Coordinated Privacy Disclosure, Final Report

Disney Solitaire Dreams Android (com.superplaystudios.disneysolitairedreams)

SuperPlay Studios Ltd, Tel Aviv, Israel, under license from The Walt Disney Company

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, SIX DAYS AFTER THE EMBARGO, NINE MESSAGES ACROSS 92 DAYS, ZERO REPLY OF ANY KIND

Target	Disney Solitaire Dreams, a Disney-licensed solitaire card game for Android
Package	com.superplaystudios.disneysolitairedreams
Operator	SuperPlay Studios Ltd, Tel Aviv, Israel (an EU adequacy jurisdiction), under license from The Walt Disney Company
Initial Disclosure	2026-06-25
Original Embargo	2026-09-19 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-25, six days after the embargo, an internal publishing gap, not a change in terms
Regulators	Austrian DSB, German BfDI (lead SA candidates), CERT.at
Total Outbound Messages	9, across 92 days, to privacy@superplaystudios.com and legal@superplaystudios.co, both of which bounced outright, before a working address was found.
Inbound Replies	0. No reply, automated or human, was ever received on any address.

rfi.irfos@gmail.com • rfi-irfos.com
ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 25 June 2026, RFI-IRFOS disclosed to SuperPlay Studios Ltd that its Disney-licensed Disney Solitaire Dreams Android app ships four advertising and platform SDK ContentProviders, all directBootAware, that fire in a fixed order at process creation, before MainActivity, before SplashActivity, and before any consent dialog: Vungle at initOrder=102 fires first, AppLovin at 101 second, Google AdMob and Firebase tied at 100 third, and Google Play Games at 99 fourth. AppLovin ships its own bundled consent management platform (applovin_consent_flow_unified_cmp.json), but AppLovinInitProvider itself fires before that CMP can ever be displayed, meaning the app's own compliance tooling cannot gate the very component it is meant to gate.

A second finding names a redundant-mediation gap, not a single tracking flow: five competing ad networks, AppLovin MAX, Google AdMob, IronSource/LevelPlay, Vungle/Liftoff, and Facebook Audience Network, run simultaneously, each with its own device-fingerprinting and audience-modeling pipeline, four of the five initializing before any user interaction. A third finding notes Meta's codeless event logging automatically captures which Disney characters a player interacts with, which levels they play, and which purchase offers they view, without explicit developer-written tracking code, with the active server-side configuration not visible in the static binary.

Nine messages were sent across 92 days. The first two addresses tried, privacy@superplaystudios.com and legal@superplaystudios.co, both bounced outright; a working channel was found and used for the remaining messages, cc'ing the Austrian DSB, German BfDI, and CERT.at. Not one reply, automated or human, was ever received on any address at any point. The 90-day embargo, set at first contact, elapsed on 19 September 2026. This report and the accompanying closure notice publish six days later, an internal gap on RFI-IRFOS's side, not a change to the terms already disclosed.

Scope: Root-level static analysis of the production Disney Solitaire Dreams Android application (com.superplaystudios.disneysolitairedreams, version 1.20.0, 183.2 MB), as pulled via ADB from a physical device and reviewed on 25 June 2026. No dynamic instrumentation, live traffic capture, or interaction with SuperPlay's, Google's, AppLovin's, Vungle's, or Meta's backend infrastructure was performed.

Disposition

Seven findings were disclosed on 25 June 2026, re-scored under CVSS v4.0. All seven correct to MEDIUM on their computed bands, including the single most aggressive pre-consent advertising stack found across this entire audit series: four ad and analytics SDK ContentProviders, Vungle, AppLovin, Google AdMob, and Firebase, all initializing at process creation, in that firing order, before AppLovin's own bundled consent management platform can ever load. Nine messages were sent across 92 days, two addresses bouncing outright before a working channel was found. Not one reply of any kind was ever received.

ID	Severity	Title
C1	MEDIUM	Four Ad and Platform SDK ContentProviders Fire in Sequence Before AppLovin's Own Consent Tool Can Load
H1	MEDIUM	Firebase and AppLovin Publisher Keys Both Hard-coded and Extractable
H2	MEDIUM	Facebook Codeless Event Logging Captures Disney-Character and Purchase-Offer Interactions
H3	MEDIUM	All Four Privacy Sandbox Permissions, Including Cross-App Custom Audience Targeting
H4	MEDIUM	Five Competing Ad Networks Run Simultaneously, Four Pre-Consent
M1	MEDIUM	Dual In-App Purchase Systems Route Purchasing Analytics to Two Platforms
M2	OBSERVATIONAL	Boot-Time Auto-Start, Duplicated

Subject & Operator Analysis

Disney Solitaire Dreams is a Disney-licensed solitaire card game operated by SuperPlay Studios Ltd of Tel Aviv, Israel, a jurisdiction with an EU adequacy decision, under license from The Walt Disney Company.

