Koordinierte Offenlegung, Abschlussbericht

OMV App Android (com.hastobe.omv)

OMV AG, Wien, Österreich (Wiener Börse: ATX OMV)

STILLE · FALL GESCHLOSSEN UND VERÖFFENTLICHT AM 26. SEPTEMBER 2026, AM ANGEGEBENEN EMBARGO-DATUM, SECHS NACHRICHTEN, KEINE ANTWORT

Ziel	OMV, ein an der Wiener Börse notierter österreichischer Energiekonzern
Package	com.hastobe.omv, Version 3.5.5 (versionCode 332418)
Betreiber	OMV AG, Wien, Österreich
Erstmeldung	2026-06-26
Angegebenes Embargo	2026-09-26, dem Betreiber direkt in der Erstmeldung mitgeteilt
Bericht veröffentlicht	2026-09-26, zum angegebenen Datum
Behörden	Österreichische Datenschutzbehörde (DSB), Finanzmarktaufsicht (FMA)
Ausgehende Nachrichten gesamt	6 über 66 Tage, an datenschutz@omv.com (dauerhaft unzustellbar) und security@omv.com (zugestellt).
Eingehende Antworten	0. Keine einzige Antwort jeglicher Art wurde je empfangen.

rfi.irfos@gmail.com • rfi-irfos.com
ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

Am 26. Juni 2026 meldete RFI-IRFOS, dass die OMV-App keine res/xml/network_security_config.xml enthält, was auf dem verwendeten targetSdk bedeutet, dass unverschlüsseltes HTTP an beliebige Server erlaubt ist. Gleichzeitig sind ein Firebase-API-Schlüssel und ein Google-Directions-API-Schlüssel im Produktiv-Binary im Klartext auslesbar, und der zugehörige Google-Cloud-Storage-Bucket ist direkt adressierbar. Bei einem ATX-gelisteten Energiekonzern ist das Fehlen einer Network Security Configuration eine messbare Abweichung vom Stand der Technik. Dieser Befund korrigiert sich auf HIGH/8.6 unter CVSS v4.0.

Ein zweiter Befund: das Facebook-App-Events-SDK, einschließlich Automatic App Matching und Facebook CloudBridge, sammelt Nutzerinteraktionen in der App und sendet sie an Meta, Tankstellensuchen, App-Öffnungen, Filterverhalten nach Kraftstoffart und Preis, Karteninteraktionen und Routenplanungen zu bestimmten Stationen. Facebook CloudBridge stellt zusätzlich eine serverseitige Weiterleitung bereit, die browserbasierte Tracking-Blockierung vollständig umgeht, eine doppelte Datenübermittlungspipeline. OMV-Kunden, die die App zum Finden von Tankstellen, zum Prüfen von Kraftstoffpreisen oder zum Einlösen von Bonuspunkten nutzen, übermitteln damit unwissentlich ihr Verhalten an Meta. Dieser Befund korrigiert sich auf MEDIUM/6.9.

Ein dritter Befund, ebenfalls MEDIUM: FirebaseInitProvider (initOrder=100) und FacebookInitProvider initialisieren beide, bevor irgendein Einwilligungssignal vorliegt, sodass Verhaltensdaten bereits beim App-Start erfasst werden, unabhängig von jeder Nutzerentscheidung. Positiv zu vermerken: die OMV-App verwendet Apollo GraphQL für die Backend-Kommunikation, eine moderne, typsichere API-Architektur, die präzise Datenabfragen ermöglicht und Over-Fetching reduziert, ein Zeichen technischer Reife in der Backend-Architektur.

Sechs Nachrichten wurden über 66 Tage gesendet, an datenschutz@omv.com, das bei allen sechs Versuchen dauerhaft unzustellbar blieb, und an security@omv.com, das zugestellt wurde. Die österreichische Datenschutzbehörde und die Finanzmarktaufsicht waren durchgehend in BCC informiert. Keine einzige Antwort, weder automatisiert noch menschlich, wurde je empfangen. Das 90-Tage-Embargo, dem Betreiber direkt in der Erstmeldung mitgeteilt, läuft heute ab. Dieser Bericht und die begleitende Abschlussmitteilung veröffentlichen zum angegebenen Datum.

Scope: Root-Level-Code-Analyse der produktiven OMV-Android-Anwendung (com.hastobe.omv, Version 3.5.5), direkt von einem Produktivgerät mit Android 16 extrahiert und am 26. Juni 2026 untersucht. Es wurde kein Konto angelegt, und es fand keine Interaktion mit der Backend-Infrastruktur von Facebook/Meta oder Firebase statt.

Disposition

Drei Befunde wurden am 26. Juni 2026 gemeldet, unter CVSS v4.0 neu bewertet. Das Fehlen einer Network Security Configuration in Kombination mit zwei hardcodierten API-Schlüsseln korrigiert sich auf HIGH. Das Facebook-App-Events-SDK mit CloudBridge auf Tankstellen-Transaktionsdaten und die doppelte Pre-Consent-Initialisierung von Firebase und Facebook korrigieren sich beide auf MEDIUM. Sechs Nachrichten wurden über 66 Tage gesendet. Keine einzige Antwort wurde je empfangen.

