Coordinated Security & Privacy Disclosure, Final Report

Disney+ for Android (com.disney.disneyplus)

Streaming platform, children's physical location tracking via Braze geofencing, zero replies in 91 days

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

Target	The Walt Disney Company, Burbank, California, US
Product audited	Disney+ for Android, com.disney.disneyplus, v26.10.0+rc3-2026.06.13
Disclosure reference	REF DISNEY-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2 Braze geofencing on children, 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 Disney+ Android application and identified eight findings, two CRITICAL, six HIGH. The most significant: the Braze Geofence Manager collects precise GPS coordinates to trigger marketing campaigns app-wide, and no code path was found that excludes this from Kids Profiles, despite Kids Profile infrastructure being clearly and deliberately engineered across 114+ smali files.

Separately, two Firebase API keys are hardcoded in the production binary, one pointing to an internal infrastructure project, disneyplus-internal, not the public-facing production project. Both were extracted verbatim from the public Play Store APK in under 60 seconds.

Two written notices were sent to privacycontact@twdc.com over 91 days. Not one produced a reply of any kind, substantive, automated, or a bounce. All eight findings stand exactly as originally reported.

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

Disposition

R1 sent 20 June 2026 to privacycontact@twdc.com, bcc the Irish DPC, Austrian DSB, and CERT.at. One further written notice followed on 4 September 2026. No acknowledgment, automated or otherwise, has ever arrived on this thread. Both findings and the full text of both messages stand unanswered.

ID	Severity	Title
C1	CRITICAL	Two Firebase API keys hardcoded in the production APK, including an internal infrastructure project
C2	CRITICAL	Braze Geofence Manager collects precise physical location app-wide, no confirmed Kids Profile exclusion
H1	HIGH	Advertising ID collected app-wide, no confirmed Kids Profile exclusion
H2	HIGH	Samsung Maps attribution: undisclosed cross-platform tracking
H3	HIGH	”Darkwing Duck” pre-install attribution: undisclosed manufacturer tracking
H4	HIGH	Conviva video analytics: children’s viewing behaviour to a US third party
H5	HIGH	DataDog RUM: session monitoring to US infrastructure
H6	HIGH	minSdk 23 (Android 6.0, 2015): a children’s platform supporting 11-year-old, unpatched devices

Subject & Operator Analysis

The Walt Disney Company (Burbank, California) operates Disney+ for a subscriber base whose brand identity is built specifically on family and children's trust, a meaningful share of whom use Kids Profiles.

Positive Observations

- compileSdk 36 (Android 16) is fully current.
- No cleartext HTTP traffic exceptions in the network security configuration.
- No Facebook advertising SDK identified.
- OneTrust consent management is integrated (434 classes).
- Kids Profile infrastructure is architecturally present and referenced across 114+ smali files, showing clear, deliberate engineering intent to differentiate children's sessions, even where specific services (C2, H1) do not appear to act on that state.

Findings

C1: Two Firebase API keys hardcoded in the production APK, including an internal infrastructure 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

res/values/strings.xml and the APK binary strings contain two complete Firebase project configurations, extracted verbatim in under 60 seconds from the public Play Store binary.

```
Project 1 (Production):
  Project ID: disneyplus-42214
  API Key:    AIzaSyCK3NBrHlmIPM0HlXvJvmi0u4tIlltI4qI
  App ID:     1:802476044819:android:4e4be59c91551f01
  DB URL:     https://disneyplus-42214.firebaseio.com

Project 2 (Internal, shipped in production binary):
  Project ID: disneyplus-internal
  API Key:    AIzaSyCpNUlLEyCK-JRSGl-CZp0aSuIXqKpi3JI
  App ID:     1:386345974412:android:6abddbbe01d9da880959a9
  DB URL:     https://disneyplus-internal.firebaseio.com
```

No response was received naming this finding, including whether either key has been rotated since 20 June 2026 or why an internal infrastructure project ships inside the public production binary.

Impact: Credentials extractable from any downloaded APK in under a minute enable FCM

probing, quota exhaustion, and potential further backend access to internal infrastructure, regardless of Disney's own confirmation of scope.

Fix: Rotate both credentials, remove the internal project reference from the production binary entirely, and restrict remaining keys to the production certificate fingerprint.

C2: Braze Geofence Manager collects precise physical location app-wide, no confirmed Kids Profile exclusion

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

355 Braze smali classes, including BrazeGeofenceManager, run alongside ACCESS_FINE_LOCATION. 114 smali files reference age-gated/Kids Profile state (account_profile_state_is_kids_profile, AGE_GATED, KidsProfile, JuniorMode, ParentalControl), but no programmatic exclusion of BrazeGeofenceManager for Kids Profile sessions was found.

```
com/braze/managers/BrazeGeofenceManager.smali
com/braze/managers/BrazeGeofenceManager$Companion.smali
com/braze/configuration/BrazeConfigurationProvider.smali
com/braze/push/BrazeFirebaseMessagingService.smali

Manifest: <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
```

No response was received naming this finding. A child using a Kids Profile on a shared family tablet has their precise GPS coordinates registered against commercial marketing geofences, a Disney Store, a cinema showing a new release, the same way an adult subscriber does. RFI-IRFOS credits that the Kids Profile state machine is clearly, deliberately engineered across 114+ smali files; the finding is that Braze geofencing does not appear to check it.