Several genuine positives are worth naming. allowBackup is correctly set to false. uses CleartextTraffic defaults correctly to false. No microphone, camera, contacts, or location permissions are declared, a notably clean permission set for an ad-monetized mobile game. AppLovin's bundled consent management platform demonstrates genuine compliance intent, even though its own initialization timing currently defeats it.

Nine Messages, Two Bounces, Zero Reply

This case's correspondence record involved two address failures before a working channel was found. The first two addresses tried, privacy@superplaystudios.com and legal@superplaystudios.co, both bounced outright on the first attempt. A working address was located and used for the remaining messages across the full 92-day period, cc'ing the Austrian DSB, German BfDI, and CERT.at. Not one reply, automated or human, was ever received on any address at any point.

Findings

C1: Four Ad and Platform SDK ContentProviders Fire in Sequence Before AppLovin's Own Consent Tool Can Load

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.

Four SDK ContentProviders are declared directBootAware and initialize at process creation in a fixed order: Vungle (initOrder=102) fires first, AppLovin (initOrder=101) second, Google AdMob and Firebase (both initOrder=100) tied third, Google Play Games (initOrder=99) fourth, all before MainActivity, SplashActivity, or any consent dialog. AppLovin ships its own bundled consent management platform (res/raw/applovin_consent_flow_unified_cmp.json), demonstrating compliance intent, but AppLovinInitProvider itself fires before that CMP can ever be displayed, meaning it cannot gate the component it is meant to gate.

```
com.vungle.ads.VungleProvider              initOrder=102, directBootAware=true (fires
    first)
com.applovin.sdk.AppLovinInitProvider      initOrder=101, directBootAware=true (fires
    second)
com.google.android.gms.ads.MobileAdsInitProvider   initOrder=100, directBootAware=true
com.google.firebase.provider.FirebaseInitProvider   initOrder=100, directBootAware=
    true
com.google.android.gms.games.provider.PlayGamesInitProvider  initOrder=99
```

Impact: Four separate advertising and platform SDKs begin processing before a player has seen a single consent notice, and the app's own bundled consent tool cannot technically precede the component it is meant to gate.

Fix: Reduce AppLovinInitProvider's initOrder below the CMP-gating component's, and defer the remaining three providers similarly. No confirmation that this has occurred was ever received.

H1: Firebase and AppLovin Publisher Keys Both Hardcoded and Extractable

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

A Firebase API key and project identifiers, and an AppLovin SDK publisher key identifying the account used for ad-revenue routing and ad-network configuration, are both extractable from the APK.

```
Firebase API key: AIzaSyBjOdCDWnOicluFozUzsHZwcK6n2PyCFEI
Firebase project: solitaire-dreams-411507
AppLovin SDK key: 0cFJSVRJyTfXalQTFfH-NyIp1AxqWW4un-
    UiE6ku3pU4EbVmNI8xVcroxXPz1v4KhHegDCKwkm19KpZJQmaiR7
```

Impact: Both keys are trivially extractable; the Firebase key carries the usual quota/billing and security-rule risks, and the AppLovin key exposes the publisher's ad-revenue routing configuration.

Fix: Restrict the Firebase API key by package name and certificate fingerprint, and rotate the AppLovin SDK key if publisher-account exposure is a concern. No confirmation that this has occurred was ever received.

H2: Facebook Codeless Event Logging Captures Disney-Character and Purchase-Offer Interactions

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.

Meta's codeless event logging (AutoLoggingOnClickListener) attaches to UI elements automatically, capturing which Disney characters a player interacts with, which levels they play, and which in-app purchase offers they view, without explicit developer-written tracking code. The active server-side configuration is not visible in the static binary.

```
com.facebook.appevents.codeless.CodelessLoggingEventListener.
    AutoLoggingOnClickListener
com.facebook.sdk.attributionTracking
```

Impact: Character-level and purchase-offer interaction data is captured automatically and forwarded to Meta with no code-level event definition available to review or limit what is actually sent.

Fix: Disable codeless event logging or document the specific event set forwarded to Meta under Art. 13(1)(e). No confirmation that this has occurred was ever received.

