Millionen Autos lassen sich einfach per Funk öffnen

Bild: Houston Police Department

Autodiebe stehlen in Texas einen Jeep.

Sicherheitsforscher haben eine Schwachstelle in den Funkschlüsseln nahezu aller Auto-Marken des VW-Konzerns entdeckt. Ihren Erkenntnissen zufolge gibt es spezielle Masterkeys, die sie aus dem Chip eines Schließsystems extrahieren konnten. Das führt dazu, dass sie Funktionen eines Schlüssels grundsätzlich reproduzieren können. Durch das einmalige Auslesen des fahrzeugspezifischen Codes, etwa wenn der Fahrer seinen Wagen abschließt, kann dann innerhalb kürzester Zeit ein elektronischer Nachschlüssel angefertigt werden. Der gesamte Vorgang dauert etwa eine Sekunde.

Die Diebe können dann das Auto öffnen, die Alarmanlage ausschalten und in das Auto eindringen, ohne Spuren zu hinterlassen. Der Fahrzeugeigentümer bemerkt den Einbruch nicht, er stellt nur fest, dass sein Auto nicht beim ersten Knopfdruck öffnet. Der VW-Konzern hat eingeräumt, dass zahlreiche Modelle der vergangenen 15 Jahre nicht auf dem aktuellen Sicherheitsniveau sind. Einen Schutz für Besitzer älterer Autos gibt es nicht, außer sie nutzen nur den mechanischen Schlüssel. Fahrzeuge aus den aktuellen Modellbaureihen wie der aktuelle Golf, Tiguan, Touran oder Passat seien nicht betroffen, so ein Sprecher des Konzerns. Allerdings gelang es den Forschern auch, die Türen eines Audis aus der 2016er Baureihe zu öffnen – direkt im Autohaus.

Für ein zweites Schlüsselsystem, das von verschiedenen großen Herstellern eingesetzt wird, konnten die Sicherheitsforscher nachweisen, dass es sich ebenso einfach öffnen lässt. Daher muss man davon ausgehen, dass der überwiegende Teil aller Fahrzeugmarken betroffen ist.

Erst vor Kurzem waren in Texas zwei Autodiebe festgenommen worden, die mit einem Laptop bewaffnet in sechs Monaten über hundert Fahrzeuge der Marken Jeep und Dodge entwendet und über die Grenze nach Mexiko gebracht hatten. Die Diebe sollen in den Wagen eingebrochen sein und knackten dann mit einer Hacking-Software die Wegfahrsperre, um das Auto zu starten. Dabei missbrauchten sie mutmaßlich die Service-Schnittstelle OBD-II oder einen USB-Port des Entertainment-Systems. *(Kai Rüsberg/fab@ct.de)*

Informationen zu den betroffenen Autos: ct.de/yzj1

Microsoft setzt aus Versehen Secure Boot schachmatt

Mit dem Anniversary Update für Windows 10 hat Microsoft eine Secure Boot Policy in den eigenen Bootloader eingebaut, die es einem Administrator erlaubt, den Secure-Boot-Schutz eines Systems zu umgehen. Dieser sollte eigentlich dafür sorgen, dass nur Komponenten geladen werden, die von Microsoft signiert sind. Durch die Policy können Nutzer aber beliebige eigene Betriebssystem-Komponenten booten. Dieser Code muss lediglich irgendwie signiert sein – zum Beispiel mit einer selbst erstellten Signatur. Bei der Policy handelt es sich wohl um eine vergessene Debug-Funktion.

Da die von Microsoft signierte und dadurch gültige Policy mittlerweile im Netz kursiert, kann ein Angreifer, sofern er Administratorrechte besitzt, Secure Boot deaktivieren. Normalerweise müsste er dafür vor dem Rechner sitzen. Bei Hardware mit erzwungenem Secure Boot (etwa Surface Tablets und Windows Phones) hat das den Effekt, dass Besitzer Secure Boot nun doch ausschalten können. Microsoft hat bereits zwei Updates veröffentlicht, die das Problem angehen sollen – bisher allerdings ohne Erfolg. Die Patches erschweren den Angriff höchstens ein bisschen. Es ist zu erwarten, dass Microsoft die anstößige Policy mit einem weiteren Update komplett entfernt und die Lücke endgültig stopft. *(fab@ct.de)*

WPAD nach 20 Jahren immer noch gefährlich

Das Web Proxy Auto Discovery Protocol (WPAD) dient zur automatischen Konfiguration eines Proxys auf dem Endgerät und ist schon lange als Schwachstelle bekannt. Seit Netscape 2.0 aus dem Jahr 1996 ist WPAD in fast allen Betriebssystemen verankert. Es kann für Angriffe missbraucht werden, da Router die Anfragen von Clients nach der Konfigurationsdatei wpad.dat mitunter ins Internet weiterleiten.

Auf der Black-Hat-Konferenz in Las Vegas hat ein Sicherheitsforscher gezeigt, wie sich beliebige Endgeräte per WPAD mit einer bösartigen Proxy-Konfiguration versorgen lassen – ohne Zutun des Anwenders und unabhängig vom Betriebssystem. Das Problem basiert darauf, wie Endgeräte nach der URL suchen, von der sie die WPAD-Konfigurationsdatei herunterladen möchten. Kontrolliert ein Angreifer die Top-Level-Domain (TLD) der angefragten URL, kann der Angreifer prinzipiell alle Clients manipulieren, die zur betreffenden Suchdomain gehören.

In Deutschland betrifft dies insbesondere Anwender, die mittels einer Fritzbox ins Internet gehen. Die Geräte geben die Suchdomain fritz.box vor. Wann die TLD .box aktiv wird, steht noch nicht fest. AVM sagte gegenüber c’t, man versuche die TLD sobald wie möglich zu registrieren. Ginge diese an jemand anderen, könnte er alle hinter einer Fritzbox betriebenen Endgeräte automatisch mit einer Proxy-Einstellung konfigurieren. *(Uli Ries/fab@ct.de)*

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover