Koordinierte Offenlegung, Abschlussbericht

Bank Austria Mobile App Android (com.bankaustria.android.olb)

UniCredit Bank Austria AG, Wien, Österreich

ABLEHNUNG DES INHALTLICHEN AUSTAUSCHS · FALL GESCHLOSSEN UND VERÖFFENTLICHT AM 26. SEPTEMBER 2026, AM ANGEGEBENEN EMBARGO-DATUM

Ziel	UniCredit Bank Austria AG, Wien, Österreich
Package	com.bankaustria.android.olb, Version 9.9.1
Betreiber	UniCredit Bank Austria AG
Erstmeldung	2026-06-26
Angegebenes Embargo	2026-09-26, dem Betreiber direkt in der Erstmeldung sowie in der Nachricht vom 12. September 2026 schriftlich bestätigt
Bericht veröffentlicht	2026-09-26, zum angegebenen Datum
Behörden	Österreichische Datenschutzbehörde (DSB), Finanzmarktaufsicht (FMA)
Ausgehende Nachrichten gesamt	6 über 92 Tage, an datenschutz@bankaustria.at (dauerhaft unzustellbar) und datenschutz@unicreditgroup.at (zugestellt).
Eingehende Antworten	Eine Antwort am 18. September 2026, ohne inhaltliches Eingehen auf einen der fünf Befunde.

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 fünf Befunde in der Bank Austria Mobile App v9.9.1. Die Network Security Configuration erlaubt cleartextTrafficPermitted=true auf einer Banking-App, unverschlüsselter HTTP-Verkehr ist damit systemseitig zulässig. Dieser Befund verbleibt bei CRITICAL/9.3 unter CVSS v4.0.

Ein zweiter Befund, ebenfalls CRITICAL: die App ist vollständig als Ionic-Capacitor-WebView-Hybrid gebaut, mit aktivem Cordova-InAppBrowser und CordovaHTTP-Plugin. In Kombination mit dem fehlenden Verschlüsselungszwang entsteht eine klassische MITM-Angriffsfläche mit JavaScript-Injektionsmöglichkeit auf laufende Banking-Sitzungen über die Capacitor-Bridge. Dieser Befund korrigiert sich auf CRITICAL/9.1.

Ein dritter Befund: ein Firebase-API-Schlüssel und die zugehörige Realtime-Database-URL (bank-austria-mobilebanking.firebaseio.com) sind im öffentlich zugänglichen Play-Store-Binary hardcodiert. Dieser Befund korrigiert sich auf HIGH/8.8.

Ein vierter Befund, MEDIUM: ThreatMark erfasst Tipp- und Touch-Dynamik zur Verhaltensbiometrie und überträgt sie an Server in Tschechien, ohne erkennbare Nennung als Auftragsverarbeiter in der Datenschutzerklärung. Ein fünfter Befund, ebenfalls MEDIUM: Huawei AGConnect und HMS sind integriert und senden Gerätekennungen und Telemetrie an chinesische Infrastruktur.

Sechs Nachrichten wurden über 92 Tage gesendet. UniCredit Bank Austria AG antwortete am 18. September 2026 auf die Nachricht vom 12. September, lehnte darin jede inhaltliche Äußerung zu den fünf Befunden ausdrücklich ab, verwies stattdessen auf eine Stellungnahme gegenüber der FMA, deren Inhalt RFI-IRFOS zu keinem Zeitpunkt zugestellt wurde, und behielt sich rechtliche Schritte für den Fall vor, dass die Veröffentlichung nach Ansicht des Unternehmens unrichtige Behauptungen enthalte. Keine der drei am 12. September gestellten Ja/Nein-Fragen wurde beantwortet. Das 90-Tage-Embargo, dem Betreiber direkt mitgeteilt, läuft heute ab. Dieser Bericht und die begleitende Abschlussmitteilung veröffentlichen zum angegebenen Datum.

