



Coordinated Security & Privacy Disclosure, Final Report

Amazon Music for Android (com.amazon.mp3)

Listening behavior linked to the amazon.com shopping profile, a security-team reply asking for what was already sent, then silence

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY DAYS, ONE PROCEDURAL REPLY, ZERO TECHNICAL ANSWERS

Target	Amazon.com, Inc., Seattle, US / Amazon Europe Core S.a.r.l., Luxembourg
Product audited	Amazon Music for Android, com.amazon.mp3, v26.19.1
Disclosure reference	REF AMAZONMUSIC-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 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

1	Executive Summary	3
2	Subject & Operator Analysis	4
3	Positive Observations	4
4	Findings	4
4.1	C1: Hardcoded Firebase API key, pointed at an AWS Pinpoint marketing-analytics project	4
4.2	C2: CUSTOMER_ATTRIBUTE_SERVICE links music listening behavior to the amazon.com shopping profile	5
4.3	H1: AWS SDK: direct client-to-cloud API calls, undisclosed processor	5
4.4	H2: Alexa integration reports every playback event with no legal basis stated for non-Alexa users	6
4.5	H3: DETECT_SCREEN_CAPTURE: overbroad scope covering non-content screens	6
4.6	H4: BLUETOOTH_ADVERTISE: undisclosed BLE broadcast	7
5	Amazon's Response, Recorded in Full	7
6	Data Protection, Article by Article	8
7	Disclosure Timeline & Outcome	8
8	Residual Risk & Recommendations	9

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of the production Amazon Music Android application and identified six findings, two CRITICAL, four HIGH. The most significant: CUSTOMER_ATTRIBUTE_SERVICE, part of Amazon's Digital Commerce Platform, grants Amazon Music read access to the same central customer attribute store powering amazon.com personalization, purchase history, product category interests, Prime membership status, and demographic segments, linking music listening behavior directly to a user's shopping profile with no disclosed purpose or opt-out.

A hardcoded Firebase API key, pointed at an AWS Pinpoint marketing-analytics project, was also extracted from the production binary. Four further findings raise separate concerns: a 3,365-class AWS SDK enabling direct client-to-cloud API calls with no processor disclosure; Alexa integration reporting every playback event, play, pause, skip, seek, like, dislike, for users who never linked an Alexa device; an overly broad screenshot-detection permission covering non-content screens including account and billing; and undisclosed Bluetooth Low Energy broadcasting.

Eight written notices were sent over 90 days. Amazon's security team replied once, one month after R1, asking RFI-IRFOS to resend the full technical report, already delivered and acknowledged three weeks earlier. Three specific yes/no questions posed on 15 August, on credential rotation, Art. 13 disclosure, and a granular opt-out, were never answered. All six findings stand exactly as originally reported.

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

Disposition

R1 sent 21 June 2026 to privacy@amazon.com, bcc the Austrian DSB and CERT.at. Amazon's security team (vrp-researchers@amazon.com) replied once, one month later, asking for the full technical report to be resent, a report already delivered and acknowledged three weeks earlier. Four further written notices followed, including three specific yes/no questions on 15 August. None was ever answered.

ID	Severity	Title
C1	CRITICAL	Hardcoded Firebase API key, pointed at an AWS Pinpoint marketing-analytics project
C2	CRITICAL	CUSTOMER_ATTRIBUTE_SERVICE links music listening behavior to the amazon.com shopping profile
H1	HIGH	AWS SDK: direct client-to-cloud API calls, undisclosed processor
H2	HIGH	Alexa integration reports every playback event with no legal basis stated for non-Alexa users

ID	Severity	Title
H3	HIGH	DETECT_SCREEN_CAPTURE: overbroad scope covering non-content screens
H4	HIGH	BLUETOOTH_ADVERTISE: undisclosed BLE broadcast

Subject & Operator Analysis

Amazon.com, Inc. (Seattle, US) operates Amazon Music for a global subscriber base, with Amazon Europe Core S.a.r.l. (Luxembourg) referenced as the relevant EU entity and CNPD Luxembourg 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: Hardcoded Firebase API key, pointed at an AWS Pinpoint marketing-analytics project

