Coordinated Security & Privacy Disclosure, Final Report

Apple Music for Android (com.apple.android.music)

A bug-bounty-framed rebuttal that named every finding and disputed all six, none conceded, embargo held throughout

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY-ONE DAYS, ONE REBUTTAL, ZERO FINDINGS CONCEDED

Target	Apple Distribution International Ltd., Cork, Ireland
Product audited	Apple Music for Android, com.apple.android.music, v5.2.1 (versionCode 1545)
Disclosure reference	REF APPLEMUSIC-2026-R1, ticket OE0106480218038
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 cleartext HTTP / C2 Firebase key, CVSS v4.0 9.3)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production Apple Music Android application, v5.2.1, and identified six findings, two CRITICAL, four HIGH. The most significant: the shipped app references a network security configuration whose base-config sets cleartextTrafficPermitted to true, while a correctly hardened alternative configuration with cleartextTrafficPermitted set to false exists in the same APK but is never referenced in the manifest, alongside a leftover development artifact pointing at a local webpack dev-server port.

A hardcoded Firebase production credential was also extracted from the binary. Four further findings raise separate concerns: Google Crashlytics crash telemetry with Google LLC never named as the receiving entity in the in-app consent text; periodic background contact synchronization for a friend-recommendation feature uploading names, phone numbers, and photo references; advertising-attribution permissions declared on a paid subscription platform; and figarometrics, Apple's internal telemetry SDK, whose enumerated event types include every search query typed, aggregated listen history, subscription purchase transactions, and a full linked-list navigation history of every screen visited.

Fifty-three days after R1, Apple Product Security replied substantively under a bug-bounty framing, naming and individually disputing all six findings as unproven absent a working proof-of-concept, expected consented behavior, or a product-and-policy matter rather than a security issue. RFI-IRFOS rebutted the same day. Two further written requests asking Apple to confirm the same findings' status in its then-current shipping version, 6.5.1, and whether the Irish DPC had been notified, went unanswered through the close of the embargo.

Scope: Static analysis of the publicly downloaded production Apple Music Android APK, on an authorized test device, only. No Apple ID, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 20 June 2026 to product-security@apple.com, cc privacy@apple.com, bcc the Austrian DSB, CERT.at, and the Irish DPC (Apple's lead supervisory authority). Fifty-three days later, Apple Product Security replied substantively, naming and disputing all six findings individually as unproven, expected, or public-by-design behavior, and demanding a working proof-of-concept against a newer app version. Two further written requests for confirmation on the same version went unanswered.

ID	Severity	Title
C1	CRITICAL	Production release ships a development network security configuration permitting cleartext HTTP
C2	CRITICAL	Hardcoded Firebase production credentials in the shipped APK
H1	HIGH	Google Crashlytics: Google LLC never named as the receiving entity in the in-app disclosure

ID	Severity	Title
H2	HIGH	Periodic background contact synchronization for social-graph construction
H3	HIGH	Advertising attribution permissions declared on a paid subscription platform
H4	HIGH	figarometrics: Apple's internal telemetry capturing full search, listening, purchase, and navigation history

Subject & Operator Analysis

Apple Distribution International Ltd. (Cork, Ireland) operates Apple Music for Android for a global subscriber base, with the Irish Data Protection Commission as lead supervisory authority.

Positive Observations

No specific positive controls were identified as a distinct section in the original disclosure; the audited binary's primary characteristics are addressed directly in the findings above.

Findings

C1: Production release ships a development network security configuration permitting cleartext HTTP

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

AndroidManifest.xml references @xml/network_security_config, whose base-config sets cleartextTrafficPermitted="true". A correctly hardened alternative, res/xml/network_security_configuration.xml with cleartextTrafficPermitted="false", exists in the same APK but is never referenced. Production strings.xml also contains debug_ip_base_url = "http://%s:4200/", port 4200 being the default webpack/Angular dev-server port.

```
<base-config cleartextTrafficPermitted="true">
  <trust-anchors><certificates src="system" /></trust-anchors>
</base-config>

debug_ip_base_url = "http://%s:4200/"  <- dev-server artifact in production strings.
    xml
```

Apple's 12 August reply, verbatim: "Permitting plaintext traffic is not a security or privacy issue absent empirical evidence that sensitive or personal data is exposed. Your report does not demonstrate that." RFI-IRFOS's position, restated in the 18 August and 31 August follow-ups: a correctly hardened configuration already exists in the same binary and is simply not

wired into the manifest, which is evidence of a build-pipeline error rather than a deliberate design choice requiring a runtime interception demonstration. The direct question of whether the currently shipping version, 6.5.1 as named by Apple itself, still ships the same misconfiguration was never answered.

