Coordinated Security & Privacy Disclosure, Final Report

Call of Duty: Mobile for Android (com.activision.callofduty.shooter)

Six written notices, ninety-one days, five identical automated inbox replies, zero human replies

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

Target	Activision Publishing, Inc. (Activision Blizzard), ultimately controlled by Microsoft Corporation (NASDAQ: MSFT)
Product audited	Call of Duty: Mobile for Android, com.activision.callofduty.shooter (developed by TiMi Studio, Tencent)
Disclosure reference	REF ACTIVISION-2026-R1
R1 sent	2026-06-23
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2 the largest Facebook SDK integration observed across 103 audited apps in 2026, auto-logging on first launch before any age gate on a PEGI 16 title with a documented under-16 player base, CVSS v4.0 8.7, unaddressed)

rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 23 June 2026, RFI-IRFOS performed static analysis of the production Call of Duty: Mobile Android application and identified three CRITICAL and three HIGH findings: READ_CALENDAR and WRITE_CALENDAR permissions declared with no disclosed gameplay mechanic requiring calendar access and no listing in the privacy policy, a Facebook SDK integration of 3,818 smali classes, the largest such integration RFI-IRFOS had observed across 103 audited apps in 2026, with auto-logging beginning at first launch before any age gate on a PEGI 16 title with a documented under-16 player base, an IronSource (Unity) ad mediation integration of 814 smali classes performing full behavioral-targeted ad mediation, usesCleartextTraffic=true permitting in-app purchase flows and session data over unencrypted HTTP, a boot-time initialization combined with Bluetooth scanning and advertising permissions, and hardcoded Chinese-language UI strings confirming TiMi Studio (Tencent) authorship, raised as relevant to the applicability of China's National Security Law Art. 7.

Across six written notices over ninety-one days, cc'd or bcc'd to the Austrian Datenschutzbehoerde and CERT.at, both privacy@activision.com and DPO.DPO@activision.com returned only an identical automated reply stating the inbox is monitored for privacy-related issues only; no named human ever responded across the entire correspondence. None of RFI-IRFOS's three standing questions, on the legal basis for calendar access, DPO awareness of the Facebook SDK's activity on accounts flagged as belonging to minors, or Art. 33/35 regulatory notification and DPIA status for the advertising SDK's exposure to minors, ever received an answer.

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

Disposition

R1 sent 23 June 2026 to privacy@activision.com, cc dpo@activision.com, bcc the Austrian Datenschutzbehoerde. Across six written notices over ninety-one days, both privacy@activision.com and DPO.DPO@activision.com returned only an identical automated reply stating the inbox is monitored for privacy-related issues only; no named human ever responded.

ID	Severity	Title
C1	CRITICAL	READ_CALENDAR and WRITE_CALENDAR declared with no disclosed purpose
C2	CRITICAL	Facebook SDK (3,818 classes) auto-logs before any age gate on a PEGI 16 title with a documented under-16 player base
C3	CRITICAL	IronSource (Unity) ad mediation with full behavioral targeting
H1	HIGH	usesCleartextTraffic=true permits in-app purchase and session data over HTTP

ID	Severity	Title
H2	HIGH	Boot-time initialization combined with Bluetooth scanning and advertising
H3	HIGH	Hardcoded Chinese-language UI strings confirm TiMi Studio (Tencent) authorship

Subject & Operator Analysis

Activision Publishing, Inc. is part of Activision Blizzard, ultimately controlled by Microsoft Corporation following its October 2023 acquisition. Call of Duty: Mobile is developed by TiMi Studio, a subsidiary of Tencent.

Findings

C1: READ_CALENDAR and WRITE_CALENDAR declared with no disclosed purpose

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

android.permission.READ_CALENDAR and WRITE_CALENDAR are declared in the manifest. No disclosed gameplay mechanic requires calendar access, and neither permission is listed as a processed data category in the privacy policy.

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

Impact: A user's calendar, capable of revealing employer, relationships, medical appointments, and travel patterns, may be accessible to a mobile game with no gameplay justification or disclosure.

Fix: Remove READ_CALENDAR and WRITE_CALENDAR unless a specific, disclosed feature requires them.

C2: Facebook SDK (3,818 classes) auto-logs before any age gate on a PEGI 16 title with a documented under-16 player base

---

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

facebook_app_id=209252576430910, with 3,818 smali classes, the largest Facebook SDK integration RFI-IRFOS observed across 103 audited apps in 2026. Auto-logging begins at first launch, before any age gate.

Call of Duty: Mobile carries a PEGI 16 rating but has a documented under-16 player base. No reply of any kind confirmed whether the DPO is aware this SDK is active on accounts flagged as belonging to minors.

