ثغرات خطيرة في سماعات لاسلكية قد تحولها لأداة تجسس

الثلاثاء 15 سبتمبر 2026 08:30 م

كشفت أبحاث حديثة في مجال الأمن السيبراني عن ثغرات خطيرة في شرائح إلكترونية تستخدمها مجموعة واسعة من سماعات الأذن والرأس والأجهزة الصوتية اللاسلكية، بما قد يسمح لمهاجم قريب من الجهاز بالوصول إلى بيانات حساسة، وفي بعض الحالات السيطرة على الميكروفون والتقاط الأصوات المحيطة بالمستخدم.

وتتركز المخاوف حول شرائح Airoha المستخدمة في منتجات لعدد من العلامات التجارية المعروفة، بعدما تمكن باحثون أمنيون من اكتشاف ثلاث ثغرات يمكن استغلالها للوصول إلى أجزاء من ذاكرة الأجهزة والبيانات المرتبطة بها، فضلًا عن إمكانات أخرى تتجاوز مجرد اختراق السماعة نفسها.

وأثارت النتائج اهتمامًا واسعًا في أوساط الأمن السيبراني، ليس فقط بسبب عدد الأجهزة التي تستخدم الشرائح المتأثرة، ولكن أيضًا بسبب طبيعة الصلاحيات التي قد يحصل عليها المهاجم في حال نجاحه في استغلال الثغرات، خصوصًا عندما يتعلق الأمر بالميكروفون والبيانات المرتبطة بالهاتف.

ثلاث ثغرات تثير المخاوف

بحسب أبحاث نشرها موقع Insinuator المتخصص في أمن الأجهزة والثغرات، جرى تحديد ثلاث ثغرات في شرائح Airoha، وحملت أرقام CVE-2025-20700 وCVE-2025-20701 وCVE-2025-20702.

وتسمح هذه الثغرات، وفق سيناريوهات الاختبار التي أجراها الباحثون، بفتح الطريق أمام المهاجم للوصول إلى أجزاء من ذاكرة الجهاز، بما في ذلك ذاكرة الوصول العشوائي وذاكرة التخزين، وهو ما قد يكشف معلومات لم يكن من المفترض أن تكون متاحة لطرف خارجي.

وتكمن المشكلة في أن السماعة اللاسلكية لا تعمل باعتبارها جهازًا مستقلًا تمامًا، بل ترتبط عادة بالهاتف وتحتفظ ببيانات ومعلومات عن الأجهزة التي سبق أن اتصلت بها، ما يجعل اختراقها بوابة محتملة للوصول إلى معلومات إضافية تتجاوز حدود السماعة.

ولا يعني ذلك أن كل سماعة تستخدم البلوتوث أصبحت معرضة تلقائيًا للاختراق، إذ يرتبط الخطر تحديدًا بالأجهزة التي تستخدم الشرائح والبرمجيات المتأثرة بهذه الثغرات، كما تختلف درجة التأثر من طراز إلى آخر.

الميكروفون في دائرة الخطر

من أبرز الجوانب التي أثارت القلق في نتائج الاختبارات إمكانية الوصول إلى ميكروفون السماعة في بعض السيناريوهات.

ويعني نجاح المهاجم في استغلال هذه الإمكانية أنه قد يتمكن من التقاط الأصوات الموجودة في محيط الجهاز، وهو ما يحول السماعة من مجرد وسيلة للاستماع إلى الموسيقى أو إجراء المكالمات إلى نقطة يمكن استخدامها في مراقبة البيئة المحيطة بالمستخدم.

وتزداد حساسية الأمر عندما تكون السماعة موجودة في أماكن خاصة أو خلال محادثات لا يرغب أصحابها في تسجيلها أو الاطلاع عليها، إذ قد لا يكون المستخدم مدركًا أصلًا لوجود محاولة للوصول إلى الميكروفون.

كما أظهرت الاختبارات إمكانية الوصول، في بعض الحالات، إلى معلومات مرتبطة بالهاتف المتصل بالسماعة، ومن بينها رقم الهاتف وسجل المكالمات وجهات الاتصال.

وبذلك لا تقتصر المخاطر على البيانات المخزنة داخل السماعة، وإنما يمكن أن تمتد إلى المعلومات التي ترتبط بها نتيجة استخدامها كجهاز متصل بالهاتف.

هجوم دون اقتران تقليدي

ومن النقاط الأكثر إثارة للانتباه أن بعض سيناريوهات الاستغلال لا تتطلب بالضرورة المرور بعملية الاقتران والمصادقة المعتادة بين الأجهزة.

وهذا الأمر يرفع مستوى الخطورة؛ لأن المستخدم قد لا يرى إشعارًا واضحًا يفيد بوجود محاولة اتصال أو اقتران جديدة، وبالتالي قد يصعب عليه اكتشاف الهجوم في الوقت المناسب.
ومع ذلك، لا يمكن تنفيذ الهجوم عن بُعد من أي مكان، إذ يحتاج المهاجم إلى أن يكون قريبًا نسبيًا من الجهاز المستهدف وأن يظل داخل نطاق اتصال البلوتوث حتى يتمكن من تنفيذ الخطوات اللازمة لاستغلال الثغرات.

