ثغرة في سماعات الرأس تتيح التجسس من مسافة 30 مترًا

الاثنين 21 سبتمبر 2026 08:30 م

كشفت دراسة أمنية حديثة عن أسلوب هجوم جديد يستغل المكونات الإلكترونية داخل سماعات الرأس والهواتف والأجهزة المنزلية الذكية لاستخراج الصوت ومعلومات أخرى عن بُعد، عبر حقن إشارات كهرومغناطيسية في الأجهزة المستهدفة.

ويحمل الهجوم اسم "InjectEave"، ويعتمد على استغلال تسربات ضعيفة في المسارات التناظرية للأجهزة، بدلًا من اعتراض البيانات الرقمية أو اختراق الاتصالات اللاسلكية التقليدية.
وأظهرت التجارب التي أجراها باحثون من هونج كونج إمكانية استعادة صوت مفهوم من بعض سماعات الرأس على مسافة تصل إلى 30 مترًا، بما في ذلك في بعض الحالات التي تفصل فيها جدران بين المهاجم والجهاز المستهدف.

وتزداد أهمية النتائج مع اتساع الاعتماد على سماعات الرأس والأجهزة الذكية في المنازل والمكاتب، خصوصًا أن الأسلوب لا يستهدف بالضرورة نظام التشغيل أو التطبيقات المستخدمة على الجهاز، وإنما يستفيد من خصائص في المكونات الإلكترونية نفسها.

هجوم يستغل المكونات التناظرية

قد تبدو فكرة التنصت على جهاز إلكتروني عن بُعد مرتبطة عادة باختراق برمجياته أو اعتراض الاتصالات التي يجريها، لكن InjectEave يعتمد على مسار مختلف تمامًا.

ويستهدف الأسلوب ما يعرف بالقنوات الجانبية الكهرومغناطيسية، وهي ظاهرة تنتج عنها إشارات أو انبعاثات يمكن أن تكشف معلومات عن العمليات التي تجري داخل الأجهزة الإلكترونية. وكانت الأساليب التقليدية تعتمد بصورة أساسية على التقاط هذه الانبعاثات بشكل سلبي، وهو ما يجعلها أكثر صعوبة عندما تكون الإشارات المراد استخراجها ضعيفة.

وتزداد المشكلة في حالة الصوت، لأن الإشارات الصوتية منخفضة التردد تنتج انبعاثات كهرومغناطيسية محدودة، ويمكن أن تختلط بسهولة بالضوضاء والتداخلات الموجودة في البيئة المحيطة.

وهنا يأتي الاختلاف في InjectEave، إذ لا ينتظر المهاجم تسرب الإشارة بصورة طبيعية، وإنما يحاول تحفيز الجهاز على إنتاج تسرب يمكن التقاطه.

ووفقًا للبحث، تُحقن إشارة كهرومغناطيسية في الجهاز بتردد يقع ضمن نطاق يصل إلى 9 ميغاهرتز. وعندما تصل هذه الإشارة إلى بعض المكونات غير الخطية داخل الجهاز، يمكن أن تتفاعل مع الإشارات منخفضة التردد الموجودة بالفعل داخله.

ومن بين المكونات التي يمكن أن تتأثر بهذه العملية مكبرات الصوت، ومحولات الإشارة التناظرية إلى الرقمية، ومحولات الطاقة، وترانزستورات MOSFET المستخدمة في عمليات التبديل.

وتؤدي هذه التفاعلات إلى تعديل الإشارة بطريقة تجعل المعلومات الموجودة في المسار التناظري قابلة للرصد من خلال معدات لاسلكية قريبة، ومن ثم تحليلها بهدف استعادة الصوت أو معلومات أخرى.

11 جهازًا خضعوا للاختبارات

اختبر الباحثون التقنية على مجموعة من المنتجات التجارية المختلفة، في محاولة لمعرفة مدى انتشار الظاهرة بين أنواع متعددة من الأجهزة.

وشملت الاختبارات 11 منتجًا، من بينها سماعات رأس سلكية من سوني، وسماعات أذن من أبل، وسماعات UGreen MAX2، وسماعات Philips TAH2020، وسماعات HP H231R.

