Mercedes-Benz me App gehackt: 28 Zugangsdaten und OAuth-Secrets öffentlich im Quellcode

26.10.2026, 06:00 | IT, New Media & Software

Pressemitteilung von: *CVD*



BuriLabs / Skylasec

Gaildorf, 27. Oktober 2026 — Wer die Mercedes me App auf seinem Smartphone nutzt, vertraut Mercedes-Benz seine Fahrzeugdaten, Zahlungsinformationen, seinen Standort und seinen digitalen Fahrzeugschlüssel an. Was die wenigsten Nutzer wissen: Im Quellcode genau dieser App lagen 28 Zugangsdaten offen — darunter OAuth-Secrets für die Connected-Vehicle-Plattform, mit denen sich die offizielle App gegenüber dem Server vollständig imitieren lässt.

Ein deutsches Sicherheitsforschungsunternehmen hat diese und 25 weitere Schwachstellen durch legale statische Analyse der öffentlich im Google Play Store verfügbaren App gefunden. Es wurde kein System angegriffen, kein Passwort ausprobiert, kein Server kontaktiert. Trotzdem dauerte es 120 Tage — und die Lücken sind bis heute nicht nachweislich geschlossen.

Wie alles begann

Am 30. Juni 2026 meldete BuriLabs neun Schwachstellen an die Product-Security-Abteilung von Mercedes-Benz. Vier Wochen vergingen, bis Mercedes erstmals antwortete. Am 4. August erteilte Mercedes eine Safe-Harbor-Zusage. Am nächsten Tag: vollständiger technischer Bericht mit PoC-Skripten und 128 IDOR-Endpunkten. Antwort: „Evaluierung läuft." Dann wurde es still.

Was die Schwachstellen für Nutzer bedeuten

5 Critical (CVSS bis 9.1): OAuth-Credentials für die ONE API — die Schnittstelle, über die Fahrzeuge gesteuert, entriegelt und lokalisiert werden. Certificate Pinning bewusst deaktiviert — in öffentlichem WLAN könnte ein Angreifer den gesamten Datenverkehr mitlesen. Fleet-Payment-Credentials. 14 interne Staging-Domains erreichbar.

8 High: Push-Notification-Schlüssel (beliebige Nachrichten an alle Nutzer), App-Distributions-Token, HERE-Maps-Secret, SharedUserId „com.daimler" — eine kompromittierte App öffnet alle anderen. Keine Root-Erkennung. ROPC Password Grant.

Dazu: ByteDance/TikTok-SDK in einer europäischen Fahrzeug-App.

120 Tage — eine Chronologie

Im September fragte Mercedes nach dem Status eines einzigen Befunds — ausgerechnet des am wenigsten kritischen. Die 27 übrigen blieben unkommentiert. BSI, BaFin und ENISA wurden parallel informiert. Im Oktober: Arbeitsgespräch mit Group CISO und Entwicklungsleitung. Ergebnis: Keine Einigung. Stattdessen der Verweis auf die konzerneigene Bug-Bounty-Plattform — bei 26 Befunden mit Cross-App-Abhängigkeiten weder skalierbar noch zweckmäßig.

Eine Branche im Widerspruch

Mercedes investiert Milliarden in Connected Services. Die me App ist das zentrale Digitalprodukt für Millionen Kunden. Dass Certificate Pinning bewusst deaktiviert und produktive Zugangsdaten im öffentlichen Quellcode belassen werden, steht im Widerspruch zum Qualitätsanspruch. Die Veröffentlichung nach 120 Tagen entspricht CERT/CC-Richtlinie und NIS-2.

Vollständiger Bericht: https://skylasec.net/news/mercedes-security-disclosure-2026/

Burilabs

Christoph-Wagner-Straße. 25
74405 Gaildorf
Deutschland

BurakYilmaz

01728170788

burak.yilmaz@brlabs.dev

skylasec.net/news/mercedes-security-disclosure-2026/

Portrait

BuriLabs / Skylasec ist ein deutsches Forschungsunternehmen im Bereich Cybersicherheit, Software-Sicherheitsanalyse und standardkonforme Schwachstellenkoordination (CVD).

News-ID: 1328021 • Views: 429 (Stand: 21.11.2026)

Link zur Pressemitteilung:
https://www.openpr.de/news/1328021/Mercedes-Benz-me-App-gehackt-28-Zugangsdaten-und-OAuth-Secrets-oeffentlich-im-Quellcode.html