تنبيه هام وعاجل لمستخدمي "آبل": ثغرات تهدد أمن أجهزتكم



حذّر فريق من خبراء الأمن أن مجرمي الإنترنت يمكنهم استغلال ثغرات Airplay لتنفيذ برمجيات خبيثة، وسرقة معلوماتك الشخصية، والتسبب في تعطل الجهاز، والاستماع إلى المحادثات.

واكتشف باحثو الأمن السيبراني ثغرات خطيرة في أجهزة "آيفون" تسمح للمهاجمين باختراق أي جهاز متصل بشبكة واي فاي نفسها، والثغرات عددها "23" وموجودة في تطبيق "AirPlay"، الذي يسمح للمستخدمين بث الصوت والفيديو والصور من أجهزة أبل إلى أجهزة ذكية أخرى.

ووجد الخبراء أن:"اثنتين من هذه الثغرات سمحتا للمهاجمين باستغلال أجهزة آيفون كسلاح، ما سمح لهم بنشر برمجيات خبيثة تنتشر إلى الأجهزة المتصلة بأي شبكة واي فاي يتصل بها الجهاز المصاب".

وأطلق الخبراء على هذه الثغرات الأمنية والهجمات اسم "AirBorne"؛ لأن الهجمات تنتقل عبر الشبكات اللاسلكية، ما يسمح للمتسللين بالسيطرة الكاملة على الأجهزة واستغلالها.

وأما الثغرات الأخرى التي تم اكتشافها، فقد سمحت للمخترقين بتنفيذ برمجيات خبيثة من موقع بعيد، ما قد يؤدي إلى اكتساب سيطرة غير مصرح بها، كما كشف الباحثون عن خلل سمح لمجرمي الإنترنت بالوصول إلى بيانات حساسة وقراءتها.

وأبلغ الباحثون شركة أبل بهذه الثغرات، التي أصدرت بدورها تحديثات برمجية لأجهزة iPhone وiPad وMac وأجهزة Pro Vision Apple لإصلاحها منذ أيام.

وصرح متحدث باسم أبل أن:"المهاجمين لا يمكنهم استغلال هذه الثغرات إلا إذا كانوا متصلين بشبكة واي فاي نفسها التي يتصل بها الجهاز الذي يستهدفونه".

وقدر الباحثون أن عدد أجهزة الجهات الخارجية المتوافقة مع AirPlay والمعرضة للخطر يبلغ عشرات الملايين، الأمر الذي قد يستغرق سنوات لإصلاحها أو هنالك بعضها لن يتم إصلاحها أبدًا.

وهذا يعني أنه إذا تمكن أحد المخترقين من الوصول إلى شبكة واي فاي نفسها التي يتصل بها أحد هذه الأجهزة، فيمكنه السيطرة عليها ثم استخدامها كنقطة وصول للتسلل إلى الأجهزة الأخرى على الشبكة.

ولذلك، حتى لو كانت أجهزة أبل الخاصة بك مُحدَّثة، فهذا لا يعني أنها محمية تمامًا من المخترقين الذين قد يستغلون ثغرات AirPlay هذه، ولحماية نفسك من الاختراق، وشدد الباحثون على ضرورة تثبيت أحدث إصدار من البرنامج على جميع أجهزة أبل الخاصة بك، كذلك يمكنك أيضًا تعطيل ميزة AirPlay بالكامل.