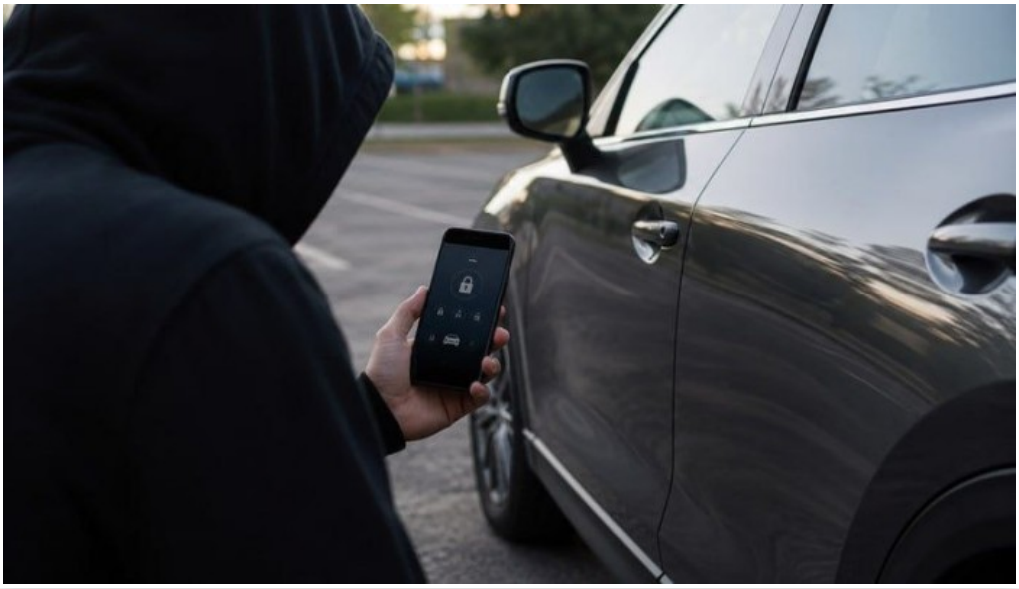
ثغرة بلوتوث تهدد ملايين السيارات اختراق عن بُعد يفتح الأبواب ويعطل الحماية الأمنية في ثوانٍ



الأربعاء 29 يوليو 2026 10:30 م

أثار اكتشاف ثغرة أمنية خطيرة في أحد أشهر أنظمة مكافحة سرقة السيارات حالة من القلق بين خبراء الأمن السيبراني، بعدما كشف باحثون أن الخلل قد يتيح للمهاجمين التحكم في سيارات عن بُعد عبر تقنية البلوتوث، بما يشمل فتح الأبواب وتشغيل بعض الوظائف الحيوية دون الحاجة إلى كسر الزجاج أو استخدام مفاتيح السيارة

وتشير التقديرات إلى أن نحو 2.2 مليون سيارة قد تكون معرضة لهذا الخطر، بعد تزويدها بأنظمة الحماية KARR وSWDS المصنعة بواسطة شركة Acrisure، والتي جرى تركيبها في آلاف السيارات المباعة عبر وكلاء السيارات، باعتبارها أنظمة إضافية لمكافحة السرقة وتتبع المركبات

ملايين السيارات قد تكون معرضة للخطر

ووفقًا لدراسة أجراها باحثون من جامعة كاليفورنيا في سان دييغو، فإن السيارات المتأثرة بيعت منذ عام 2017 عبر عدد من وكلاء السيارات في جنوب ولاية كاليفورنيا، إلا أن انتشار سوق السيارات المستعملة يعني أن هذه المركبات انتقلت إلى ولايات أمريكية أخرى، بل وربما وصلت إلى دول مختلفة حول العالم، من بينها اليابان

ويحذر الباحثون من أن حجم المشكلة قد يكون أكبر من المتوقع، خصوصًا مع انتقال ملكية السيارات بين المستخدمين دون إزالة أنظمة الحماية المثبتة داخلها

كيف يعل نظام الحماية؟

تعتمد أنظمة KARR وSWDS على جهاز إلكتروني يتم تثبيته داخل السيارة، ويرتبط بتطبيق على الهاتف الذكي عبر تقنية البلوتوث، ويمنح مالك السيارة مجموعة من الوظائف، من بينها:

قفل وفتح أبواب السيارة

تشغيل بوق التنبيه

تشغيل وإطفاء أضواء المصابيح الأمامية

تعطيل تشغيل المحرك لمنع السرقة في بعض الحالات

إدارة بعض وظائف الأمان عن بُعد

وكان الهدف من هذه الأنظمة هو توفير طبقة إضافية من الحماية ضد السرقة، إلا أن الباحثين اكتشفوا أن تصميمها الأمني يحتوي على نقطة ضعف خطيرة قد تحولها من وسيلة حماية إلى أداة يمكن استغلالها ضد مالكي السيارات

أين تكمن الثغرة الأمنية؟

بحسب الدراسة، فإن جميع الأجهزة تعتمد على مفتاح أمني موحد للتحقق من الاتصال عبر البلوتوث.

ويعني ذلك أنه بمجرد تمكن المهاجم من معرفة هذا المفتاح أو كسره، يصبح بإمكانه التواصل مع جميع الأجهزة من النوع نفسه، وهو ما يسمح بإرسال أوامر مباشرة للنظام.

