



Coordinated Security & Privacy Disclosure, Final Report

Max for Android (com.wbd.stream, v7.4.0.55)

Four written notices, ninety days, two permanently dead mailboxes, zero replies of any kind

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL SIX FINDINGS UNADDRESSED AFTER FOUR NOTICES

Target	Warner Bros. Discovery (WBD)
Product audited	Max for Android, com.wbd.stream, v7.4.0.55
Disclosure reference	REF WBDMAX-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2 an Apptentive SDK activity overriding both the application-level and Network Security Config cleartext prohibitions, 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

1	Executive Summary	3
2	Subject & Operator Analysis	4
3	Findings	4
3.1	C1: Firebase API key hardcoded in the production APK	4
3.2	C2: Apptentive SDK activity overrides both the manifest and Network Security Config cleartext prohibitions	5
3.3	H1: Braze behavioral marketing registered app-wide alongside Max Kids with no confirmed gating	5
3.4	H2: Nielsen DCR and Comscore – dual audience measurement with device ID collection, including on the ad-free tier	6
3.5	H3: AppsFlyer routes individual subscriber lifetime-value data to US adtech	6
3.6	H4: Pending Paramount acquisition creates an unresolved Art. 14 controller-change notification obligation	7
4	Two Dead Mailboxes, Four Notices, Zero Replies	7
5	Data Protection, Article by Article	8
6	Disclosure Timeline & Outcome	8
7	Residual Risk & Recommendations	9

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of the production Max Android application and identified two CRITICAL and four HIGH findings: a Firebase project key hardcoded in the shipped APK, an Apptentive in-app feedback SDK activity that declares `android:usesCleartextTraffic="true"` at the activity level, overriding both the application manifest's own `usesCleartextTraffic="false"` and the Network Security Config's `cleartextTrafficPermitted="false"`, meaning any HTTP link opened through Apptentive's feedback mechanism transmits in cleartext during active authenticated subscriber sessions, a Braze behavioral-marketing SDK registered app-wide alongside the Max Kids framework with no confirmed technical mechanism disabling behavioral tracking when a child's profile is active, simultaneous Nielsen DCR and Comscore audience-measurement integrations, the former still under a pre-merger Discovery namespace never refactored after the Warner-Discovery merger, both collecting device identifiers with unclear legal basis on the ad-free paid tier, an AppsFlyer integration routing individual subscriber acquisition-channel, conversion-timeline, and lifetime-value data to US servers with no confirmed Art. 46 transfer mechanism, and an unresolved GDPR Art. 14 controller-change notification obligation arising from WBD's pending Paramount acquisition, expected to close in Q3 2026, which would transfer all of the above subscriber personal data to Paramount as a new controller.

Across four written notices over ninety days, no reply of any kind, human or automated, was ever received from Warner Bros. Discovery. `privacy@wbd.com` and `datenschutz@bfdi.bund.de` both bounced permanently on the first attempt; correspondence was corrected to `security@wbd.com` from 24 July onward, with three further follow-ups on 24 July, 4 September, and 12 September, none of which received a reply. None of RFI-IRFOS's five standing questions, on Art. 6/7 legal basis, DPO awareness, a documented risk assessment, Max Kids' Braze gating mechanism, or Art. 14 preparation for the Paramount transition, ever received an answer.

Scope: Static analysis of the publicly downloaded production Max Android APK (v7.4.0.55), on an authorized test device, only. No WBD account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to `privacy@wbd.com` (bounced permanently), bcc the Austrian Datenschutzbehörde, the German BfDI (also bounced permanently), and CERT.at. Correspondence moved to `security@wbd.com` from 24 July onward, with the Austrian DSB moved to visible cc. Across four written notices over ninety days, no reply of any kind, human or automated, was ever received from Warner Bros. Discovery; the only inbound mail was permanent-bounce notifications for the two originally used dead addresses.

ID	Severity	Title
C1	CRITICAL	Firebase API key hardcoded in the production APK
C2	CRITICAL	Apptentive SDK activity overrides both the manifest and Network Security Config cleartext prohibitions

ID	Severity	Title
H1	HIGH	Braze behavioral marketing registered app-wide alongside Max Kids with no confirmed gating
H2	HIGH	Nielsen DCR and Comscore – dual audience measurement with device ID collection, including on the ad-free tier
H3	HIGH	AppsFlyer routes individual subscriber lifetime-value data to US adtech
H4	HIGH	Pending Paramount acquisition creates an unresolved Art. 14 controller-change notification obligation

Subject & Operator Analysis

Warner Bros. Discovery operates the Max streaming platform, consolidating Max, HBO, CNN, Discovery, and Cartoon Network content under a single Firebase project, wbd-stream. A pending acquisition by Paramount was expected to close in Q3 2026 as of this disclosure.

Findings

C1: Firebase API key hardcoded in the production APK

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

Firestore key AlzaSyC45CoWf5_35p-FuoPkBU_KWgDSSFvoZMA, project wbd-stream, App ID 1:345051420332:android:64bedb0e5075983e023109, storage bucket wbd-stream.appspot.com, is embedded verbatim in the public Play Store binary. With it, the wbd-stream project can be probed, Remote Config read (A/B test parameters, paywall experiments, Max Kids configuration, ad-tier targeting rules), and Firestore Storage accessed.

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

Impact: A production Firestore project's attack surface, including paywall and ad-targeting configuration, cannot be independently ruled safe from outside the console once its key ships in every installed client.

Fix: Restrict the key to the com.wbd.stream package name and SHA-256 signing fingerprint, rotate it immediately, and audit access logs from the current APK version's publish date.

C2: Apptentive SDK activity overrides both the manifest and Network Security Config cleartext prohibitions

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 application manifest correctly declares `android:usesCleartextTraffic="false"`, and the Network Security Config's base configuration correctly declares `cleartextTrafficPermitted="false"`. But the Apptentive feedback SDK's `NavigateToLinkActivity` declares `android:usesCleartextTraffic="true"` at the activity level, overriding both. This activity is registered app-wide and can fire during active authenticated subscriber sessions.

Any HTTP (non-HTTPS) URL opened through Apptentive's in-app feedback or ratings link mechanism is transmitted in cleartext, notwithstanding the app's own correctly-configured global cleartext prohibition. No reply of any kind addressed this finding.

Impact: An authenticated subscriber session's traffic can be transmitted in cleartext through a single third-party SDK activity, despite the app's own manifest and Network Security Config both correctly prohibiting this globally.

Fix: Remove `usesCleartextTraffic="true"` from `NavigateToLinkActivity`, audit all Apptentive endpoint URLs for HTTPS-only delivery, and update the SDK.

H1: Braze behavioral marketing registered app-wide alongside Max Kids with no confirmed gating

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

Braze (814 smali classes) and the Max Kids framework (2,563 smali classes) are both present. Braze's UI components, `BrazeWebViewActivity`, `BrazeFeedActivity`, and `ContentCardsActivity`, are registered app-wide rather than scoped to adult-only contexts. Whether Braze's behavioral tracking and marketing automation is technically disabled when a child's profile is active in Max Kids mode cannot be resolved from static analysis alone.

No reply of any kind answered whether this gating mechanism exists.

Impact: Behavioral marketing automation may continue operating during children's viewing sessions with no confirmed technical separation from adult-context processing.

Fix: Publish the specific technical mechanism disabling Braze during Max Kids sessions, with a distinct legal basis for adult versus children's analytics.

H2: Nielsen DCR and Comscore – dual audience measurement with device ID collection, including on the ad-free tier

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

Nielsen DCR (177 smali classes, still under the pre-merger com.discovery.adtech.sdk.nielsen.dcr namespace, never refactored after the Warner-Discovery merger, active in Production mode) and Comscore (140 smali classes, PublisherUniqueDeviceIdListener) both fire simultaneously, actively collecting a unique device identifier.

The specific concern is EU subscribers on the ad-free paid tier, where audience measurement serving ad-pricing purposes lacks a contractual-necessity legal basis. No reply of any kind addressed this finding.

Impact: Device-identifying audience-measurement data may be collected from subscribers on a tier where its stated commercial purpose, ad pricing, does not apply.

Fix: Disclose both platforms in the Art. 13 notice, audit whether measurement fires on ad-free EU tiers, and implement a separate consent mechanism if it does.

