البلوتوث يسمح للقراصنة بالسيطرة على الأجهزة

السبت 16 سبتمبر 2017 04:09 م

اكتشف الباحثون في شركة أبحاث الأمن أرميس Armis وسيلة جديدة للسيطرة على الأجهزة من خلال اتصال البلوتوث Bluetooth، وتهدد الوسيلة الجديدة المسماة BlueBorne الملايين من الهواتف المحمولة وأجهزة الحواسيب المحمولة والأجهزة المنزلية الذكية وتضعها ضمن مدى القراصنة، حيث تؤثر هذه الوسيلة على جميع الأجهزة تقريباً المالكة لاتصال البلوتوث، ووفقاً لشركة أبحاث الأمن فإن المشكلة لا تقتصر على نوع واحد من الهاتف أو نظام التشغيل

ويمكن استغلال الثغرات الأمنية في البلوتوث، والتي تسمح للاجهزة بالارتباط لاسلكياً عبر مسافات قصيرة، للسماح للقراصنة بالاستيلاء على الأجهزة وسرقة البيانات وكلمات المرور، حيث تؤثر المشكلة على المنتجات المختلفة من العلامات التجارية الكبرى، بما في ذلك شركة آبل وسامسونج وجوجل ومايكروسوفت

وقد تمكن الباحثون من التسلل للهاتف الذكي جوجل بيكسل Google Pixel، وهواتف وحواسيب سامسونج جالاكسي Samsung Galaxy، وساعة إل جي الذكية LG Sports، ونظام الصوت في السيارة، وقال الباحثون أنهم قد عثروا على هذه المشكلة أيضاً عبر المليارات من أجهزة العاملة بواسطة أنظمة أندرويد ومايكروسوفت وسامسونج ولينكس، كما أن أجهزة آيفون وحواسيب آيباد غير المحدثة إلى نسخة iOS 10 أو أحدث هي أيضاً عرضة للخطر

وصرحت شركة أرميس أن هجوم بلوبورن BlueBorne يتعلق بنا بسبب الوسيلة التي يعمل بها، على عكس غالبية هجمات اليوم التي تعتمد على الانترنت، حيث ينتشر بلوبورن عبر الهواء، وأن هجمات البلوتوث قد تكون أكثر عدوانية بالمقارنة مع الهجمات السابقة، والتي لا تزال مكتشفة بمعظم الإجراءات الأمنية الحالية، وعلى عكس البرامج الضارة التقليدية أو الهجمات فإن المستخدم لا يضطر إلى الضغط على وصلة أو تحميل ملف مشكوك فيه، أي لا يلزم أي إجراء من قبل المستخدم لتمكين الهجوم

ويستغرق هجوم بلوبورن حوالي 10 ثواني، بحيث يمكنه اختراق الأجهزة التي يكون فيها ميزة البلوتوث مفعلة، حتى لو كانت الأجهزة غير متصلة بأي شيء، وقد قدمت كل من مايكروسوفت وجوجل ولينكس تحديثات لإصلاح المشكلة، وأن أجهزة آبل التي يتم تحديثها محمية، بينما لم توضح شركة سامسونج، والتي تعتبر اكبر الشركات المصنعة للهواتف الذكية في العام، موعد صدور التحديث الأمني الخاص بها