Impact: A production build ships the insecure of two available network security configurations, exposing traffic to cleartext fallback, with no confirmation the currently shipping version differs.

Fix: Reference the already-present hardened configuration in the manifest, remove the development artifact, and confirm the fix version number in writing.

C2: Hardcoded Firebase production credentials in the shipped APK

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

A complete Firebase project configuration is extracted verbatim from res/values/strings.xml.

```
google_api_key:        AIzaSyB2az7ihbVLcmh81YKR5TEeLYuH_wCt1Sc
google_app_id:         1:843686588413:android:460563c870948822
gcm_defaultSenderId:   843686588413
project_id:            apple-music-8cac2
firebase_database_url: https://apple-music-8cac2.firebaseio.com
```

Apple's 12 August reply, verbatim: "The Firebase and Google API keys and the app and project identifiers are client-side identifiers that are public by design. They are not secrets, and access is controlled server-side by Firebase security rules. Their presence in the app is expected behavior, not a credential leak." RFI-IRFOS's standing position, applied identically across every case in this research series: a publicly extractable Firebase key is a finding regardless of that classification, because the burden of demonstrating the actual security-rules configuration rests with the operator, not an outside researcher working from a downloaded APK alone.

Impact: A publicly extractable production credential enables probing of the project and potential further backend access, subject to security-rules configuration Apple has not disclosed.

Fix: Publish the Firebase project's security-rules configuration, or rotate and restrict the key to the production certificate fingerprint.

H1: Google Crashlytics: Google LLC never named as the receiving entity in the in-app disclosure

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

15 Google Crashlytics smali classes transmit crash telemetry to Google LLC, Mountain View, California. The in-app consent text states only: "Personal data is either not logged at all or is removed from any reports before they're sent to Apple and Crashlytics."

Apple's 12 August reply, verbatim: "How Crashlytics is named in the in-app disclosure is a product and policy matter, not a demonstrated security or privacy issue. Your report does not show any user data being exposed across a security or privacy boundary." The direct question of whether the currently shipping build names Google LLC specifically as the recipient entity was never answered.

Impact: Crash telemetry is transmitted to a named third-party service without the receiving corporate entity, Google LLC, being identified in the user-facing disclosure.

Fix: Name Google LLC explicitly as the Crashlytics processing entity in the in-app consent text and privacy documentation.

H2: Periodic background contact synchronization for social-graph construction

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

READ_CONTACTS is declared with periodic background sync for a "friends on Apple Music" feature. In-app text: "Apple Music will periodically check the contacts on your devices to recommend new friends." Fields queried and uploaded: contact_id, display_name, data1 (phone/email), mimetype, photo_uri, is_primary.

Apple's 12 August reply, verbatim: "The contacts functionality operates with explicit user consent, as reflected in the consent text quoted in your own report. A consented feature working as described is expected behavior, not an exposure of user data."

Impact: A social-graph-construction feature periodically uploads contact names, contact details, and photo references, a data minimization question independent of whether a general consent notice covers it.

Fix: Scope the data actually uploaded to the minimum required for friend-matching, and document the specific retention period for uploaded contact data.

H3: Advertising attribution permissions declared on a paid subscription platform

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

ACCESS_ADSERVICES_ATTRIBUTION, ACCESS_ADSERVICES_AD_ID, and AD_ID are all declared.

Apple's 12 August reply, verbatim: "A declared application permission is not the same as a demonstrated data flow. If you believe advertising or attribution data is actually collected or transmitted, please provide a working proof of concept demonstrating that behavior against the latest shipping software, currently 6.5.1." RFI-IRFOS's own 18 August letter records this specifically as an open question rather than a confirmed runtime data flow, since static analysis alone shows declared permissions, not confirmed transmission.

Impact: Advertising-attribution capability is declared on a paid subscription platform with no disclosed Art. 6(1) legal basis, though whether it is actively exercised was not confirmed by static analysis alone.

Fix: Confirm whether these permissions are exercised in the current shipping build and, if so, publish the Art. 6(1) legal basis for advertising attribution on paid accounts.

H4: figarometrics: Apple's internal telemetry capturing full search, listening, purchase, and navigation history

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

com/apple/android/music/figarometrics/, 42 smali classes, Apple's internal telemetry SDK. Enumerated event types include search, playsSummary, transaction, and page.

```
search           <- captures every query typed
playsSummary     <- aggregates listen history
transaction      <- captures subscription purchases
page             <- maintains a linked list of every screen visited
+ click, componentRender, dialog, downloadComplete, enter, exit, impressions,
  linking, loadUrl, notificationAction, notificationRequest, pageRender,
  playbackError, playbackSession, playbackStart
```

Apple's 12 August reply, verbatim: "This is first-party Apple telemetry sent to Apple. If you believe this data flow crosses a security or privacy boundary, please provide a working proof of concept demonstrating the alleged behavior against the latest shipping software, currently 6.5.1."