H3: AppsFlyer routes individual subscriber lifetime-value data to US adtech

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

AppsFlyer (450 smali classes: 383 internal, 5 share, 5 deeplink, 2 attribution) routes which ad campaign or channel acquired each subscriber, the subscription conversion timeline, and lifetime-value metrics to AppsFlyer's US servers.

No reply of any kind addressed this finding.

Impact: Individual subscriber acquisition and value data is transferred to a named US processor with no confirmed Art. 46 transfer mechanism.

Fix: Disclose AppsFlyer explicitly in the Art. 13 notice together with a GDPR-compliant transfer mechanism.

H4: Pending Paramount acquisition creates an unresolved Art. 14 controller-change notification obligation

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

WBD's pending acquisition by Paramount, expected to close in Q3 2026, would transfer all Max subscriber personal data, Braze behavioral profiles, Nielsen DCR/Comscore audience-measurement records, AppsFlyer attribution data, and wbd-stream Firebase analytics, to Paramount as the new controller. Under GDPR Art. 14, since Paramount would not have obtained this data directly from data subjects, an Art. 13-equivalent disclosure must reach data subjects within one month of the new controller obtaining it.

No reply of any kind confirmed whether an Art. 14 notification plan exists for the closing. GDPR liability unresolved at close becomes the acquiring party's day-one regulatory exposure.

Impact: EU Max subscribers may not be informed within the statutory one-month window that their controller has changed and that behavioral and viewing-history data are among the transferring assets.

Fix: Prepare and publish an Art. 14 notification plan for EU subscribers ahead of the acquisition's close, naming Paramount as the incoming controller and confirming persisting Art. 17/18/20/21 rights.

Two Dead Mailboxes, Four Notices, Zero Replies

privacy@wbd.com and datenschutz@bfdi.bund.de both bounced permanently on the very first attempt. Correspondence was corrected to security@wbd.com from 24 July onward, and the Austrian DSB was moved from bcc to visible cc at the same time. Three further follow-ups, 24 July, 4 September, and 12 September, received no reply of any kind from Warner Bros. Discovery.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 25(1), Art. 32(1)(b)	Hardcoded Firebase key exposing paywall and ad-targeting configuration
C2	GDPR Art. 32(1)(a), Art. 5(1)(f)	Third-party SDK activity overriding the app's own cleartext prohibitions
H1	GDPR Art. 8, Recital 38	Unconfirmed behavioral-marketing gating during children's sessions
H2	GDPR Art. 6(1), Art. 13(1)(e)	Device-ID audience measurement on a tier without a contractual-necessity basis
H3	GDPR Art. 13(1)(e), Art. 46	Undisclosed transfer of subscriber value data to a US processor
H4	GDPR Art. 14	Unresolved controller-change notification ahead of the Paramount acquisition

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to privacy@wbd.com (bounces permanently), bcc Austrian DSB/German BfDI (also bounces permanently)/CERT.at; 2 CRITICAL + 4 HIGH findings
2026-07-24	First real follow-up, corrected to security@wbd.com, Austrian DSB moved to visible cc, three standard questions posed
2026-09-04	Follow-up, 42 days since the corrected-address send, 75 days since original disclosure, zero substantive reply
2026-09-12	Follow-up, 83 days since original disclosure, zero substantive reply, findings restated unchanged

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

Residual Risk & Recommendations

- Remove the Apptentive activity-level cleartext override that undermines the app's own correctly-configured global prohibition.
- Rotate the exposed Firebase key and restrict it to the correct package name and signing fingerprint.
- Publish the technical gating mechanism separating Braze behavioral marketing from Max Kids sessions.
- Disclose Nielsen DCR, Comscore, and AppsFlyer explicitly as recipients with applicable legal bases and transfer mechanisms.
- Prepare and publish a GDPR Art. 14 notification plan for EU subscribers ahead of the Paramount acquisition's close.

RFI-IRFOS rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethnergasse 25/10, 8020 Graz, Austria Coordinated disclosure per ISO/IEC 29147. GDPR

Art. 5, 6, 8, 13, 14, 25, 32, 46. REF WBDMAX-2026-R1.