ويرى خبراء الأمن السيبراني أن استخدام مفتاح موحد لملايين الأجهزة يعد من أخطر الأخطاء الأمنية في تصميم الأنظمة الإلكترونية، لأنه يجعل اختراق جهاز واحد كافيًا لتهديد عدد هائل من السيارات.

فتح السيارة دون لمسها

أوضح الباحثون أن اللصوص لن يكونوا بحاجة بعد الآن إلى كسر نوافذ السيارات أو استخدام أدوات تقليدية لسرقتها.

فبمجرد الاقتراب من السيارة، يمكن للمهاجم الاتصال بالنظام عبر البلوتوث وإرسال أوامر لفتح الأبواب، وهو ما قد يختصر عملية السرقة إلى ثوانٍ معدودة.

كما يستطيع النظام تنفيذ أوامر أخرى، مثل تشغيل البوق أو التحكم في الإضاءة، الأمر الذي يؤكد امتلاك الجهاز صلاحيات واسعة داخل السيارة.

قاعدة بيانات مكشوفة للعامة

ولم تتوقف المفاجآت عند الثغرة الأمنية فقط، إذ كشف الباحثون عن العثور على قاعدة بيانات متاحة للعامة تضم معلومات خاصة بالمركبات المزودة بهذه الأنظمة.

ويرى متخصصون أن وجود هذه البيانات على الإنترنت قد يسهل على المهاجمين تحديد السيارات المستهدفة، ويزيد من احتمالات استغلال الثغرة على نطاق واسع.

حتى غير المشتركين معرضون للخطر

ومن أكثر النتائج إثارة للقلق أن الخطر لا يقتصر على العملاء الذين يستخدمون التطبيق الإلكتروني.

فالعديد من السيارات لا تزال تحتوي على جهاز KARR مثبتًا داخلها، حتى وإن لم يقم مالكها بتفعيل الخدمة أو الاشتراك في التطبيق.

وبذلك يبقى الجهاز محتفظًا بكامل صلاحياته داخل السيارة، بما في ذلك التحكم في الأقفال وأنظمة التشغيل والإضاءة والتنبيه، وهو ما يجعل المركبة معرضة للهجوم رغم عدم استخدام الخدمة فعليًا.

إزالة الجهاز ليست مهمة سهلة

وأشار الباحثون إلى أن التخلص من الجهاز ليس أمرًا بسيطًا، إذ يتطلب فك أجزاء من لوحة القيادة وقطع وإعادة توصيل أسلاك كهربائية مرتبطة مباشرة بحاسوب السيارة ونظام الإشعال.

وأوضح الباحث ييبو وي، طالب الدكتوراه في علوم الحاسوب بجامعة كاليفورنيا في سان دييغو، أن إزالة النظام تحتاج إلى تدخل فني متخصص بسبب اندماجه العميق مع الأنظمة الإلكترونية للمركبة، ما يجعل كثيرًا من المالكين غير قادرين على التخلص منه بأنفسهم.

سيارات من علامات تجارية متعددة

وبحسب الدراسة، فإن السيارات التي رُكبت بها هذه الأنظمة بيعت عبر وكلاء لعدد من العلامات التجارية العالمية، من بينها:

هوندا.

تويوتا.

مازدا

فورد

جيب

ويمكن التعرف على بعض السيارات المتأثرة من خلال وجود ملصق يحمل اسم KARR-SWDS على نافذة جهة السائق، بينما يوجد الجهاز الإلكتروني عادة أسفل لوحة القيادة

الشركة تعلن إصدار تحديث أمني

من جانبها، أكدت شركة KARR أن الثغرة تؤثر فقط في السيارات المزودة بمكونات محددة تعتمد على تقنية البلوتوث، مشيرة إلى أنها أطلقت تحديثًا جديدًا للبرامج الثابتة (Firmware) لمعالجة المشكلة وسد الثغرة الأمنية

ولم توضح الشركة عدد السيارات التي تلقت التحديث بالفعل، أو ما إذا كان جميع المستخدمين قد أصبحوا محميين من الاستغلال المحتمل

دعوات لتحديث الأنظمة سريعًا

ويرى خبراء الأمن السيبراني أن هذه الواقعة تعكس أهمية تصميم أنظمة حماية السيارات وفق معايير تشفير أكثر صرامة، خاصة مع الاعتماد المتزايد على الاتصالات اللاسلكية والتطبيقات الذكية

كما ينصح المختصون مالكي السيارات المزودة بأنظمة حماية إضافية بالتواصل مع الوكلاء أو مراكز الصيانة المعتمدة للتأكد من تثبيت آخر التحديثات الأمنية، والتأكد من عدم وجود ثغرات قد تعرض سياراتهم للاختراق أو السرقة

ويؤكد الخبراء أن السيارات الحديثة أصبحت تعتمد بشكل متزايد على البرمجيات والاتصالات الرقمية، الأمر الذي يجعل الأمن السيبراني جزءًا أساسيًا من سلامة المركبات، تمامًا مثل أنظمة المكابح والوسائد الهوائية، ويستدعي تحديثات مستمرة لمواجهة التهديدات الإلكترونية المتزايدة