كما شملت التجارب هاتف Flyingvoice P23GW VoIP، إلى جانب عدد من الأجهزة المنزلية الذكية، بينها مراوح من Oidire وشاومي، ومصابيح من Jingzao وشاومي.

واستخدم الفريق خلال التجارب جهاز راديو معرفًا بالبرمجيات من نوع USRP B210، بالإضافة إلى هوائيات ومحلل طيف Siglent SSA3075X Plus وحاسوب محمول. وفي بعض التجارب، استعان الباحثون بمكبر لإشارة التردد اللاسلكي بهدف زيادة مدى الهجوم.

وأظهرت النتائج أن معظم الاختبارات الناجحة جرت على مسافات تتجاوز مترين، مع إمكانية استمرار الهجوم في بعض الحالات عند وجود جدران بين مصدر الإشارة والجهاز المستهدف.

وبحسب نتائج الدراسة، تراوحت المسافات المرتبطة بالأجهزة المختلفة في الاختبارات عمومًا بين متر واحد و6 أمتار، إلا أن استخدام مكبر لإشارة التردد اللاسلكي سمح للباحثين باستعادة صوت مفهوم من سماعات الرأس على مسافة وصلت إلى 30 مترًا.

الجدران لا تمنع الإشارة بالكامل

من أبرز الجوانب التي ركزت عليها التجارب اختبار الأجهزة في ظروف أقرب إلى الاستخدام اليومي، بدلًا من الاكتفاء بوضعها على طاولة داخل مختبر.

وشملت السيناريوهات التي اختبرها الباحثون وجود أجهزة مستهدفة داخل حقيبة سفر، وخلف جدار غرفة في فندق، وكذلك داخل أثاث مكتبي.

وتشير هذه التجارب إلى أن وجود حاجز مادي بين الجهاز ومصدر الإشارة لا يعني بالضرورة توقف الهجوم، إذ يمكن للإشارة الكهرومغناطيسية أن تصل إلى بعض المكونات الداخلية وتؤدي إلى الظاهرة التي يعتمد عليها InjectEave.

لكن ذلك لا يعني أن أي شخص يستطيع تنفيذ الهجوم بسهولة باستخدام هاتف أو جهاز لاسلكي عادي. فالسيناريو الذي اختبره الباحثون اعتمد على معدات متخصصة، كما يتطلب معرفة بطريقة استجابة الجهاز المستهدف للإشارات المحقونة.

كذلك لم يكشف الباحثون عن جميع الإعدادات التقنية الدقيقة اللازمة لتطبيق الهجوم، وهو ما يجعل الانتقال من التجربة البحثية إلى تنفيذ عملي واسع النطاق أمرًا أكثر تعقيدًا.

ومع ذلك، فإن النتائج تطرح تساؤلات أمنية بشأن الأجهزة الإلكترونية التي تحتوي على مكونات تناظرية يمكن أن تتفاعل مع الإشارات الكهرومغناطيسية الخارجية.

سماعات الرأس الأكثر حساسية

تبدو سماعات الرأس من أكثر الأجهزة إثارة للقلق في هذا السياق، لأنها قد تكون مرتبطة بمحادثات واجتماعات ومكالمات خاصة.

وفي حالة نجاح الهجوم، لا يحتاج المهاجم بالضرورة إلى اختراق الهاتف المرتبط بالسماعة أو الدخول إلى التطبيق الذي تُجرى من خلاله المكالمة. فالفكرة الأساسية تعتمد على استغلال الإشارات المتسربة من المكونات الإلكترونية نفسها.

وقال يان لونغ، الأستاذ المساعد في جامعة هونغ كونغ للعلوم والتكنولوجيا في غوانغتشو، إن مشروع InjectEave أظهر إمكانية استخدام إشارات التردد اللاسلكي لتحفيز تسرب المعلومات من سماعات الرأس المستخدمة يوميًا، بما يسمح باستعادة الصوت من مسافات بعيدة، وفق ما نقل عنه موقع The Register.