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 the production binary. The project name, amazon-music-pinpoint, confirms an interface with AWS Pinpoint, Amazon's marketing-analytics and push platform.

```
API Key: AIzaSyCriuwxMKTst4Q9nQkoZzk0aHBupRIm7s8
Project: amazon-music-pinpoint
App ID: 1:799826913133:android:f5146ea01718e554
Bucket: amazon-music-pinpoint.appspot.com
```

No response was received naming this finding, including the direct question of whether the key has been rotated and restricted to the production certificate fingerprint. The key enables probing of the project, reading remote config including A/B test parameters, feature flags, and premium-conversion experiments, and accessing Firebase Storage.

Impact: A publicly extractable credential enables configuration probing and potential further access to Amazon's marketing-analytics infrastructure.

Fix: Rotate the key, restrict it to the production certificate fingerprint, and confirm the rotation in writing.

C2: CUSTOMER_ATTRIBUTE_SERVICE links music listening behavior to the amazon.com shopping profile

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

CUSTOMER_ATTRIBUTE_SERVICE, CAN_CALL_MAP_INFORMATION_PROVIDER, and CALL_AMAZON_DEVICE_INFORMATION_PROVIDER grant Amazon Music read access to Amazon's central customer attribute store, the same system powering amazon.com personalization.

No response was received naming this finding, including the direct question of whether this specific data flow is individually disclosed under Art. 13(1)(c) and whether a granular opt-out exists distinct from a blanket account-level setting. EntityTrackingIntentService routes every song, artist, album, and podcast interaction, played, skipped, liked, replayed, into Amazon's inter-app communication framework, while AmazonMusicMAPInformationProvider returns marketing identity attributes back to the wider Amazon ecosystem.

Impact: Music listening behavior is linked to a user's amazon.com purchase history, Prime membership status, and demographic segments, with no disclosed purpose limitation or opt-out specific to this data flow.

Fix: Disclose the CUSTOMER_ATTRIBUTE_SERVICE data flow explicitly under Art. 13(1)(c) and provide a granular opt-out for music-behavior-to-commerce-profile linkage.

H1: AWS SDK: direct client-to-cloud API calls, undisclosed processor

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

3,365 small classes enable direct client-to-AWS API calls (S3, Cognito, DynamoDB, Pinpoint), potentially bypassing API gateway mediation for behavioral telemetry.

No response was received naming this finding. AWS's role as primary processing infrastructure is not individually disclosed under Art. 13.

Impact: Behavioral telemetry may be written directly to cloud infrastructure with no disclosed processor relationship.

Fix: Disclose AWS as a data processor under Art. 13(1)(e) and confirm whether device-to-cloud calls bypass API gateway logging/mediation.

H2: Alexa integration reports every playback event with no legal basis stated for non-Alexa users

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

AlexaEMPPlaybackEventObserver reports every playback event, play, pause, skip, seek, like, dislike, to Alexa's ecosystem, and AlexaAwareMTSMetricsSender sends voice-aware metrics.

No response was received naming this finding. For users without an Alexa device who have not explicitly linked Amazon Music to Alexa, no legal basis is stated for routing playback events to Alexa infrastructure, potentially used for voice model training.

Impact: Playback behavior is routed to Alexa's ecosystem for users who never linked an Alexa device, with no disclosed legal basis for this specific data flow.

Fix: Confirm and disclose the Art. 6(1) legal basis for routing playback events to Alexa infrastructure independent of active Alexa device linkage.

H3: DETECT_SCREEN_CAPTURE: overbroad scope covering non-content screens

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

DETECT_SCREEN_CAPTURE notifies Amazon Music whenever a user screenshots while the app is foregrounded, including non-content screens such as account and billing.

No response was received naming this finding. A pattern of which screens a user screenshots is behavioral metadata requiring disclosure under Art. 13; RFI-IRFOS requested the scope be limited to DRM-protected content screens only.

