Coordinated Privacy Disclosure, Final Report — With Operator-Attribution Correction

Merci Android (com.amadeus.merci.client.ui), version 26.6.0

Operator disputed — see correction notice below

OPERATOR-ATTRIBUTION CORRECTED · AMADEUS IT GROUP DENIES ANY CONNECTION · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, ON THE ORIGINAL EMBARGO DATE

Package Reviewed	com.amadeus.merci.client.ui, version 26.6.0
Original Attribution	The package's identifier and developer strings pointed to Amadeus IT Group, S.A. at the time of review, 27 June 2026
Operator Correction	Amadeus IT Group, S.A. states, in writing, that no version 26.x of Merci was ever released by Amadeus, and that the package is not a product or service operated or maintained by Amadeus. RFI-IRFOS has not independently confirmed an alternative historical operator for this exact package identifier and version; the current live Play Store listing for this package resolves to Singapore Airlines Limited, independently confirmed 27 August 2026, a fact not in dispute
Initial Disclosure	2026-06-27
Original Embargo	2026-09-25 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-25, on the original embargo date
Regulators	Spanish AEPD (originally cited as lead SA for Amadeus IT Group, now uncertain given the correction), Austrian DSB, German BfDI, CERT.at
Total Outbound Messages	7, across 90 days to DPO@amadeus.com.
Inbound Replies	2 substantive replies, 27 August and 24 September 2026, both from Amadeus's Digital Trust Office, denying any operational connection to this package. Neither reply, nor any other correspondence, has established who did build or operate this specific package and version.

rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 27 June 2026, RFI-IRFOS disclosed technical findings from a decompiled Android binary at package identifier com.amadeus.merci.client.ui, version 26.6.0, addressed to Amadeus IT Group, S.A. based on the package's developer strings and naming at the time. The binary itself, independent of who built it, contains Microblink's BlinkCard payment-card OCR SDK (643 classes) reading card number, expiry, and cardholder name from a camera scan; Mastercard's NuDetect behavioral-biometrics sensor stack (363 classes) reading accelerometer, gyroscope, and magnetometer data as a device-motion behavioral fingerprint; and both a full Alipay stack (449 classes, Ant Group, PRC) and a full Huawei HMS stack (977 classes), both subject to China's National Security Law.

Amadeus IT Group's Digital Trust Office replied twice, on 27 August and 24 September 2026, stating that this package is not operated or maintained by Amadeus and, in the most recent reply, that no version 26.x of Merci was ever released by Amadeus. RFI-IRFOS asked one direct factual question three times: whether this exact package identifier was ever connected to any Amadeus account or infrastructure at any point, including as an earlier white-label build later transferred elsewhere. That precise historical question was never answered in those exact terms, but Amadeus's specific, written denial of ever releasing version 26.x is treated here as sufficient grounds to withdraw the Amadeus attribution, consistent with the policy RFI-IRFOS stated when the question was first raised.

RFI-IRFOS has not independently identified who did build or operate this package at version 26.6.0 on 27 June 2026. The package's current live Play Store listing, independently confirmed 27 August 2026, resolves to Singapore Airlines Limited; RFI-IRFOS makes no claim that Singapore Airlines built or operated the specific version reviewed, only that it is the confirmed current publisher of the package identifier today. The technical findings below are published as an accurate record of the binary as found, attributed to the package identifier itself, not to any named corporate operator, given the unresolved history.

Scope: Root-level static analysis of a decompiled Android binary at package identifier com.amadeus.merci.client.ui, version 26.6.0, as reviewed on 27 June 2026. No dynamic instrumentation, live traffic capture, or interaction with any backend infrastructure was performed. The findings describe the binary reviewed at that specific version; they make no claim about any other version, past or present, of any product carrying a similar name.

Disposition

A correction, not a standard closure. RFI-IRFOS decompiled a real, live binary at this exact package identifier and version on 27 June 2026; the technical findings below describe that binary as found, independent of who built it. The binary's developer strings and package identifier at the time pointed to Amadeus IT Group, and the original disclosure was addressed to Amadeus on that basis. Amadeus has since stated in writing, twice, that it never released this package or version. RFI-IRFOS asked a single direct factual question three times, whether any Amadeus account or infrastructure was ever connected to this exact package identifier at any point, including as a white-label build later transferred elsewhere, and did not receive a direct answer to that specific question; Amadeus's most recent reply does state plainly that no 26.x version was released by Amadeus, which RFI-IRFOS treats as sufficient to withdraw the attribution to Amadeus, per RFI-IRFOS's own stated policy set at the time the question was first asked. The findings themselves stand, unaltered, as an accurate technical record of the binary reviewed; only the corporate attribution is withdrawn.