Scope: Root-Level-Code-Analyse der produktiven Bank Austria Mobile App (com.bankaustria.android.olb, Version 9.9.1), direkt von einem Produktivgerät extrahiert und am 26. Juni 2026 untersucht. Es wurde kein Konto angelegt, und es fand keine Interaktion mit der Backend-Infrastruktur von UniCredit, ThreatMark oder Huawei statt.

Disposition

Fünf Befunde wurden am 26. Juni 2026 gemeldet, unter CVSS v4.0 neu bewertet. Die fehlende Network Security Configuration in Kombination mit dem WebView-Injection-Vektor verbleiben auf CRITICAL. Der hardcodierte Firebase-Schlüssel korrigiert sich auf HIGH. Die undokumentierte ThreatMark-Verhaltensbiometrik und die Huawei-HMS/AGConnect-Einbindung korrigieren sich beide auf MEDIUM. UniCredit Bank Austria AG antwortete am 18. September 2026, lehnte eine inhaltliche Stellungnahme jedoch ausdrücklich ab und verwies stattdessen auf eine ausschließlich der FMA übermittelte Stellungnahme, deren Inhalt RFI-IRFOS nie vorlag.

ID	Severity	Title
B1	CRITICAL	Network Security Configuration erlaubt unverschlüsselten Verkehr
B2	CRITICAL	Capacitor-WebView-Hybrid mit InAppBrowser und CordovaHTTP als MITM-Injektionsfläche
B3	HIGH	Firebase-API-Schlüssel und Realtime-Database-URL hardcodiert
B4	MEDIUM	ThreatMark-Verhaltensbiometrik ohne Nennung als Auftragsverarbeiter
B5	MEDIUM	Huawei AGConnect und HMS routen Telemetrie über chinesische Infrastruktur

Die Antwort vom 18. September 2026

UniCredit Bank Austria AG antwortete am 18. September 2026 auf die Nachricht von RFI-IRFOS vom 12. September. Die Antwort bestätigt, dass eine Stellungnahme gegenüber der österreichischen Finanzmarktaufsichtsbehörde (FMA) abgegeben wurde, lehnt eine inhaltliche Äußerung gegenüber RFI-IRFOS zu den fünf Befunden jedoch ausdrücklich ab und behält sich rechtliche Schritte vor, sollte die angekündigte Veröffentlichung nach Ansicht des Unternehmens unrichtige Behauptungen enthalten. Der Inhalt der an die FMA übermittelten Stellungnahme wurde RFI-IRFOS zu keinem Zeitpunkt zugestellt. Keine der drei am 12. September gestellten Ja/Nein-Fragen wurde beantwortet.

Findings

B1: Network Security Configuration erlaubt unverschlüsselten Verkehr

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 9.3.

res/xml/network_security_config.xml setzt cleartextTrafficPermitted=”true” für eine Banking-App. Unverschlüsselter HTTP-Verkehr ist damit systemseitig zulässig, ohne dokumentierte Ausnahmeregel im Rahmen einer Datenschutz-Folgenabschätzung.

```
res/xml/network_security_config.xml:
<base-config cleartextTrafficPermitted="true">
```

Impact: Auf einer Banking-App erlaubt diese Konfiguration Angreifern in derselben Netzwerkumgebung, unverschlüsselten Verkehr mitzulesen oder zu manipulieren. Art. 32 DSGVO, § 25a BWG.

Fix: cleartextTrafficPermitted=false setzen und ausschließlich TLS-Verbindungen zulassen. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

B2: Capacitor-WebView-Hybrid mit InAppBrowser und CordovaHTTP als MITM-Injektionsfläche

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 9.1.

Die App ist vollständig als Ionic-Capacitor-WebView-Hybrid gebaut, mit aktivem Cordova-InAppBrowser und CordovaHTTP-Plugin. In Kombination mit cleartextTrafficPermitted="true" (B1) entsteht eine MITM-Angriffsfläche mit JavaScript-Injektionsmöglichkeit auf Banking-Sessions über die Capacitor-Bridge.

```
Cordova InAppBrowser (aktiv)
CordovaHTTP-Plugin (aktiv)
Capacitor-Bridge: JS <-> Native, ungeschützt gegen Injection bei MITM-Position
```

Impact: Ein Angreifer mit MITM-Position kann JavaScript in eine laufende Banking-Sitzung injizieren und über die Capacitor-Bridge auf native Funktionen zugreifen. Art. 32 DSGVO, § 25a BWG.