H3: All Four Privacy Sandbox Permissions, Including Cross-App Custom Audience Targeting

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.

AD_ID, ACCESS_ADSERVICES_ATTRIBUTION, ACCESS_ADSERVICES_TOPICS, and ACCESS_ADSERVICES_CUSTOM_AUDIENCE are all declared. Custom Audience enables SuperPlay to build behavioral cohorts of players (for example, daily-paying Disney Solitaire players) and serve ads to those cohorts inside other, unrelated apps.

```
android.permission.ACCESS_ADSERVICES_AD_ID
android.permission.ACCESS_ADSERVICES_ATTRIBUTION
android.permission.ACCESS_ADSERVICES_TOPICS
android.permission.ACCESS_ADSERVICES_CUSTOM_AUDIENCE
```

Impact: A player of a Disney-branded card game can be turned into a cross-app advertising targeting cohort without a disclosed purpose located in the app's privacy documentation.

Fix: Document an individual Art. 6(1) legal basis for Custom Audience targeting or remove the permission. No confirmation that this has occurred was ever received.

H4: Five Competing Ad Networks Run Simultaneously, Four Pre-Consent

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.

AppLovin MAX, Google AdMob, IronSource/LevelPlay, Vungle/Liftoff, and Facebook Audience Network are all active simultaneously, each with its own device-fingerprinting and audience-modeling pipeline; four of the five initialize before any user interaction, as documented in C1.

```
AppLovin MAX, Google AdMob, IronSource/LevelPlay, Vungle/Liftoff, Facebook Audience
    Network
```

Impact: Behavioral advertising infrastructure from five separate networks is active before any user interaction, each independently fingerprinting the device.

Fix: Consolidate the mediation stack and document each processor individually under Art. 28 and Art. 13(1)(e). No confirmation that this has occurred was ever received.

M1: Dual In-App Purchase Systems Route Purchasing Analytics to Two Platforms

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.

Unity Purchasing sits as an abstraction layer over Google Play Billing, with purchasing analytics confirmed flowing to both Unity and AppsFlyer simultaneously.

```
com.unity.purchasing v5.3.1
com.android.vending.BILLING
```

Impact: Purchase behavior is duplicated across two separate analytics destinations instead of a single documented pipeline.

Fix: Document both purchasing-analytics destinations under Art. 28 and Art. 13(1)(e). No confirmation that this has occurred was ever received.

M2: Boot-Time Auto-Start, Duplicated

OBSERVATIONAL — not independently CVSS-scored; auto-start alone carries no direct confidentiality, integrity, or availability impact to score.

RECEIVE_BOOT_COMPLETED is declared twice in the manifest, alongside the IAB Open Measurement SDK, a disclosed, industry-standard viewability-measurement library.

Impact: The app begins running at every device boot without an explicit user launch, a transparency point, not a demonstrated technical exposure on its own.

Fix: Document the purpose of boot-time auto-start, or remove the duplicate declaration if not load-bearing. No confirmation that this has occurred was ever received.

Article	Finding	Basis

Data Protection, Article by Article

The findings map onto a small, specific set of GDPR provisions, set out below in one place instead of scattered across the findings themselves.

Article	Finding	Basis
Art. 7, Art. 25	C1	Four SDK Content-Providers architected to fire before any consent mechanism, including the app's own CMP.
Art. 32	H1	Two hardcoded, trivially extractable SDK keys.
Art. 5(1)(a), Art. 13(1)(e)	H2	Undisclosed automatic capture of character and purchase-offer interactions.
Art. 5(1)(b), Art. 6(1)	H3	Undisclosed cross-app advertising cohort targeting.
Art. 13(1)(e), Art. 28	H4	Five undisclosed, independently fingerprinting ad-mediation processors.
Art. 28, Art. 13(1)(e)	M1	Purchasing analytics duplicated across two undocumented processors.

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 CVSS v4.0 is RFI-IRFOS's scoring guideline, not a ceiling or a floor. It gives a reproducible, third-party-legible starting point for severity, and it does not capture real-world blast radius on its own, factors such as user population size, a vulnerable or protected class of users, or a standing corporate governance exposure the technical vector alone cannot express. RFI-IRFOS reserves the right to weigh that blast radius above the bare CVSS score, and, more rarely, to hold a score below what CVSS alone would suggest when the underlying claim is unconfirmed or disputed with evidence. In this report, all six scored findings correct to MEDIUM to match their own computed bands; M2 is classified OBSERVATIONAL because auto-start alone carries no direct scoreable impact. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: DISNEYSOLITAIRE-2026-R1.