Coordinated Security & Privacy Disclosure, Final Report

Netflix for Android (com.netflix.mediaclient)

Streaming platform, Netflix Games voice chat and camera access, six identical automated replies

PUBLIC DISCLOSURE, 18 SEPTEMBER 2026 – NINETY DAYS, SIX AUTOMATED REPLIES, NO HUMAN EVER

Target	Netflix, Inc., Los Gatos, California, US
Product audited	Netflix for Android, com.netflix.mediaclient, v9.70.1, build 7
Disclosure reference	REF NETFLIX-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-18
Report published	2026-09-19
Severity	CRITICAL (C2 voice chat / H2 camera, CVSS v4.0 8.7 High)

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 Netflix Android application and identified seven findings, two CRITICAL, five HIGH. The most significant: Netflix Games ships a complete real-time voice chat engine, backed by a FOREGROUND_SERVICE_MICROPHONE declaration allowing the microphone to run in the background, with no confirmed exclusion for sessions running under a Kids Profile, despite the app tracking Kids Profile state across 645 smali files.

Separately, a Facebook client-style Firebase credential using the api-project- naming convention, a scheme Google retired around 2016, remains hardcoded and unrotated in the production binary, suggesting close to a decade of continuous, unrotated production use. A camera permission is accessed via a WebChromeClient inside Netflix Games with no clear disclosure that children playing these games may have camera access invoked as part of gameplay.

Seven written notices were sent to privacy@netflix.com over 90 days. Six produced the identical automated Zendesk notice, simply forwarding RFI-IRFOS's own message back within seconds, never a substantive human reply. press@netflix.com hard-bounced partway through the correspondence and was removed from the thread. All seven findings stand exactly as originally reported.

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

Disposition

R1 sent 20 June 2026 to privacy@netflix.com, bcc the Dutch Autoriteit Persoonsgegevens, Austrian DSB, and CERT.at. Six further written notices followed through 31 August 2026. Every single reply received, six in total, was the identical automated Zendesk mailbox notice from privacy@legal.netflix.com, in each case simply forwarding RFI-IRFOS's own message back, arriving within seconds of sending. No human ever answered. press@netflix.com hard-bounced on 15 August 2026 and was removed from the thread.

ID	Severity	Title
C1	CRITICAL	Hardcoded Firebase credential using a naming convention retired circa 2016, unrotated for approximately a decade
C2	CRITICAL	Netflix Games: complete voice chat engine with a background microphone service, Kids Profile exclusion not confirmed
H1	HIGH	POST_PROMOTED_NOTIFICATIONS: an advertising push channel on a paid subscription service
H2	HIGH	Undisclosed camera access in Netflix Games via WebChromeClient

ID	Severity	Title
H3	HIGH	Bugsnag crash reporting: session data to US third-party infrastructure
H4	HIGH	Advertising ID collected with no confirmed Kids Profile exclusion
H5	HIGH	Legacy permissions with no disclosed current use case

Subject & Operator Analysis

Netflix, Inc. (Los Gatos, California) operates the audited application for a subscriber base publicly reported at over 300 million accounts globally, a meaningful share of which include Kids Profiles used by children.

Positive Observations

- minSdk 28 (Android 9, 2018) is more defensible than the industry average in RFI-IRFOS's audit series; most streaming competitors target Android 5-6.
- No cleartext HTTP exceptions in the network security configuration.
- No Chinese SDK dependencies identified.
- compileSdk 36 is current.
- The Kids Profile state machine (account_profile_state_is_kids_profile) is architecturally present across 645 smali files, showing clear, deliberate engineering intent to differentiate children's sessions, even where specific services (C2, H4) do not appear to act on that state.
- No Facebook advertising SDK identified.

Findings

C1: Hardcoded Firebase credential using a naming convention retired circa 2016, unrotated for approximately a decade

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

res/values/strings.xml contains API key AIzaSyCMgAVw3DCCsxEagIOr-X8pUyINcvZTQi0, project api-project-484286080282, a naming scheme Google retired when Firebase rebranded its console circa 2015-2016.

```
API Key:  AIzaSyCMgAVw3DCCsxEagIOr-X8pUyINcvZTQi0
DB URL:   https://api-project-484286080282.firebaseio.com
Bucket:   api-project-484286080282.appspot.com
Project:  api-project-484286080282
```

No response was received naming this finding, including the direct yes/no question of whether this credential has been rotated since 20 June 2026 and when it was first issued. The naming convention alone suggests continuous production use for approximately ten years without rotation.

Impact: A credential extractable from any downloaded APK in under 60 seconds enables FCM probing and potential further backend access, regardless of its exact age, which itself remains unconfirmed by Netflix.

Fix: Rotate the credential, confirm and disclose its actual issue date, and restrict it to the production certificate fingerprint.

C2: Netflix Games: complete voice chat engine with a background microphone service, Kids Profile exclusion not confirmed

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 complete real-time voice chat system (VoiceChat, VoiceChatViewModel, VoiceChatJsBridge, joinChannel, leaveChannel, VOICE_TOKEN) runs as a foreground microphone service. The app tracks Kids Profile state via account_profile_state_is_kids_profile, present in 645 smali files, but no confirmed exclusion of the voice chat microphone service for Kids Profile sessions exists.