ID	Severity	Title
C1	HIGH	Behavioral-Biometrics Sensor Stack Reads Device Motion as Art. 9 Data
C2	HIGH	Full Alipay and Huawei HMS Stacks, Both PRC-NSL-Obligated
H1	HIGH	Chucker HTTP Debug Interceptor Compiled Into the Production Binary
H2	MEDIUM	Payment-Card OCR via Camera, Processed by a Third-Party SDK
H3	MEDIUM	Obfuscated CyberfEnd SDK, Shared With Two Other Audited Travel Apps
H4	MEDIUM	Firebase API Key Hardcoded and Extractable
M1	LOW	Persistent Microphone Access With No Disclosed Purpose

Operator-Attribution Correction

At the time this binary was reviewed, 27 June 2026, the package identifier and developer strings pointed to Amadeus IT Group, S.A., and the original disclosure was addressed there on that basis. Amadeus's Digital Trust Office replied twice, on 27 August and 24 September 2026, stating that the package is not operated or maintained by Amadeus, and, in the most recent reply, that no version 26.x of Merci was ever released by Amadeus. RFI-IRFOS asked a single, precise historical question three times, whether any Amadeus account or infrastructure was ever connected to this exact package identifier at any point, including as a white-label build later transferred elsewhere, in order to distinguish a genuine attribution error from a later ownership transfer that would not retroactively change what was true when the binary was found. That precise question was not answered in those exact terms. Amadeus's specific, written denial that any version 26.x was ever released by Amadeus is treated here as sufficient to withdraw the attribution, consistent with the policy stated to Amadeus when the question was first raised: RFI-IRFOS is not escalating this dispute and is not asserting Amadeus built or operated the binary reviewed.

RFI-IRFOS has not independently established who did build or operate this package at version 26.6.0 on 27 June 2026. The package's current live Play Store listing, independently confirmed 27 August 2026, resolves to Singapore Airlines Limited; this report makes no claim that Singapore Airlines built or operated the specific version reviewed, and names it here only as the confirmed current publisher of the package identifier as of that check. The technical findings below stand as an accurate, independently reproducible record of the binary as decompiled and reviewed; they are attributed to the package identifier itself, not to any named corporate operator, given this unresolved history.

Seven Messages, Two Substantive Replies, One Unresolved Question

This case's correspondence record involved a working contact channel and real, substantive engagement, not silence. Seven messages were sent to DPO@amadeus.com across 90 days, cc'ing Spanish AEPD, Austrian DSB, and German BfDI. Two replies were received, both from Amadeus's Digital Trust Office, both denying operational responsibility for the package; neither, until the most recent, addressed the specific historical question of whether any Amadeus infrastructure was ever connected to this package identifier. This closing report treats the 24 September reply's specific denial of ever releasing version 26.x as sufficient grounds to correct the attribution, in line with the policy stated to Amadeus throughout this exchange.

Findings

C1: Behavioral-Biometrics Sensor Stack Reads Device Motion as Art. 9 Data

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7. This finding reaches HIGH on the computed CVSS v4.0 score alone; no editorial escalation was applied or needed.

Mastercard's NuDetect SDK (363 classes) is compiled in and confirmed active via DefaultSensorEventHandler, reading accelerometer, gyroscope, and magnetometer data continuously. This device-motion data is used as behavioral biometric input, a GDPR Art. 9 special category, via a MobileNuCaptcha flow and associated ListenerConfiguration/RegisterListenersModifierKt classes.

```
NuDetect/Mastercard (363 classes): DefaultSensorEventHandler (accelerometer, gyroscope
    , magnetometer)
ListenerConfiguration, RegisterListenersModifierKt, MobileNuCaptcha
```

Impact: The specific way a user physically moves their device is captured and processed as behavioral biometric data, a special category under GDPR Art. 9, with no independently confirmed consent or disclosure mechanism located.

Fix: Document the NuDetect integration explicitly as Art. 9 processing with an appropriate legal basis, or remove it. No confirmation of remediation was received, and no party has claimed responsibility for the binary to remediate it.

C2: Full Alipay and Huawei HMS Stacks, Both PRC-NSL-Obligated

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7. This finding reaches HIGH on the computed CVSS v4.0 score alone; no editorial escalation was applied or needed.

A full Alipay stack (449 classes, including apmobilesecuritysdk and mobilesecuritysdk, Ant Group, PRC) and a full Huawei HMS stack (977 classes, HuaweiAaidInitProvider at initOrder=500) are both compiled into the binary. Both Ant Group and Huawei are PRC companies subject to China's National Security Law Art. 7, an obligation to cooperate with PRC state intelligence on demand.

```
Alipay stack: 449 classes, incl. apmobilesecuritysdk + mobilesecuritysdk (Ant Group,
    PRC)
Huawei HMS stack: 977 classes, HuaweiAaidInitProvider initOrder=500
```

Impact: Two independent PRC-NSL-obligated processor stacks are present in a travel/payment-adjacent app, with no EU adequacy decision covering either transfer as documented in the reviewed binary.

Fix: Document Art. 44-49 transfer mechanisms for both integrations or remove them. No confirmation of remediation was received, and no party has claimed responsibility for the binary to remediate it.