Impact: Behavioral data may be logged to Meta's advertising graph from minor players before any age verification occurs.

Fix: Gate Facebook SDK auto-logging behind an age-verification step, and confirm no data is logged from accounts identified as belonging to minors.

C3: IronSource (Unity) ad mediation with full behavioral targeting

---

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.ironsource.mediationsdk (814 smali classes, owned by Unity Technologies) provides full ad mediation, banner, interstitial, rewarded, and offerwall formats, with behavioral targeting.

No reply of any kind confirmed whether the lead supervisory authority has been notified under Art. 33 regarding this SDK's data flows, or whether a DPIA exists for its exposure to minor players.

Impact: Behaviorally-targeted advertising infrastructure operates on a title with a documented under-16 player base with no confirmed regulatory notification or impact assessment.

Fix: Confirm and publish Art. 33/35 status for IronSource's data flows given the documented minor player base.

H1: usesCleartextTraffic=true permits in-app purchase and session data over HTTP

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

android:usesCleartextTraffic="true" is declared, permitting in-app purchase flows and session data to be transmitted over unencrypted HTTP.

No reply of any kind addressed this finding.

Impact: Purchase and session traffic can be intercepted or altered on any untrusted network.

Fix: Set usesCleartextTraffic to false and implement certificate pinning for purchase and session endpoints.

H2: Boot-time initialization combined with Bluetooth scanning and advertising

---

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

RECEIVE_BOOT_COMPLETED, BLUETOOTH_SCAN, and BLUETOOTH_ADVERTISE are declared together, with the app initializing on device boot and scanning the local Bluetooth environment.

No reply of any kind addressed this finding.

Impact: Bluetooth proximity scanning starting at device boot exceeds what a mobile game's stated functionality would typically require.

Fix: Remove boot-time initialization of Bluetooth scanning unless a specific, disclosed feature requires it.

H3: Hardcoded Chinese-language UI strings confirm TiMi Studio (Tencent) authorship

---

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

Hardcoded Chinese-language UI strings in the binary confirm development by TiMi Studio, a Tencent subsidiary, raised as relevant to the applicability of China's National Security Law Art. 7 to any data the studio can access.

No reply of any kind addressed this finding.

Impact: Development attribution to a PRC-based studio raises a question about which entity can access player data and under what jurisdiction's legal obligations.

Fix: Disclose the development studio's identity and jurisdiction, and clarify the applicable data-access and transfer arrangements.

Six Notices, Two Mailboxes, One Automated Reply, Zero Humans

Across six written notices and ninety-one days, both privacy@activision.com and DPO.DPO@activision.com returned only an identical automated reply: 'This email account is used to monitor privacy-related issues only.' No named human ever responded on the merits of any finding.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 5(1)(c), Art. 13	Undisclosed calendar access with no gameplay justification
C2	GDPR Art. 8	Pre-age-gate behavioral logging on a title with a documented under-16 player base
C3	GDPR Art. 8, Art. 33, Art. 35	Behaviorally-targeted ad mediation on a minor-inclusive player base
H1	GDPR Art. 32(1)(a)	Cleartext-permitted purchase and session traffic
H2	GDPR Art. 5(1)(c)	Boot-time Bluetooth scanning beyond stated functionality
H3	GDPR Art. 13, Art. 44	Development-studio jurisdiction and data-access disclosure gap

Disclosure Timeline & Outcome

Date	Event
2026-06-23	R1 sent to privacy@activision.com, cc dpo@activision.com, bcc Austrian DSB; 3 CRITICAL + 3 HIGH findings
2026-06-27	Follow-up, four days, two automated replies, zero humans
2026-08-12	Follow-up, fifty days, three automated responses, still zero humans
2026-08-25	Follow-up, sixty-three days, four automated replies, subject renamed to 'Root Level Code Analysis'
2026-09-06	Follow-up, seventy-six days, five automated replies, zero humans, three questions posed with an internal deadline of 11 September, embargo confirmed fixed for 19 September
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Establish a functioning privacy contact capable of routing GDPR disclosures to a human, distinct from the automated monitoring inbox.
- Gate Facebook SDK auto-logging behind an age-verification step, given the documented under-16 player base.
- Confirm Art. 33/35 status for IronSource's behaviorally-targeted advertising data flows.
- Remove READ_CALENDAR and WRITE_CALENDAR unless a specific feature requires them.
- Set usesCleartextTraffic to false and implement certificate pinning for purchase and session traffic.

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. 5, 8, 13, 32, 33, 35, 44. REF ACTIVISION-2026-R1.