وتشير هذه النقطة إلى أن الخطر، رغم كونه حقيقيًا، ليس بالضرورة تهديدًا عشوائيًا يطال جميع مستخدمي السماعات اللاسلكية في أي مكان، وإنما يصبح أكثر أهمية في الحالات التي يكون فيها الشخص أو المكان هدفًا محتملًا للمراقبة المتعمدة.

علامات تجارية ضمن القائمة

وشملت قائمة الأجهزة التي تعتمد على شرائح Airoha المتأثرة منتجات تابعة لعدد من الشركات المعروفة في سوق الأجهزة الصوتية، بينها سوني وبوز وجيبه بي إل وجابرا ومارشال وبيردايناميك وجيبه لاب.

لكن وجود إحدى هذه العلامات التجارية في القائمة لا يعني أن جميع منتجاتها معرضة للخطر.

فالشرائح المستخدمة تختلف بين الطرازات، كما تختلف إصدارات البرمجيات الثابتة وطريقة دمج الشرائح داخل الأجهزة، ولذلك يعتمد تحديد مدى التأثر على الطراز والإصدار البرمجي المستخدمين في كل جهاز.

ولهذا السبب، فإن مجرد امتلاك سماعة من إحدى الشركات المذكورة لا يكفي وحده للحكم بأنها معرضة للاختراق، بل يجب التأكد من الطراز المحدد وما إذا كان ضمن الأجهزة التي تتأثر بالثغرات المكتشفة.

خطر يتجاوز التنصت

لا تتوقف المخاطر التي كشفها الباحثون عند إمكانية الوصول إلى الميكروفون أو استخراج بعض البيانات.

فقد أظهرت الاختبارات إمكانية استغلال بعض الثغرات للوصول إلى مفاتيح وبيانات مرتبطة بعملية الاقتران بين السماعة والهاتف، وهو ما قد يسمح في ظروف معينة بمحاولة انتحال الجهاز أمام الهاتف الذي سبق أن اتصل به.

وتعني هذه الإمكانية أن المشكلة ليست مجرد ثغرة يمكن استخدامها للاستماع إلى المحادثات، وإنما قد تؤثر أيضًا في آلية الثقة التي تنشأ بين الأجهزة عند الاتصال ببعضها.

ومع ذلك، فإن الوصول إلى هذه المرحلة لا يحدث بمجرد وجود السماعة بالقرب من مهاجم، إذ يتطلب استغلال سلسلة الثغرات مهارات تقنية ومعرفة متقدمة بطريقة عمل الشرائح والبرمجيات، وهو ما يقلل من احتمالية تعرض المستخدم العادي لهجوم عشوائي.

لكن الباحثين يحذرون من أن طبيعة المخاطر تصبح أكثر أهمية عندما يكون الجهاز مملوكًا لشخص قد يمثل هدفًا محددًا للمراقبة أو التجسس.

تحديثات لمواجهة الثغرات

وبعد اكتشاف الثغرات، عملت شركة Airoha على توفير تحديثات لمعالجة المشكلات وإرسال الإصلاحات إلى الشركات المصنعة للأجهزة

المتأثرة.

لكن وصول التحديث إلى المستخدم لا يعتمد على الشركة المطورة للشرائح وحدها، وإنما يرتبط أيضًا بالشركة المنتجة للسماعة والطراز المستخدم، إضافة إلى الطريقة التي تتيح بها الشركة تحديث البرنامج الثابت للجهاز.

وهنا تظهر أهمية عدم التعامل مع السماعات اللاسلكية باعتبارها أجهزة لا تحتاج إلى تحديثات. فالبرنامج الثابت، مثل أنظمة تشغيل الهواتف والحواسيب، قد يحتوي على ثغرات أمنية تحتاج إلى إصلاحات دورية.

وينصح المستخدمون بالتحقق من تطبيق الشركة المصنعة للسماعة، أو إعدادات الجهاز، لمعرفة ما إذا كان هناك إصدار جديد من البرنامج الثابت، خصوصًا بالنسبة للطرازات التي تعتمد على شرائح متأثرة.

كيف يقلل المستخدم الخطر؟

يمكن اتخاذ مجموعة من الإجراءات البسيطة لتقليل فرص التعرض لهجمات تستهدف البلوتوث أو الأجهزة اللاسلكية.

ويأتي في مقدمة هذه الإجراءات تحديث السماعة والهاتف باستمرار، وعدم تأجيل تثبيت التحديثات الأمنية والبرمجيات الثابتة عندما تكون متاحة. كما يُنصح بإيقاف البلوتوث عندما لا تكون هناك حاجة لاستخدامه، خاصة في البيئات التي تتطلب مستوى مرتفعًا من الخصوصية.

ومن المفيد كذلك مراجعة قائمة الأجهزة المقترنة بالهاتف وحذف الأجهزة القديمة أو التي لم تعد مستخدمة، إلى جانب تجنب قبول اتصالات أو طلبات اقتران غير معروفة.