وأوضح لونغ أن الفريق وجد المشكلة في أجهزة من شركات مختلفة، من بينها سوني وHP وفيليبس، إلى جانب منتجات أخرى خضعت للاختبارات.

ولا تقتصر المخاوف على سماعات الرأس، إذ يمكن أن تحمل بعض الأجهزة الذكية الأخرى معلومات يمكن الاستفادة منها حتى لو لم تكن تنقل محادثات صوتية.

الأجهزة المنزلية تكشف أنماط الاستخدام

اختبار المراوح والمصابيح الذكية أضاف جانبًا آخر إلى البحث، إذ أظهر أن التقنية قد تكون قادرة على استخراج معلومات من أجهزة لا تحتوي بالضرورة على محتوى صوتي حساس.

فالإشارات التي تنتجها هذه الأجهزة يمكن أن تكشف أنماطًا مرتبطة بالتشغيل أو التحكم أو استهلاك الطاقة. ومن خلال تحليل هذه البيانات، قد يصبح من الممكن استنتاج أوقات استخدام بعض الأجهزة داخل المنزل أو المكتب.

وتكمن خطورة هذا النوع من المعلومات في أنها قد تقدم صورة عن النشاط داخل المكان المستهدف، حتى من دون الحصول على تسجيل صوتي أو الوصول المباشر إلى شبكة الأجهزة.

وفي بيئة مكتبية مثلًا، يمكن أن تكشف أنماط تشغيل بعض الأجهزة عن أوقات وجود أشخاص أو نشاط داخل مساحة معينة، بينما قد تقدم في المنزل مؤشرات حول استخدام أجهزة محددة خلال اليوم.

ولا يعني ذلك أن كل جهاز ذكي معرض بالضرورة لاستخراج هذه المعلومات بنفس الدرجة، فنتائج الهجوم تختلف بحسب تصميم الجهاز ومكوناته وطريقة استجابتها للإشارات الكهرومغناطيسية.

التشفير وحده لا يكفي

تكشف الدراسة أيضًا عن تحدٍ مهم أمام وسائل الحماية التقليدية، إذ إن التشفير لا يعالج بالضرورة هذا النوع من التسرب.

فالتشفير يحمي البيانات الرقمية أثناء تخزينها أو نقلها، بينما يعتمد InjectEave على ظاهرة تحدث في المسار التناظري داخل الجهاز قبل أن تكون المشكلة مرتبطة بتشفير البيانات.

ولهذا السبب، يرى الباحثون أن إجراءات مثل تشفير الاتصالات أو إخفاء البيانات والعشوائية لا تمنع مصدر التسرب الذي يستغله الهجوم.

ويختلف الأمر عندما يتعلق الأمر بالحماية المادية للمكونات. فالدروع الكهرومغناطيسية، ومرشحات الإشارات، واستخدام الأسلاك المزدوجة المجدولة، يمكن أن تقلل كمية طاقة التردد اللاسلكي التي تصل إلى المكونات الحساسة.

لكن هذه الإجراءات قد تزيد صعوبة تنفيذ الهجوم بدلًا من القضاء عليه بصورة مطلقة.

وتشير نتائج البحث، التي قدمها الفريق تحت عنوان «الحقن والتسريب: الحث النشط لتسريب القناة الجانبية باستخدام الحقن الكهرومغناطيسي واللاخطية في الأجهزة» خلال مؤتمر USENIX Security 2026، إلى أن أمن الأجهزة الإلكترونية لا يتعلق فقط بالبرمجيات والاتصالات المشفرة.

فالعتاد نفسه قد يمثل مسارًا لتسريب المعلومات، حتى عندما تكون البيانات محمية بالوسائل الرقمية المعتادة. ولذلك يفتح InjectEave بابًا جديدًا أمام أبحاث أمن الأجهزة، خصوصًا مع انتشار سماعات الرأس والأجهزة المنزلية المتصلة، والحاجة إلى تطوير وسائل حماية تبدأ من تصميم المكونات الإلكترونية نفسها ولا تقتصر على البرمجيات.