H1: Chucker HTTP Debug Interceptor Compiled Into the Production Binary

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. This finding reaches HIGH on the computed CVSS v4.0 score alone; no editorial escalation was applied or needed.

ChuckerInterceptor (8 classes) is compiled into the production binary, the second consecutive app in this audit series carrying this specific debug-inspection tool in a production release. If active, it exposes local HTTP traffic to inspection on the same network.

```
ChuckerInterceptor (8 classes) -- second consecutive audited app carrying this same
    debug SDK in production
```

Impact: If initialized, a debug HTTP interceptor in a production binary handling payment-card OCR data represents a significant local-network exposure vector.

Fix: Confirm and strip all Chucker classes from production release builds. No confirmation of remediation was received, and no party has claimed responsibility for the binary to remediate it.

H2: Payment-Card OCR via Camera, Processed by a Third-Party SDK

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.

Microblink's BlinkCard SDK (643 classes) extracts card number, expiry, and cardholder name via camera-based OCR, processed through Microblink's own infrastructure.

```
Microblink BlinkCard (643 classes): payment card OCR via camera
```

Impact: Payment card details are extracted and processed through a third-party OCR vendor's infrastructure, requiring an Art. 28 processor relationship to be documented.

Fix: Document Microblink as a named processor under Art. 28 and Art. 13(1)(e). No confirmation of remediation was received, and no party has claimed responsibility for the binary to remediate it.

H3: Obfuscated CyberfEnd SDK, Shared With Two Other Audited Travel Apps

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.

CyberfEnd (62 classes), an obfuscated SDK, is present in this binary. This is the second of three consecutive audited travel-sector apps in this series found to contain the same obfuscated SDK (trivago, this package, and Air Canada), suggesting a shared upstream vendor or build pipeline across otherwise unrelated travel-industry Android apps.

```
CyberfEnd (62 classes) -- also confirmed in trivago and Air Canada Android binaries
    reviewed in this same audit series
```

Impact: An obfuscated, unidentified SDK's presence across multiple unrelated travel-industry apps suggests a shared build pipeline or vendor whose data-processing role has not been independently established.

Fix: Identify and document CyberfEnd's function and data-processing role. No confirmation of remediation was received, and no party has claimed responsibility for the binary to remediate it.

H4: Firebase API Key Hardcoded and Extractable

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

A Firebase API key and project identifier are hardcoded and extractable from the binary.

```
AIzaSyCvQ9--NHQyzKPAakel8KRwC-Zs7a6jqQY (Firebase project: stoked-monitor-852)
```

Impact: The key is trivially extractable, and depending on the security-rule configuration behind it, could enable unauthorized access or denial of service against legitimate users.

Fix: Restrict the Firebase API key by package name and SHA-1 certificate fingerprint. No confirmation of remediation was received, and no party has claimed responsibility for the binary to remediate it.

M1: Persistent Microphone Access With No Disclosed Purpose

LOW, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.4.

RECORD_AUDIO and FOREGROUND_SERVICE_MICROPHONE are both declared, meaning microphone access can run as a persistent foreground service, with no disclosed feature located that requires it.

Impact: Persistent microphone capability is present with no disclosed purpose; the practical exploitation path requires local conditions the static review could not establish, which keeps the computed score low.

Fix: Document the specific feature requiring persistent microphone access, or remove it. No confirmation of remediation was received, and no party has claimed responsibility for the binary to remediate it.

Data Protection, Article by Article

The findings map onto a small, specific set of GDPR provisions, set out below in one place instead of scattered across the findings themselves. These citations describe the binary reviewed, independent of the unresolved operator question above.

Article	Finding	Basis
Art. 9	C1	Device-motion behavioral biometrics captured via NuDetect.
Art. 44-49	C2	Two PRC-NSL-obligated processor stacks (Alipay, Huawei HMS).
Art. 32	H1	Debug HTTP interceptor compiled into a production binary handling payment data.
Art. 28, Art. 13(1)(e)	H2	Undisclosed third-party payment-card OCR processor.
Art. 13(1)(e)	H3	Unidentified obfuscated SDK shared across multiple travel-sector apps.
Art. 32	H4	Hardcoded, trivially extractable Firebase API key.

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 is RFI-IRFOS's scoring guideline, not a ceiling or a floor. It gives a reproducible, third-party-legible starting point for severity, and it does not capture real-world blast radius on its own. In this report, C1, C2, and H1 reach HIGH on their computed CVSS v4.0 scores alone, no editorial escalation applied; H2, H3, and H4 correct to MEDIUM to match their own computed bands; M1 corrects to LOW on its own computed band. This report additionally documents a genuine operator-attribution correction: the findings describe a real binary as decompiled and reviewed, but the corporate attribution originally made to Amadeus IT Group is withdrawn following Amadeus's written denial, per the policy stated to Amadeus throughout this exchange. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: AMADEUSMERCI-2026-R1.