ID	Severity	Title
B2	HIGH	Keine Network Security Configuration, zwei API-Schlüssel hardcodiert
B1	MEDIUM	Facebook App Events und CloudBridge auf Tankstellen-Transaktionsdaten
B3	MEDIUM	Doppelte Pre-Consent-Initialisierung von Firebase und Facebook

Was die OMV-App richtig macht

Die OMV-App verwendet Apollo GraphQL für die Backend-Kommunikation, eine moderne, typsichere API-Architektur, die präzise Datenabfragen ermöglicht und Over-Fetching reduziert. Das zeigt technische Reife in der Backend-Architektur.

Sechs Nachrichten, keine Antwort

Alle sechs Nachrichten dieses Falls wurden über 66 Tage gesendet. datenschutz@omv.com blieb bei allen sechs Versuchen dauerhaft unzustellbar; security@omv.com wurde zugestellt. Die österreichische Datenschutzbehörde und die Finanzmarktaufsicht waren durchgehend in BCC informiert. Keine einzige Antwort, weder automatisiert noch menschlich, wurde je empfangen.

Findings

B2: Keine Network Security Configuration, zwei API-Schlüssel hardcodiert

HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 8.6.

res/xml/network_security_config.xml ist nicht vorhanden, was bei targetSdk 35 bedeutet, dass unverschlüsseltes HTTP an beliebige Server standardmäßig erlaubt ist. Zusätzlich sind ein Firebase-API-Schlüssel und ein Google-Directions-API-Schlüssel im Produktiv-Binary hardcodiert, und der zugehörige Google-Cloud-Storage-Bucket ist direkt adressierbar.

```
google_api_key (Firebase) = AIzaSyDmtxs6OX4cWj6I8KclnuqeHQh2AmVickM
google_directions_api_key = AIzaSyAgq07sxKc52qD9subkgCgeCsS2hPQng1M
google_storage_bucket = hastobe-omv.appspot.com
```

Impact: Ohne Network Security Configuration kann die App unverschlüsseltes HTTP an beliebige Server senden, und beide API-Schlüssel sind für jeden auslesbar, der die APK herunterlädt, was unauthentifizierte Aufrufe gegen das Firebase-Projektkontingent ermöglicht.

Fix: Eine Network Security Configuration mit cleartextTrafficPermitted=false implementieren und beide API-Schlüssel nach Package-Name und Zertifikat einschränken. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

B1: Facebook App Events und CloudBridge auf Tankstellen-Transaktionsdaten

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9.

Das Facebook-App-Events-SDK, einschließlich Automatic App Matching (com/facebook/appevents/aam/) und Facebook CloudBridge (com/facebook/appevents/cloudbridge/), erfasst Tankstellensuchen, App-Öffnungen, Filterverhalten nach Kraftstoffart und Preis, Karteninteraktionen und Routenplanungen zu bestimmten Stationen und sendet diese an Meta. CloudBridge stellt zusätzlich eine serverseitige Weiterleitung bereit, die browserbasierte Tracking-Blockierung umgeht.

```
com/facebook/appevents/ (Facebook App Events SDK)
com/facebook/appevents/aam/ (Automatic App Matching)
com/facebook/appevents/cloudbridge/ (serverseitige Ereignisweiterleitung)
com/facebook/internal/FacebookInitProvider (Pre-Consent-Autostart)
```

Impact: OMV-Kunden, die die App zum Finden von Tankstellen, zum Prüfen von Kraftstoffpreisen oder zum Einlösen von Bonuspunkten nutzen, übermitteln ihr Verhalten unwissentlich an Meta, über eine doppelte, browserblocker-resistente Übermittlungspipeline.

Fix: Das Facebook-App-Events-SDK und CloudBridge entfernen oder hinter eine explizite Einwilligung stellen. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

B3: Doppelte Pre-Consent-Initialisierung von Firebase und Facebook

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:L/SC:N/SI:N/SA:N, 6.9.

FirebaseInitProvider (initOrder=100) und FacebookInitProvider initialisieren beide automatisch beim App-Start, bevor irgendein Einwilligungssignal vorliegt.

Impact: Verhaltensdaten werden bereits beim App-Start erfasst, unabhängig von jeder Nutzerentscheidung, ein direkter Verstoß gegen das Erfordernis, dass Einwilligung der Verarbeitung vorausgehen muss.

Fix: Beide Provider hinter einen Consent-Mechanismus stellen. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

Datenschutz, Artikel für Artikel

Die Befunde ordnen sich einer kleinen, spezifischen Gruppe von DSGVO-Bestimmungen zu, hier gesammelt statt über die Befunde verstreut.

Artikel	Befund	Grundlage
Art. 32	B2	Keine Network Security Configuration, zwei API-Schlüssel hardcodiert.
Art. 6, Art. 7, Art. 13	B1	Facebook App Events und CloudBridge auf Tankstellen-Transaktionsdaten.
Art. 7	B3	Doppelte Pre-Consent-Initialisierung von Firebase und Facebook.

RFI-IRFOS rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria CVSS v4.0 ist die Scoring-Richtlinie von RFI-IRFOS, keine Ober- oder Untergrenze. Sie liefert einen reproduzierbaren, für Dritte nachvollziehbaren Ausgangspunkt für den Schweregrad und erfasst reale Blast-Radius-Effekte nicht von sich aus. In diesem Bericht korrigiert sich B2 auf HIGH, B1 und B3 korrigieren sich auf MEDIUM, jeweils auf ihrer eigenen berechneten Stufe, ohne Eskalation. Offenlegung nach ISO/IEC 29147 und dem österreichischen Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: OMV-APP-2026.