تهديد سيبراني واسع يطال أجهزة آبل وأنظمة المنازل الذكية في العالم

كشفت شركة الأمن السيبراني "Security Oligo" عن، ثغرات أمنية خطيرة في تقنية "AirPlay"، تتيح للقراصنة اختراق أجهزة "آيفون" وMac وحتى أنظمة السيارات الذكية، دون الحاجة لأي تفاعل من المستخدم.

وحملت مجموعة الثغرات اسم "AirBorne"، وبلغ عددها "23" ثغرة تم اكتشافها في بروتوكول AirPlay المستخدم لبث الصوت والفيديو والصور بين أجهزة آبل والأجهزة الذكية المتوافقة.

ووفقاً للباحثين، فإن:"17 من هذه الثغرات يمكن استغلالها فعلياً لتنفيذ هجمات سيبرانية تستهدف مليارات الأجهزة المتصلة بالشبكات اللاسلكية، وقد تمكن فريق Oligo من إثبات إمكانية تنفيذ هجمات "دون نقرة"، حيث يُصاب الجهاز دون أن يقوم المستخدم بأي إجراء".

ولا تقتصر التهديدات على أجهزة آبل فقط، بل تشمل أيضاً الأنظمة الداعمة لـCarPlay ومكبرات الصوت الذكية، مما يتيح تنفيذ هجمات خفية داخل السيارات أو المنازل دون علم المستخدمين.

ومن بين الثغرات المكتشفة، هناك ثغرة وصفها الباحثون بـ"الخطيرة" تتيح استبدال تطبيق Music Apple على نظام "macOS" برمز خبيث يُثبّت تلقائياً، ما يمنح القراصنة القدرة على التحكم بالجهاز عن بُعد.

وتتيح ثغرات أخرى تنفيذ تعليمات برمجية خبيثة عن بُعد، وسرقة البيانات الحساسة، بل ونشر برمجيات ضارة إلى أجهزة أخرى على الشبكة نفسها.

وأصدرت شركة آبل تحديثات أمنية في 31 آذار/مارس شملت أنظمة iOS 18.4 وmacOS Sequoia 15.4 وtvOS 18.4، بهدف سد هذه الثغرات.

ورغم ذلك، لا تزال عشرات الملايين من الأجهزة التي تنتجها جهات خارجية وتدعم AirPlay مهددة، نظراً لاحتمال عدم تلقيها تحديثات أمنية من الشركات المصنعة.

-وقال متحدث باسم آبل لموقع "ديلي ميل" إن:"استغلال هذه الثغرات يتطلب تواجد القراصنة على شبكة Wi Fi نفسها الخاصة بالجهاز المستهدف، إلا أن Oligo رتّحذ من أنه كافياً يعد لا هذا أن خصوصاً، للحماية كافيا يعد لا هذا أن من رتّحذ Oligo أن إلا ،المستهدف بالجهاز الخاصة نفسها Fi الأماكن العامة التي تشهد اتصال عدد كبير من الأجهزة بشبكة واحدة".

وقدّرت آبل عدد أجهزتها النشطة حتى يناير 2025 بنحو "2.35" مليار جهاز، بينها "1.8" مليار جهاز آيفون و"500" مليون جهاز آخر يدعم AirPlay، ما يعكس حجم التهديد الذي تشكله هذه الثغرات.

خطوات للحماية من تهديدات AirBorne:

تعطيل AirPlay من الإعدادات، وتقنين الوصول ليشمل "المستخدم الحالي" فقط.

تثبيت برامج أمان موثوقة على أجهزة آبل.

مراجعة الشركات المصنعة لأجهزة AirPlay من جهات خارجية، والتأكد من توفر التحديثات الأمنية بانتظام.

وكما توصي Oligo بتعطيل ميزة AirPlay نهائياً، خصوصاً في البيئات الحساسة، نظراً لأن الجهاز يبقى

في وضع الاستماع لإشارات AirPlay حتى عند عدم استخدامه، مما يوسّع "سطح الهجوم" أمام القراصنة.

كيفية تعطيل AirPlay على "آيفون":

افتح تطبيق الإعدادات.

اذهب إلى: عام > AirPlay والاستمرارية.

في خيار "AirPlay تلقائياً"، اختر "أبداً".