Impact: A first-party telemetry system captures a complete behavioral profile, search queries, listening history, purchases, and full navigation history, without per-category disclosure granularity under Art. 13(1)(c).

Fix: Publish a per-category breakdown of figarometrics data collection under Art. 13(1)(c), including retention periods for search, listening, and navigation event data.

Apple's Response, Recorded in Full

Fifty-three days after R1, on 12 August 2026, Apple Product Security replied under ticket OE0106480218038, signed "Robert, Apple Product Security": "The Apple Security Bounty program rewards researchers for actionable security or privacy issues affecting Apple devices, software, or services. We do not purchase engagements to learn more about a finding, and all details must be provided in full as part of the submission. Please also note that static analysis alone is not sufficient to establish a security or privacy issue. To evaluate a report, we need a valid, working proof of concept demonstrating the behavior against actual shipping software." The reply then addressed all six findings individually, quoted in full alongside each finding above, disputing each as either unproven absent a proof-of-concept, expected consented behavior, or a product-and-policy matter rather than a demonstrated security or privacy issue.

RFI-IRFOS's same-day rebuttal rejected the bug-bounty/case-ID framing for a coordinated GDPR disclosure, rejected the position that a publicly extractable but non-secret credential cannot itself be a finding, and reasserted that a GDPR Art. 9 lawful-basis obligation exists independent of any voluntary bug-bounty program's terms, and that publication proceeds unconditionally and is not for sale. A follow-up on 18 August restated three specific yes/no questions with a 25 August deadline: whether cleartextTrafficPermitted is still true in version 6.5.1, whether Google LLC is now named in the Crashlytics consent text, and whether the Irish DPC was notified. A further follow-up on 31 August, after the 25 August deadline passed with silence, restated the same three questions with a new deadline of 7 September. No reply of any kind was received after 12 August, and both subsequent deadlines passed unanswered through the close of the embargo.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1)(b), Art. 25(1)	Development network config shipped in production
C2	GDPR Art. 32(1)(b), Art. 13(1)(e)	Hardcoded, publicly extractable production credential
H1	GDPR Art. 13(1)(e), Art. 44-49	Undisclosed receiving entity for crash telemetry
H2	GDPR Art. 5(1)(c), Art. 13(1)(c)	Contact data upload for social-graph construction
H3	GDPR Art. 5(1)(b), Art. 6(1)	Undisclosed legal basis for ad-attribution permissions
H4	GDPR Art. 13(1)(c), Art. 5(1)(b)	Undisclosed granular scope of internal behavioral telemetry

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to product-security@apple.com, cc privacy@apple.com, bcc Austrian DSB/CERT.at/Irish DPC, 6 findings; automated ticket OE0106480218038 assigned
2026-06-27	Follow-up, 48h deadline set; dpireland@apple.com found invalid and dropped
2026-07-27	Day-30 follow-up, findings restated
2026-08-12	Apple Product Security substantively replies, disputes all six findings, demands PoC against v6.5.1; RFI-IRFOS rebuts same day
2026-08-18	Three specific yes/no questions posed, deadline 25 August
2026-08-31	25 August deadline passed unanswered; questions restated, new deadline 7 September; weekly SHA-256 re-pull instituted
2026-09-19	7 September deadline passed unanswered; embargo, as stated identically throughout the correspondence, closes and this report publishes

Apple engaged more substantively than most targets in this research series, naming and individually disputing all six findings rather than ignoring them. None was conceded, and the specific follow-up questions asking Apple to confirm the same findings' status in its own currently shipping version went unanswered through the close of the embargo.

Residual Risk & Recommendations

- Confirm whether cleartextTrafficPermitted is still true in the currently shipping version and reference the already-present hardened configuration.
- Publish the Firebase project's security-rules configuration underlying the CRITICAL classification dispute.
- Name Google LLC explicitly as the Crashlytics processing entity in the in-app consent text.
- Publish a per-category breakdown of figarometrics telemetry collection and its retention periods.
- Confirm whether the advertising-attribution permissions are actively exercised and, if so, their Art. 6(1) legal basis.
- Confirm whether the Irish DPC was notified under Art. 33 in relation to any of these findings.

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