وفي الحالات التي يكون فيها المستخدم بحاجة إلى مستوى أعلى من الحماية، يمكن اللجوء إلى السماعات السلكية، خصوصًا أثناء الاجتماعات أو المحادثات شديدة الحساسية. فإزالة الاتصال اللاسلكي في هذه الحالة تقلل من مساحة الهجوم المرتبطة بالبلوتوث.

وبصورة عامة، لا تعني الثغرات المكتشفة أن استخدام السماعات اللاسلكية أصبح غير آمن، لكنها تذكر بأن الأجهزة الصغيرة المتصلة بالهواتف قد تحتوي على بيانات وصلاحيات أكثر مما يتوقعه المستخدم.

ومع توسع الاعتماد على الأجهزة اللاسلكية في الحياة اليومية، تصبح حماية هذه الأجهزة وتحديثها جزءًا أساسيًا من الأمن الرقمي، لا سيما عندما تكون قادرة على تسجيل الصوت أو الوصول إلى بيانات مرتبطة بالهاتف.

وتبقى الخطوة الأهم هي معرفة طراز الجهاز وإصداره البرمجي والتأكد من حصوله على الإصلاحات الأمنية المتاحة، بدلًا من افتراض أن السماعة مجرد ملحق بسيط لا يمكن أن يشكل مدخلًا محتملًا للهجوم.

ميديا

فضيحة... مسئولون باتحاد الملاكمة يطلبون 81 ألف جنيه من عمرو خالد و90 ألفا من حسام حسن مقابل المشاركة بأولمبياد البحر المتوسط

الخميس 16 يوليو 2026 01:00 م

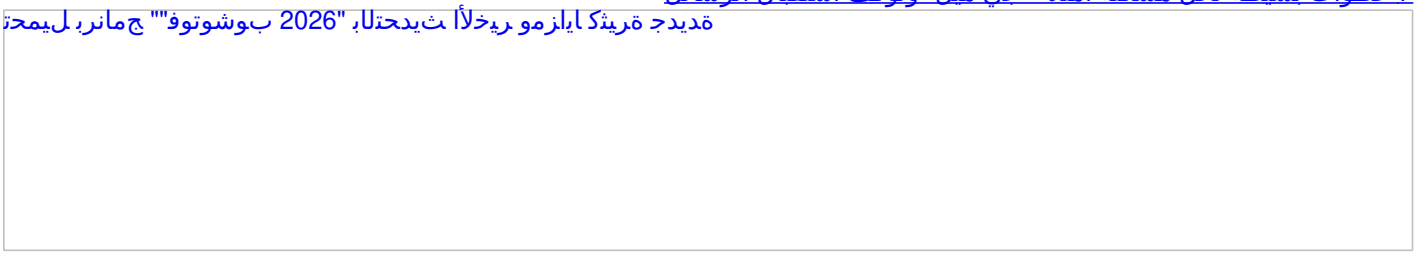
ميديا

خصم 50% على مونوريل شرق النيل يكشف أزمة التسعير وضعف إقبال محدودي الدخل

الجمعة 22 مايو 2026 06:30 م

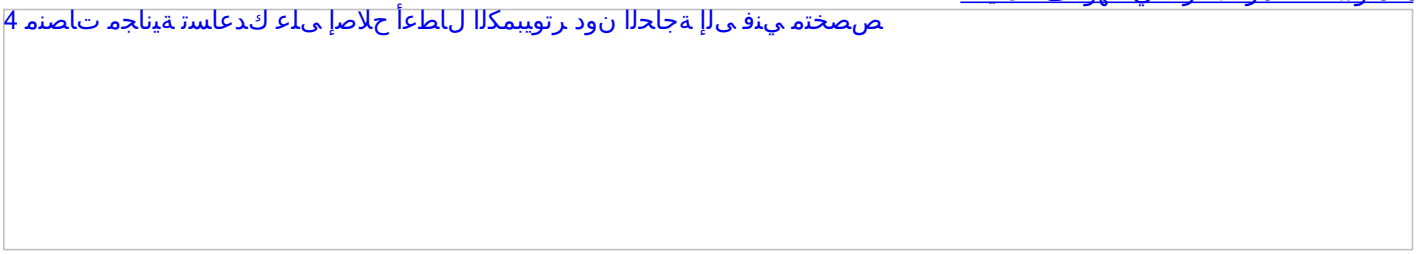
مقالات متعلقة

7 خطوات بسيطة لحل مشكلة امتلاء "جي ميل" وتوقف استقبال الرسائل



تحميل برنامج ""فوتوشوب 2026" بالتحديث الأخير ومزايا كثيرة جديدة

ما متوسط العمر الافتراضي للهواتف الذكية؟



4 منصات مجانية تساعدك على إصلاح أعطال الكمبيوتر دون الحاجة إلى فني متخصص

- التكنولوجيا
- دعوة
- التنمية البشرية
- الأسرة
- ميديا

- الأخبار
- المقالات
- تقارير
- الرياضة
- تراث
- حقوق وحريات

-
-
-
-
-
-

إشترك ادخل بريدك الإلكتروني