Fix: WebView-Hybrid-Architektur durch natives UI oder gehärtete WebView-Konfiguration mit Content-Security-Policy und Bridge-Whitelisting ersetzen. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

B3: Firebase-API-Schlüssel und Realtime-Database-URL hardcodiert

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 8.8.

Ein Firebase-API-Schlüssel und die zugehörige Realtime-Database-URL (bank-austria-mobilebanking.firebaseio.com) sind im öffentlich zugänglichen Play-Store-Binary hardcodiert.

```
firebase_database_url = https://bank-austria-mobilebanking.firebaseio.com
google_api_key (Firebase, aus Play-Store-Binary extrahierbar)
```

Impact: Jeder, der die APK herunterlädt, kann den Schlüssel extrahieren und unauthentifizierte Aufrufe gegen das Firebase-Projekt versuchen. Art. 32 DSGVO.

Fix: Schlüssel nach Package-Name und Zertifikat einschränken, Datenbankregeln serverseitig prüfen. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

B4: ThreatMark-Verhaltensbiometrik ohne Nennung als Auftragsverarbeiter

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.

ThreatMark erfasst Tipp- und Touch-Dynamik zur Verhaltensbiometrie und überträgt sie an Server in Tschechien, ohne erkennbare Nennung als Auftragsverarbeiter in der D atenschutzerklärung.

Impact: Biometrische Verhaltensdaten (Art. 9 DSGVO) werden an einen nicht namentlich genannten Auftragsverarbeiter im EU-Ausland übermittelt. Art. 9, Art. 13 DSGVO.

Fix: ThreatMark namentlich als Auftragsverarbeiter in der Datenschutzerklärung nennen oder Verarbeitung einstellen. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

B5: Huawei AGConnect und HMS routen Telemetrie über chinesische Infrastruktur

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.

Huawei AGConnect und HMS sind integriert und senden Gerätekennungen und Telemetrie an chinesische Infrastruktur, die dem chinesischen Geheimdienstgesetz unterliegt.

```
Huawei AGConnect SDK (aktiv)
Huawei Mobile Services (HMS) (aktiv)
```

Impact: Gerätekennungen und Telemetrie einer EU-Banking-App verlassen den EWR ohne dokumentierte Transferfolgenabschätzung. Art. 44 DSGVO.

Fix: Huawei AGConnect/HMS entfernen oder Transferfolgenabschätzung nach Art. 46 DSGVO dokumentieren. Keine Bestätigung, dass dies erfolgt ist, wurde je empfangen.

Datenschutz, Artikel für Artikel

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

Artikel	Befund	Grundlage
Art. 32 DSGVO, § 25a BWG	B1	Network Security Configuration erlaubt unverschlüsselten Verkehr.
Art. 32 DSGVO, § 25a BWG	B2	Capacitor-WebView-Hybrid als MITM-Injektionsfläche.
Art. 32 DSGVO	B3	Firebase-API-Schlüssel und Realtime-Database-URL hardcodiert.
Art. 9, Art. 13 DSGVO	B4	ThreatMark-Verhaltensbiometrik ohne Nennung als Auftragsverarbeiter.
Art. 44 DSGVO	B5	Huawei AGConnect/HMS routen Telemetrie über chinesische Infrastruktur.

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 verbleiben B1 und B2 auf CRITICAL, B3 korrigiert sich auf HIGH, B4 und B5 korrigieren sich auf MEDIUM, jeweils auf ihrer eigenen berechneten Stufe. Offenlegung nach ISO/IEC 29147 und dem österreichischen Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: BA-MOBILE-2026.