Coordinated Security & Privacy Disclosure, Final Report

SoundCloud for Android (com.soundcloud.android, v2026.06.10-release)

Ten written notices, ninety-one days, two dead mailboxes, zero replies of any kind

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL EIGHT FINDINGS UNADDRESSED AFTER TEN NOTICES

Target	SoundCloud Group GmbH, Alexanderufer 26, 10117 Berlin, Germany
Product audited	SoundCloud for Android, com.soundcloud.android, v2026.06.10-release (versionCode 359050, minSdk 32/targetSdk 36)
Disclosure reference	REF SOUNDCLOUD-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2 Network Security Config permitting cleartext traffic for every domain except soundcloud.com itself, CVSS v4.0 8.6, unaddressed)

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 SoundCloud Android application and identified two CRITICAL and six HIGH findings: seven hardcoded production credentials in a single strings.xml file, a Firebase API key, a MoEngage workspace key, an AppsFlyer developer key, two simultaneously active Segment write keys, a Sentry DSN, and a DataDome client key, a Network Security Configuration whose base configuration permits cleartext traffic for every domain except soundcloud.com itself, meaning all traffic to MoEngage, Segment, AppsFlyer, Comscore, Facebook Audience Network, Amazon Publisher Services, Sentry, and DataDome can run unencrypted, a 3,515-class Facebook Audience Network integration receiving listening behavior with Meta not individually named as a recipient, a 1,991-class MoEngage CRM integration with a hardcoded, publicly extractable workspace key and a debug validator UI left in the production build, a Segment customer-data-platform integration running two write keys simultaneously mid-migration with unclear downstream vendor status on the legacy pipeline, a 135-class Comscore audience-measurement integration, a 159-class Amazon Publisher Services ad integration, neither disclosed as a recipient, and a Telescope debug screen-capture tool left active in the production build.

Across ten written notices over ninety-one days, cc'd or bcc'd throughout to the Austrian Datenschutzbehoerde, CERT.at, and Berlin's data protection authority as SoundCloud's lead supervisory authority, no message from any @soundcloud.com address was ever received. presse@soundcloud.com and privacy@support.soundcloud.com bounced on every attempt across the case; the only inbound mail in either thread was mailer-daemon delivery-failure notifications. No reply of any kind, human or automated, ever came from dataprotection@soundcloud.com itself.

Scope: Static analysis of the publicly downloaded production SoundCloud Android APK (v2026.06.10-release), on an authorized test device, only. No SoundCloud account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 20 June 2026 to dataprotection@soundcloud.com, cc privacy@soundcloud.com and presse@soundcloud.com, bcc/cc the Austrian Datenschutzbehoerde, CERT.at, and Berlin's data protection authority (BlnBDI, SoundCloud's lead supervisory authority). presse@soundcloud.com and privacy@support.soundcloud.com bounced on every attempt. Across ten written notices over ninety-one days, no message from any @soundcloud.com address was ever received; the only inbound mail was mailer-daemon bounce notifications.

ID	Severity	Title
C1	CRITICAL	Seven hardcoded production credentials in a single strings.xml
C2	CRITICAL	Network Security Config permits cleartext traffic for every domain except soundcloud.com

ID	Severity	Title
H1	HIGH	Facebook Audience Network (3,515 classes)
H2	HIGH	MoEngage CRM (1,991 classes), hardcoded key, debug validator left in production
H3	HIGH	Segment CDP – two simultaneously active write keys mid-migration
H4	HIGH	Comscore Streaming (135 classes)
H5	HIGH	Amazon Publisher Services (159 classes)
H6	HIGH	Telescope debug screen-capture tool active in the production build

Subject & Operator Analysis

SoundCloud Group GmbH is headquartered at Alexanderufer 26, 10117 Berlin, Germany. Berlin's data protection authority (BInBDI) is SoundCloud's lead supervisory authority under GDPR one-stop-shop rules.

Findings

C1: Seven hardcoded production credentials in a single strings.xml

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

res/values/strings.xml contains, in plaintext: a Firebase API key (AIzaSyAdgWP9wC36Ays-Gr3cB9o-Rxyi6KRbF4Q, project soundcloud.com:soundcloud), a MoEngage workspace key, an AppsFlyer developer key, two simultaneously active Segment write keys (a new and a legacy key), a Sentry DSN, and a DataDome client key, all extractable from any Play Store APK in under 60 seconds.

No reply of any kind addressed this finding across ten notices.

Impact: Seven separate vendor integrations' attack surfaces cannot be independently ruled safe from outside each vendor's own console once their keys ship in every installed client.

Fix: Rotate all seven exposed credentials and confirm each vendor project's access controls are deny-by-default.

C2: Network Security Config permits cleartext traffic for every domain except soundcloud.com

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

The base configuration declares cleartextTrafficPermitted=true, with soundcloud.com itself as the only domain-level exception. All SDK traffic to MoEngage, Segment, AppsFlyer, Comscore, Facebook Audience Network, Amazon Publisher Services, Sentry, and DataDome can run over unencrypted HTTP.

No reply of any kind addressed this finding.

Impact: Traffic to eight separate third-party vendors can be intercepted or altered on any untrusted network, while the app's own first-party domain is separately protected.

Fix: Set cleartextTrafficPermitted=false as the base configuration and add explicit exceptions only where genuinely required.

