BMW, MERCEDES, KIA, PORSCHE

Sicherheitsforscher hacken etliche Autohersteller

Forschern ist es gelungen die API-Endpunkte etlicher Autohersteller wie BMW oder Kia zu hacken - von der Konten- bis zur Autoübernahme war alles möglich.

Von Moritz Tremmel

3. Januar 2023, 15:54 Uhr

(Bild: Mylène/Pixabay [https://pixabay.com/de/photos/bmw-hintergrund-regentropfen-4612551/])

Auch der Autohersteller BMW ist von den entdeckten Sicherheitslücken betroffen.

Über die API-Endpunkte der Telemetriesysteme etlicher Autohersteller ist es dem Sicherheitsforscher Sam Curry und seinen Freunden gelungen, Funktionen in Autos zu übernehmen und zu steuern. Auf die Idee zu den Hacks kamen sie auf einer Reise zu einer Cybersicherheitskonferenz im vergangenen Herbst.

Während sie die Universität Maryland besuchten, bemerkten sie die E-Scooter, die überall auf dem Gelände herumstanden. Also beschlossen sie, sich die App der Scooter anzusehen. *"Zu unserer Überraschung bewirkten unsere Aktionen, dass sich die Hupen und Scheinwerfer aller Roller 15 Minuten lang einschalteten",* erklärte Curry [https://samcurry.net/web-hackers-vs-the-auto-industry/] .

Als sich alles wieder beruhigt hatte und die Studenten weiterschlafen konnten, schickten die Sicherheitsforscher einen Bericht an den E-Scooter-Hersteller. *"Wir überlegten eine Weile und stellten dann fest, dass nahezu jedes Auto, das in den letzten fünf Jahren hergestellt wurde, eine fast identische Funktion hat",* sagte Curry.

Vom E-Scooter-Hack zum Auto-Hack

Wäre ein Angreifer in der Lage, Schwachstellen in den API-Endpunkten zu finden, die von Fahrzeugtelemetriesystemen verwendet werden, könnte er hupen, blinken, die Fahrzeuge ver- und entriegeln oder starten und stoppen - und das alles aus der Ferne. Auch eine Verfolgung der Fahrzeuge sei möglich.

Die Sicherheitsforscher starteten einen Chatgruppe und machten sich an die Arbeit, entsprechende Schwachstellen zu finden - und wurden fündig. Sie fanden umfangreiche und weitreichende Sicherheitslücken bei vielen namhaften Herstellern, darunter Mercedes-Benz, BMW, Porsche, Jaguar, Ford, Hyundai, Honda, Kia und Ferrari.

Alle BMW-Konten gehören uns

Mit Fuzzing und Ausprobieren entdeckten die Sicherheitsforscher API-Endpunkte von BMW. Eine erste Sicherheitslücke ermöglichte ihnen, alle BMW-Benutzerkonten abzufragen, indem sie ein Sternchen im Benutzerfeld an den API-Endpunkt sendeten. Bei einer weiteren Sicherheitslücke konnten sie über die API die TOTP-Codes für eine Zwei-Faktor-Authentifizierung (2FA) [https://www.golem.de/news/2fa-wie-sicher-sind-totp-fido-sms-und-push-apps-2206-166287-3.html] abfragen.

Anschließend testeten sie die Passwort-zurücksetzen-Funktion [https://www.golem.de/news/sicherheit-wie-sich-passwort-zuruecksetzen-missbrauchen-laesst-1902-139573.html] mit einem Beispielkonto. Auf die Frage nach dem 2FA-Code verwendeten sie die zuvor verwendete Sicherheitslücke und gaben den so erlangten TOTP-Code an. Das funktionierte tatsächlich: Sie konnten das Beispielkonto und beliebige andere Konten von BMW-Angestellten oder -Partnern zurücksetzen - und damit übernehmen.

Um die Auswirkungen der Schwachstelle zu demonstrieren, suchten die Sicherheitsforscher nach BMWs Händlerportal, das von BMW- und Rolls-Royce-Händlern genutzt wird. *"Nach dem Einloggen stellten wir fest, dass das von uns übernommene Demokonto mit einem echten Händler verbunden war und wir auf alle Funktionen zugreifen konnten, auf die auch die Händler selbst Zugriff hatten"*, schrieb Curry. Darunter waren beispielsweise Verkaufsunterlagen der Fahrzeuge.

"Mit unseren Zugriffsrechten hätten wir eine Vielzahl von Funktionen für BMW- und Rolls-Royce-Kundenkonten und Kundenfahrzeuge nutzen können. Wir brachen die Tests an diesem Punkt ab und meldeten die Sicherheitslücke", erklärte der Sicherheitsforscher. Doch das waren noch längst nicht alle Sicherheitslücken, die die Forscher entdecken konnten. So konnten sie im Falle von Kia gar die Autos sperren, entriegeln oder starten und stoppen.

Nächste Seite: Von der vermeintlichen Kfz-Werkstatt zum Mercedes-Angestellten [/news/bmw-mercedes-kia-porsche-sicherheitsforscher-hacken-etliche-autohersteller-2301-170901-2.html]

1 2

Themenseiten:

Auto, 2-FA, BMW, Datensicherheit, E-Scooter, Ford, Git, Hacker, Honda, Hyundai, Jaguar Land Rover, Kia