No response was received naming this finding, including the direct yes/no question of whether the voice chat microphone service is excluded from Kids Profile sessions. COPPA (16 CFR 312.2) classifies voice recordings from children under 13 as personal information requiring verifiable parental consent, and GDPR Art. 8(1) requires parental consent for processing children's data. A foreground microphone service with no confirmed exclusion for children's profiles is a direct exposure on both frameworks. RFI-IRFOS credits that the Kids Profile state machine is clearly, deliberately engineered across the codebase; the finding is that this specific service does not appear to check it.

Impact: Children using Kids Profiles on a platform with over 300 million subscribers may have background microphone access active during Netflix Games sessions with no confirmed age-appropriate exclusion.

Fix: Confirm and enforce exclusion of FOREGROUND_SERVICE_MICROPHONE for all sessions running under a Kids Profile, and publish the Art. 35 DPIA covering this feature.

H1: POST_PROMOTED_NOTIFICATIONS: an advertising push channel on a paid subscription service

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

A system-level permission for privileged promotional notification delivery is declared.

No response was received naming this finding. Subscribers paying for ad-free tiers have a reasonable expectation that a privileged promotional notification channel is not present in their app.

Impact: Users on paid, ad-free subscription tiers may receive privileged promotional notifications inconsistent with what they are paying for.

Fix: Scope POST_PROMOTED_NOTIFICATIONS away from ad-free subscription tiers, or disclose its actual use case clearly.

H2: Undisclosed camera access in Netflix Games via WebChromeClient

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

CAMERA permission is accessed via GameControllerWebChromeClient inside the MSSI game framework.

No response was received naming this finding. Children playing Netflix Games may have camera access invoked as part of gameplay with no clear disclosure or parental notice at the point of use.

Impact: Camera access during children's gameplay sessions occurs with no clear point-of-use disclosure to a parent or guardian.

Fix: Add explicit, parent-facing disclosure at the point any Netflix Games title requests camera access, independent of the general app permission grant.

H3: Bugsnag crash reporting: session data to US third-party infrastructure

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

com.bugsnag.android transmits crash reports, device state, and session breadcrumbs to Bugsnag's US infrastructure, with no EU transfer mechanism disclosed at the app level.

No response was received naming this finding.

Impact: Device state and session data are transmitted to a US third party with no disclosed transfer safeguard.

Fix: Disclose Bugsnag as a data recipient under Art. 13(1)(e) and publish the applicable Art. 44-49 transfer mechanism.

H4: Advertising ID collected with no confirmed Kids Profile exclusion

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

com.google.android.gms.permission.AD_ID is declared. The Kids Profile state key exists in 645 smali files, but no confirmed programmatic advertising ID suppression for children's sessions was found.

No response was received naming this finding.

Impact: Advertising identifiers may be collected during children's Kids Profile sessions with no confirmed suppression mechanism.

Fix: Confirm and enforce AD_ID suppression for all sessions running under a Kids Profile.

H5: Legacy permissions with no disclosed current use case

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

WRITE_EXTERNAL_STORAGE, superseded by scoped storage on Android 10 and later, and MANAGE_OWN_CALLS, granting telecom call-stack access, are both declared with no disclosed streaming use case.

No response was received naming this finding.

Impact: Legacy and telecom-adjacent permissions persist with no apparent connection to the app's core streaming function.

Fix: Remove both permissions unless a specific, currently-active feature requires each individually.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 25, Art. 32	Near-decade-old unrotated credential
C2	GDPR Art. 6(1), Art. 8; COPPA 16 CFR 312.2	Background microphone service, no confirmed Kids Profile exclusion
H1	Consumer expectation, ad-free tier	Privileged promotional notification channel
H2	Parental notice	Undisclosed camera access during children's gameplay
H3	GDPR Art. 13(1)(e), Art. 44-49	Undisclosed US third-party data recipient
H4	GDPR Art. 8	Advertising ID, no confirmed Kids Profile suppression
H5	GDPR Art. 5(1)(c)	Legacy permissions with no disclosed use case

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to privacy@netflix.com, bcc Dutch AP/Austrian DSB/CERT.at, 7 findings
2026-06-27 / 07-23 / 08-04	Follow-ups; each produces the identical automated Zendesk notice, forwarding our own message back within seconds
2026-08-15	press@netflix.com hard-bounces and is removed from the thread; sixth automated notice received
2026-08-18	Follow-up sets a 25 August deadline for a substantive human answer to three questions
2026-08-31	25 August deadline passed; final follow-up restates the record, seventh message, seventh identical automated reply
2026-09-18	Embargo, as actually communicated to Netflix, closes
2026-09-19	This report publishes

Seven written notices across 90 days produced seven identical automated Zendesk notices, each one simply Netflix's own ticketing system forwarding RFI-IRFOS's message back within seconds, never a substantive human reply. All seven findings, including a background microphone service with no confirmed children's exclusion on a platform serving over 300 million subscribers, stand exactly as originally reported.

Residual Risk & Recommendations

- Confirm and enforce Kids Profile exclusion for the Netflix Games voice chat microphone service; this is the single highest-priority item given the direct child-safety and COPPA/Art. 8 exposure.
- Rotate the near-decade-old Firebase credential and confirm its actual issue date.
- Add explicit parental disclosure for camera access invoked during Netflix Games sessions.
- Confirm AD_ID suppression for Kids Profile sessions.
- Disclose Bugsnag as a data recipient and publish its transfer mechanism.
- Remove legacy permissions with no current disclosed use case.
- Establish a working substantive-reply path independent of the automated Zendesk mailbox, which produced seven identical automated forwards across 90 days rather than any human engagement.

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. 6, 8, 25, 32, 33, 35, 44-49. REF NETFLIX-2026-R1.