H1: Facebook Audience Network (3,515 classes)

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/facebook/ads/ is present with 3,515 smali classes; Meta receives genre, time-of-day listening behavior, playback duration, artist preferences, and engagement frequency. Meta is not individually named as a recipient in the privacy policy.

No reply of any kind addressed this finding.

Impact: Detailed listening-behavior data is transmitted to a named third party with no matching Art. 13(1)(e) disclosure of that specific recipient.

Fix: Name Meta explicitly as a recipient of listening-behavior data in the privacy policy.

H2: MoEngage CRM (1,991 classes), hardcoded key, debug validator left in production

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

MoEngage receives play events, track engagement, skip patterns, and session frequency for targeted push campaigns. Its workspace key is hardcoded and publicly extractable, and a 'MoEngage Validator' debug UI was left in the production build.

No reply of any kind addressed this finding.

Impact: A debug diagnostic surface intended for development remains reachable in the production app alongside an exposed workspace credential.

Fix: Remove the MoEngage Validator debug UI from production builds and rotate the exposed workspace key.

H3: Segment CDP – two simultaneously active write keys mid-migration

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

528 classes are present, and the internal label event_logger_monitor_legacy_segment_switch confirms an ongoing migration during which both a legacy and a new Segment write key remain simultaneously active. Downstream vendor status on the legacy pipeline, and whether those vendors remain under contract, is unclear from static analysis.

No reply of any kind addressed this finding.

Impact: Data may continue flowing to legacy downstream vendors whose contractual status cannot be confirmed externally.

Fix: Complete the Segment migration and retire the legacy write key, confirming which downstream vendors remain under an active agreement.

H4: Comscore Streaming (135 classes)

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

Comscore (Reston, Virginia, USA) receives listening duration, content metadata, and device identifiers for syndicated industry audience-reach measurement; not individually disclosed as a recipient.

No reply of any kind addressed this finding.

Impact: Listening data is transmitted to an undisclosed third-party audience-measurement vendor.

Fix: Name Comscore explicitly as a recipient of listening and device-identifier data.

H5: Amazon Publisher Services (159 classes)

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

A third ad network, alongside Meta and Comscore, sends listening behavior to Amazon Ads (Seattle, USA) for ad optimization; not disclosed.

No reply of any kind addressed this finding.

Impact: Listening behavior is transmitted to a third undisclosed advertising recipient.

Fix: Name Amazon Publisher Services explicitly as a recipient of listening-behavior data.

H6: Telescope debug screen-capture tool active in the production build

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

31 classes (TelescopeLayout, RequestCaptureActivity, MediaProjectionCallback) plus a declared FOREGROUND_SERVICE_MEDIA_PROJECTION permission remain in the production build, the same debug-tool-left-in-production pattern previously identified in the Oesterreichische Lotterien case (Facebook Flipper) and the Klarna case (Chucker).

No reply of any kind addressed this finding.

Impact: A screen-capture debug tool intended for development remains reachable in the shipped production app.

Fix: Strip the Telescope debug tool and its associated permission from production release builds.

Ten Notices, Two Dead Mailboxes, Zero Replies

presse@soundcloud.com and privacy@support.soundcloud.com bounced on every single attempt across this case's ten written notices and ninety-one days. No message from any @soundcloud.com address, automated or otherwise, was ever received; the only inbound mail in either correspondence thread was mailer-daemon delivery-failure notifications.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 25(1), Art. 32(1)(b)	Seven hardcoded vendor credentials in the production APK
C2	GDPR Art. 32(1)(a)	Cleartext traffic permitted to eight third-party vendors
H1	GDPR Art. 13(1)(e)(f)	Undisclosed Facebook Audience Network recipient
H2	GDPR Art. 32	Debug diagnostic UI reachable in production alongside an exposed credential
H3	GDPR Art. 28	Unclear downstream vendor status on a legacy data pipeline
H4	GDPR Art. 13(1)(e)(f)	Undisclosed Comscore recipient
H5	GDPR Art. 13(1)(e)(f)	Undisclosed Amazon Publisher Services recipient
H6	GDPR Art. 32	Screen-capture debug tool active in the production build

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to dataprotection@soundcloud.com, cc privacy@soundcloud.com; bcc Austrian DSB/CERT.at/BlnBDI; 2 CRITICAL + 6 HIGH findings; a EUR 75,000 NDA remediation engagement was offered under the R1 policy then in force – historical record only, not a currently open offer; presse@soundcloud.com and privacy@support.soundcloud.com bounce
2026-06-27	Seven-day follow-up sets a new deadline of 29 June 18:00; both alternate addresses bounce again
2026-06-28	Follow-up restates all 7 hardcoded credentials, screen capture, and the Facebook Audience Network finding
2026-08-18	Three messages sent the same morning: a deadline reminder, an embargo restatement, and a clarification of the binding 19 September date; each accompanied by a matching bounce
2026-09-12	Follow-up, day 84, seven messages, zero replies; matching bounce
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Establish a functioning privacy or press contact address, given both alternate channels bounced throughout this case.
- Set cleartextTrafficPermitted=false as the base Network Security Config and add exceptions only where required.
- Rotate all seven exposed vendor credentials.
- Name Meta, Comscore, and Amazon Publisher Services explicitly as recipients of listening-behavior data.
- Strip the Telescope debug screen-capture tool from production release builds.

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. GDPR Art. 13, 25, 28, 32. REF SOUNDCLOUD-2026-R1.