الخبراء أمام تحدٍ، وهو إمكانية إصدار بروتوكول جديد أكثر أمنًا.

**** الأجهزة المستهدفة**

وبحسب مكتشف هذه الثغرة، ماثي فانهوف، فإن طريقة الهجوم "مُدمرة بشكل استثنائي" لأنظمة "أندرويد" الخاصة بالهواتف المحمولة، وأنظمة "لينوكس" و"ويندوز" المُستخدمة في تشغيل أجهزة الكمبيوتر، و"أو إس إكس" الخاصة بهواتف شركة "أبل"، وغيرها.

وقال أستاذ الأمن الإلكتروني في جامعة "ساري" البريطانية، البروفيسور آلن وودورد، إن "هذه ثغرة في نمط التشغيل المعتاد، ولذا على الأرجح فإنها تمثل خطورة عالية على جميع الاتصالات اللاسلكية الموجودة، سواء في الشركات أو المنازل".

وأوضح وودورد، في حديث لهيئة الإذاعة البريطانية (بي بي سي) الإثنين الماضي، أن "مدى الخطورة يعتمد على عدد من العوامل، بينها الوقت الذي يستغرقه شن هجوم أو إذا كان الشخص بحاجة للاتصال بالشبكة لإطلاق هجوم، لكن البحث يشير إلى أنه من السهل نسبياً شن هجوم بسبب هذه الثغرة".

وأضاف أن "هذا الأمر يجعل معظم الاتصالات بشبكة الاتصالات اللاسلكية عرضة للخطر، حتى يتسنى لموردي أجهزة التوجيه (الشركات) من إصدار تحديثات أمنية للتغلب على هذه المشكلة".

**** استجابة من الشركات**

وعلى الفور تلقت شركات التكنولوجيا الكبرى المصنعة لنقاط الاتصال والأجهزة الإلكترونية وأنظمة التشغيل، هذا التحذير الأمني.

وأعلنت "مايكروسوفت" عن إصدار تحديث لنظام "ويندوز 7و8 و10"، داعية المستخدمين إلى تحميله فوراً.

وكشفت أنها تعتزم إصدار تحديث لبرنامج "أندرويد"، الذي تعمل عليه غالبية الهواتف الذكية، بحلول 6 نوفمبر/ تشرين ثانٍ المقبل.

فيما أعلنت شركة "أبل" أنها أصلحت الثغرة في التحديثات المقبلة لأنظمة تشغيل أجهزتها، المتوقع إصدارها قبل نهاية أكتوبر/ تشرين أول الجاري.

أما شركة "جوجل" فأعلنت أنها على دراية بالثغرة، وستعمل على تحديث أي أجهزة متضررة لتأمينها، خلال الأسابيع المقبلة.

**** منع الاختراق**

وعامة، سارعت شركات التكنولوجيا وخبراء أمن المعلومات إلى إصدار تعليمات وتحذيرات لمستخدمي الإنترنت عبر شبكات الـ"واي فاي"، بعد اكتشاف هذه الثغرة الأمنية.

ووفق صحيفة "تليغراف" البريطانية، الإثنين الماضي، يجب إتباع ست نصائح لتجنب هجوم "كراك" (Krac) المدمر على أجهزة الهواتف الذكية والكمبيوتر المتصلة بشبكة الـ"واي فاي".

ودعا خبراء أمن المعلومات مستخدمي شبكات الـ"واي فاي" إلى التنبه والتحميل الفوري للتحديثات التي ستصدرها شركات التقنية لأنظمة التشغيل، مثل و"يندوز" و"أندرويد" و"آي يو إس"، وغيرها، لتجنب الاختراق.

وأضافوا أن شبكات الـ"واي فاي" غير المزودة بكلمة المرور (السر) عرضة في الغالب لهجمات القراصنة، لذا يرجى تزويد هذه الشبكات بكلمات مرور قوية وتغييرها باستمرار.

ودعا الخبراء المستخدمين أيضًا إلى تجنب الاتصال بشبكات الـ"واي فاي" الموجودة في الأماكن العامة، كالمقاهي والمطارات والفنادق والشوارع، كلما أمكن ذلك.

كما نصحوا بتزويد متصفحات الإنترنت بخاصية تسمى "HTTPS Everywhere"، لتأمين البيانات، ويمكن تنزيلها على الرابط التالي:

https://www.eff.org/https-everywhere

وكذلك طالب الخبراء بالتأكد من زيارة المواقع التي تستخدم بروتوكول "HTTPS" قبل عنوان الموقع، الذي يبدأ بـ ".www"؛ لأنه آمن نسبيا ضد هجمات القراصنة، وعدم زيارة المواقع التي تستخدم بروتوكول "HTTP".

وفي حال وجود مواقع ضرورية للمستخدم على بروتوكول "HTTP" غير الأمن، يمكن له أن يستخدام برنامج الحماية "VPN"، وهي اختصار للشبكه الخاصة الافتراضية (Virtual Private Network)، وهي تخفي معلومات المستخدمين وتحميها، ومنها برامج "NordVPN" و"TunnelBear".