



Coordinated Security & Privacy Disclosure, Final Report

Amazon Business for Android
(com.amazon.mShop.android.business.shopping)

B2B procurement app, live production credential, corporate purchasing data feeding a \$47B advertising platform, 75 days of total silence

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY DAYS, ZERO REPLIES OF ANY KIND

Target	Amazon Europe Core S.a.r.l., Luxembourg (lead supervisory authority: CNPD Luxembourg)
Product audited	Amazon Business for Android, com.amazon.mShop.android.business.shopping, v32.12.4.451
Disclosure reference	REF AMAZONBUSINESS-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 live 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, live Firebase API key in the production APK	4
4.2	C2: CUSTOMER_ATTRIBUTE_SERVICE routes B2B procurement data into Amazon's commerce and advertising profile	5
4.3	H1: WhisperJoin ultrasonic/BLE provisioning framework present in a B2B procurement app	5
4.4	H2: A9 Visual Search: camera-based product identification with undisclosed retention	6
4.5	H3: HIPAA-designated WebView interface for medical supply procurement, no identified EU legal basis	6
5	Data Protection, Article by Article	7
6	Disclosure Timeline & Outcome	7
7	Residual Risk & Recommendations	8

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of the production Amazon Business Android application, a B2B procurement app, and identified five findings, two CRITICAL, three HIGH. The most significant: a live, publicly extractable Firebase API key remains valid in every installed copy of the app, and CUSTOMER_ATTRIBUTE_SERVICE routes corporate procurement data, including spending patterns, supplier relationships, and contract-level pricing, into the same platform underlying Amazon's advertising business.

Three further findings raise questions specific to a B2B enterprise context: WhisperJoin, an ultrasonic/BLE provisioning framework built for Alexa device setup, ships inside a workplace procurement app; A9 Visual Search enables camera-based product identification that may inadvertently capture proprietary workplace environments; and a HIPAA-designated WebView interface handles medical supply procurement with no identified EU legal basis.

Five written notices were sent over 90 days. Not one produced a reply of any kind, substantive, automated, or a bounce. All five findings stand exactly as originally reported, including the live Firebase key, whose rotation status was never confirmed.

Scope: Static analysis of the publicly downloaded production Amazon Business 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. Four further written notices followed through 4 September 2026, cc amazon-privacy@amazon.com and press@amazon.com. No address in this thread has ever replied, not once, of any kind, substantive, automated, or a bounce.

ID	Severity	Title
C1	CRITICAL	Hardcoded, live Firebase API key in the production APK
C2	CRITICAL	CUSTOMER_ATTRIBUTE_SERVICE routes B2B procurement data into Amazon's commerce and advertising profile
H1	HIGH	WhisperJoin ultrasonic/BLE provisioning framework present in a B2B procurement app
H2	HIGH	A9 Visual Search: camera-based product identification with undisclosed retention
H3	HIGH	HIPAA-designated WebView interface for medical supply procurement, no identified EU legal basis

Subject & Operator Analysis

Amazon Europe Core S.a.r.l. operates Amazon Business, a B2B procurement platform used by corporate and institutional buyers across the EU, with the CNPD Luxembourg as its lead supervisory authority.

Positive Observations

- No cleartext HTTP traffic exceptions were identified in the network security configuration.
- No Chinese SDK dependencies were identified in the audited binary.

Findings

C1: Hardcoded, live Firebase API key in the production 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 the production binary and remains valid in every installed copy of the app.

```
API Key: AIzaSyDhjWoaUC1a09vuiQBv9L5wr_fY1tS8eik
Project: api-project-16912134167
App ID: 1:16912134167:android:adffc714890ada5ae6ec52
Bucket: api-project-16912134167.appspot.com
```

No response was received naming this finding, including the direct yes/no question of whether the key has been rotated. The key enables probing of the project, reading remote config including B2B pricing experiments and enterprise tier parameters, and accessing Firebase Storage, and cannot be rotated without shipping a new app release.

Impact: A live credential extractable from any downloaded APK enables probing of enterprise pricing configuration and further backend access, with no confirmed rotation across 90 days of notice.

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

C2: CUSTOMER_ATTRIBUTE_SERVICE routes B2B procurement data into Amazon's commerce and advertising 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 C_ALL_AMAZON_DEVICE_INFORMATION_PROVIDER grant Amazon Business read/write access to Amazon's central customer attribute store.

No response was received naming this finding. In a B2B context, this store contains corporate spending patterns, approved supplier relationships, employee purchasing behavior, business account tier, procurement category mix, and contract-level pricing. This data flows into the same platform powering Amazon DSP and Amazon Business's own sponsored product placements. For employees using one account for both personal and business purchases, procurement behavior also feeds their personal consumer profile via the same service.