Impact: Screenshot-detection metadata is collected app-wide, including on sensitive account and billing screens, beyond any DRM-protection purpose.

Fix: Limit DETECT_SCREEN_CAPTURE scope to DRM-protected content screens only, and disclose the collection under Art. 13.

H4: BLUETOOTH_ADVERTISE: undisclosed BLE broadcast

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

BLUETOOTH_ADVERTISE allows the app to actively broadcast BLE signals from the user's device, making it discoverable to nearby BLE scanners while the app runs, likely for Echo device pairing.

No response was received naming this finding.

Impact: A user's device becomes discoverable via BLE broadcast to nearby scanners with no disclosed scope of what is broadcast or to whom.

Fix: Disclose the BLE broadcast activity and its specific purpose under Art. 13(1)(c).

Amazon's Response, Recorded in Full

One month after R1, on 20 July 2026, Amazon's security team (vrp-researchers@amazon.com) replied, in full: "wir schreiben Ihnen vom Sicherheitsteam von Amazon... Wir können an keiner kostenpflichtigen Zusammenarbeit teilnehmen. Wir kaufen keine Sicherheitsberichte und gehen keine kostenpflichtigen Offenlegungsvereinbarungen ein. Wir würden es begrüßen, den vollständigen technischen Bericht, den Sie angeboten haben, zu erhalten... Bitte senden Sie uns den Bericht schriftlich zu, mit allen technischen Details zu jeder der sechs Feststellungen."

This asked for a full technical report already sent, and its receipt already acknowledged, three weeks earlier on 21-22 June. RFI-IRFOS clarified this the next day and restated all findings again in full. No further reply, technical or otherwise, was received from vrp-researchers@amazon.com or privacy@amazon.com across four subsequent written notices, including three specific yes/no questions posed on 15 August that were never answered.

Finding	Provision	Concern
---------	-----------	---------

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(1)(b)	Hardcoded, publicly extractable production credential
C2	GDPR Art. 5(1)(b), Art. 6(1)(b)/(f), Art. 13(1)(c), Art. 21	Undisclosed cross-service behavior-to-commerce linkage
H1	GDPR Art. 13(1)(e)	Undisclosed direct-to-cloud processing infrastructure
H2	GDPR Art. 6(1)	Undisclosed legal basis for playback data to Alexa
H3	GDPR Art. 13	Overbroad screenshot-detection scope
H4	GDPR Art. 13(1)(c)	Undisclosed BLE broadcast activity

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to privacy@amazon.com, bcc Austrian DSB/CERT.at, 6 findings
2026-06-27	Follow-up #1, deadline set for 29 June
2026-07-20	vrp-researchers@amazon.com replies, asks for the full report to be resent
2026-07-21	RFI-IRFOS clarifies the report was already sent and acknowledged; restates all findings
2026-08-05 / 08-15	Follow-ups; three specific yes/no questions posed 15 August, never answered
2026-08-29 / 09-04	Final follow-ups restate all findings; weekly SHA-256 re-pull instituted

Date	Event
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Eight written notices across 90 days produced one procedural reply asking for a report already delivered, and zero technical answers to any of the six findings or the three specific questions posed. All six findings stand exactly as originally reported.

Residual Risk & Recommendations

- Disclose the CUSTOMER_ATTRIBUTE_SERVICE music-to-commerce data flow explicitly and provide a granular opt-out; this is the single highest-priority item given the scale of cross-service profile linkage involved.
- Rotate the Firebase key and restrict it to the production certificate fingerprint.
- Disclose AWS as a processor and confirm the Art. 6(1) legal basis for playback data reaching Alexa infrastructure.
- Limit screenshot-detection scope to DRM-protected content and disclose BLE broadcast activity.
- Provide a substantive technical response to the three specific questions posed on 15 August, unanswered for over a month before the embargo closed.

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 Coordinated disclosure per ISO/IEC 29147. Research activity protected under Austria's Forschungsfreiheitsgesetz (Art. 17 StGG). GDPR Art. 5, 6, 13, 21, 32. REF AMAZONMUSIC-2026-R1.