Impact: Children in Kids Profiles may have their real-world location tracked for marketing purposes with no confirmed age-appropriate exclusion, engaging GDPR Art. 8.

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

H1: Advertising ID collected app-wide, no confirmed Kids Profile exclusion

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.google.android.gms.permission.AD_ID is declared. 25 smali files reference the advertising ID, with no confirmed programmatic exclusion for children's sessions.

No response was received naming this finding.

Impact: Persistent advertising identifiers may be collected during children's Kids Profile sessions with no confirmed suppression mechanism, enabling cross-app profiling of a child.

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

H2: Samsung Maps attribution: undisclosed cross-platform tracking

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

The BAMTech Dominguez platform includes a MapsModel integration correlating Samsung Maps usage with Disney+ subscription events. This correlation is not disclosed to users.

No response was received naming this finding.

Impact: Cross-platform behavioral correlation between a third-party mapping app and subscription events occurs without user-facing disclosure.

Fix: Disclose the Samsung Maps correlation as a data-sharing arrangement under Art. 13(1)(e), or remove it.

H3: "Darkwing Duck" pre-install attribution: undisclosed manufacturer tracking

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

A DarkwingDataModel component paired with the REQUEST_PRELOAD_INFORMATION permission attributes pre-install revenue-share deals from first launch, meaning a pre-installed device is tracked for attribution from the moment it is first turned on.

No response was received naming this finding. A device pre-installed with Disney+, including a device gifted to or used by a child, is attributed for revenue-share purposes from first launch, before any account is created or consent flow is shown.

Impact: Pre-install attribution tracking begins before any user-facing consent mechanism runs, including on devices used by children.

Fix: Disclose the pre-install attribution mechanism and its manufacturer revenue-share counterpart under Art. 13(1)(e), and confirm it does not fire before consent is obtained.

H4: Conviva video analytics: children's viewing behaviour to a US third party

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

cws.conviva.com and pings.conviva.com receive content-watched telemetry, including ad-tier eligibility signals, for all sessions including Kids Profile sessions.

No response was received naming this finding.

Impact: Viewing behaviour data from children's sessions is transmitted to US analytics infrastructure with no disclosed Art. 44-49 transfer mechanism at the app level.

Fix: Disclose Conviva as a data recipient under Art. 13(1)(e) and publish the applicable transfer mechanism, with specific confirmation for Kids Profile sessions.

H5: DataDog RUM: session monitoring to US infrastructure

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

com.datadog.android.rum and its NDK component transmit action traces, A/B test feature-flag evaluations, and session data to Datadog's US infrastructure, with no disclosed EU transfer mechanism at the app level.

No response was received naming this finding.

Impact: Session and behavioral data is transmitted to a US third party with no disclosed transfer safeguard.

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

H6: minSdk 23 (Android 6.0, 2015): a children's platform supporting 11-year-old, unpatched devices

MEDIUM, CVSS v4.0 AV:P/AC:H/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N, 5.4

The app declares minSdk 23. Android 6 devices have received no Google security patches since 2019.

No response was received naming this finding. A children's entertainment platform supporting devices with no security patches in over six years represents disproportionate exposure for a vulnerable audience, independent of any single vulnerability.

Impact: Users, disproportionately including children on hand-me-down family devices, run the application on platforms with no current security patches.

Fix: Raise minSdk to a currently-patched Android baseline, or publish a documented risk acceptance specific to the children's-audience context.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32	Hardcoded production and internal-infrastructure credentials
C2	GDPR Art. 8, Art. 35	Physical location tracking, no confirmed Kids Profile exclusion
H1	GDPR Art. 8	Advertising ID, no confirmed Kids Profile suppression
H2	GDPR Art. 13(1)(e)	Undisclosed cross-platform correlation
H3	GDPR Art. 13(1)(e)	Pre-install attribution before consent
H4	GDPR Art. 13(1)(e), Art. 44-49	Undisclosed US third-party data recipient, children's viewing data
H5	GDPR Art. 13(1)(e), Art. 44-49	Undisclosed US third-party data recipient
H6	GDPR Art. 5(1)(f), Art. 32	Eleven-year-old unpatched platform baseline

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to privacycontact@twdc.com , bcc Irish DPC/Austrian DSB/CERT.at, 8 findings
2026-09-04	First and only follow-up; still zero acknowledgment of any kind
2026-09-19	Embargo closes and this report publishes

Two written notices across 91 days produced no reply of any kind, not a substantive answer, not an automated acknowledgment, not even a bounce. All eight findings, including a physical location tracking system with no confirmed exclusion for children on a platform whose brand identity is built on family trust, stand exactly as originally reported.

Residual Risk & Recommendations

- Confirm and enforce Kids Profile exclusion for Braze Geofence Manager; this is the single highest-priority item given the direct child-safety and Art. 8 exposure.
- Rotate both Firebase credentials and remove the internal infrastructure project from the production binary.
- Confirm AD_ID suppression for Kids Profile sessions.
- Disclose Samsung Maps correlation, pre-install attribution, Conviva, and Datadog as data recipients with their respective transfer mechanisms.
- Raise minSdk from Android 6.0 or publish a documented risk acceptance specific to the children's-audience context.
- Establish any working reply path at all: two written notices across 91 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, 8, 13, 25, 32, 35, 44-49. REF DISNEY-2026-R1.