Impact: Corporate procurement data, including contract-level pricing and supplier relationships, feeds an advertising and commerce profiling platform with no disclosed opt-out or purpose separation.

Fix: Disclose the CUSTOMER_ATTRIBUTE_SERVICE data flow explicitly under Art. 13(1)(c), provide an opt-out for procurement data feeding the commerce profile, and separate B2B and consumer profiles for shared-use accounts.

H1: WhisperJoin ultrasonic/BLE provisioning framework present in a B2B procurement app

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

1,587 smali classes for Amazon's WhisperJoin framework, originally built for Echo/Alexa device setup, ship inside the Amazon Business app, including active cryptographic channel establishment classes.

No response was received naming this finding. In enterprise environments such as conference rooms and executive offices, an app with active background ultrasonic provisioning capability raises corporate information-security questions independent of its original consumer use case.

Impact: An enterprise procurement app carries a device-pairing framework with no disclosed purpose in a B2B context, and its full data-transmission scope is not documented.

Fix: Disclose WhisperJoin's presence and scope under Art. 13(1)(c), or remove it if it serves no function in the B2B app.

H2: A9 Visual Search: camera-based product identification with undisclosed retention

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

2,141 small classes enable camera-based product identification, with all query images processed by A9's servers, an Amazon subsidiary in Seattle.

No response was received naming this finding. In a workplace context, camera use to identify a product may inadvertently capture proprietary workplace environments, competitor products in view, or supply-room inventories.

Impact: Workplace imagery captured for product identification is processed by a US subsidiary with no disclosed retention policy or confirmation of whether it is used for model training.

Fix: Disclose the image retention period and whether captured images are used for model training, under Art. 13(1)(c).

H3: HIPAA-designated WebView interface for medical supply procurement, no identified EU legal basis

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

HealthHIPAAWebViewDelegate, HealthHIPAAWebViewClient, and HealthHIPAAWebChromeClient classes implement a HIPAA-designated interface for medical/health supply procurement.

No response was received naming this finding. For European healthcare employers purchasing medical supplies through Amazon Business, procurement patterns, which medical products, which quantities, which departments, may constitute health-adjacent data under GDPR Art. 9. No EU legal basis or Art. 13 disclosure was identified for this specific processing.

Impact: Health-adjacent procurement data from European healthcare purchasers is processed through a US-designed HIPAA interface with no identified GDPR Art. 9 legal basis.

Fix: Publish the Art. 9(2) legal basis relied upon for EU healthcare procurement data, or exclude EU accounts from this processing path.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32	Live, publicly extractable production credential
C2	GDPR Art. 5(1)(b), Art. 6(1)(b), Art. 13(1)(c), Art. 21	Cross-purpose procurement-to-advertising data flow
H1	GDPR Art. 13(1)(c)	Undisclosed device-pairing framework in enterprise context
H2	GDPR Art. 13(1)(c)	Undisclosed image retention for camera-based product ID
H3	GDPR Art. 9	Health-adjacent procurement data, no identified legal basis

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to privacy@amazon.com, bcc Austrian DSB/CERT.at, 5 findings
2026-06-27	First follow-up, cc amazon-privacy@amazon.com and press@amazon.com added
2026-08-09	Second follow-up, standardized three-questions format introduced
2026-08-24	Third follow-up, Art. 33(4) 72-hour notification clock argument invoked
2026-09-04	Fourth follow-up, restates C1/C2 in full, weekly SHA-256 re-pull instituted to catch a silent fix
2026-09-19	Embargo closes and this report publishes

Five written notices across 90 days produced zero replies of any kind from any address used in this case. All five findings, including a live production credential and a corporate-to-advertising data flow, stand exactly as originally reported.

Residual Risk & Recommendations

- Rotate the live Firebase credential and confirm rotation in writing; this is the single highest-priority item given its confirmed live status across 90 days.
 - Disclose the CUSTOMER_ATTRIBUTE_SERVICE data flow and provide an opt-out for procurement data feeding the commerce/advertising profile.
 - Publish the Art. 9(2) legal basis for health-adjacent procurement data or exclude EU healthcare accounts from that processing path.
 - Disclose WhisperJoin and A9 Visual Search's actual scope and retention in the B2B context.
 - Establish any working reply path at all: five written notices over 90 days received zero acknowledgment of any kind.
-

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, 9, 13, 21, 32. REF AMAZONBUSINESS-2026-R1.