Coordinated Privacy Disclosure, Final Report

Last War: Survival Game Android (com.fun.lastwar.gp)

60M+ installs; correspondence conducted via funplus.com/firstfun.com addresses, publisher ownership later disputed by FunPlus corporate office

CS-DEFLECT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, ONE DAY AFTER THE STATED 24 SEPTEMBER EMBARGO, TWELVE MESSAGES, ONE TECHNICAL REPLY REBUTTED POINT BY POINT, ONE LATE PUBLISHER-IDENTITY DISPUTE, THREE AUTOMATED SURVEY CLOSURES

Target	Last War: Survival Game, a mobile strategy war game
Package	com.fun.lastwar.gp, 60M+ installs
Operator	Correspondence conducted throughout via privacyoffice@funplus.com, privacy@firstfun.com, legal@funplus.com, and named FunPlus staff (Andy Zhong, Chris Petrovic, Michael Tong); FunPlus's GC Office disputed publisher ownership of the title on 2026-09-01, after this engagement had already occurred
Initial Disclosure	2026-06-23
Stated Embargo	2026-09-24, as restated directly to the target in later correspondence, superseding the 2026-09-19/2026-09-23 dates given at earlier points
Report Published	2026-09-25, one day after the stated date
Regulators	Austrian DSB, Germany's BfDI, CERT.at, EDPS
Total Outbound Messages	12, across 70 days, to a rotating set of funplus.com/firstfun.com/lastwar.com addresses as bounces and dead addresses were identified.
Inbound Replies	Three automated satisfaction-survey ticket closures, one 'under review' auto-acknowledgment, one substantive technical response on 2026-08-24 (reviewed and rebutted point by point on 2026-09-01), and one publisher-identity dispute from FunPlus's GC Office on 2026-09-01. No reply of any kind followed the 1 September rebuttal.

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 disclosed to privacyoffice@funplus.com that the production binary of Last War: Survival Game, downloaded more than 60 million times, routes in-game voice chat audio through Tencent's Game Multimedia Engine (885 compiled classes), infrastructure operated by a company incorporated in the People's Republic of China and subject to PRC National Security Law Art. 7, which compels cooperation with state intelligence operations without judicial review or notice to the data subject. Tencent is not named as a data recipient anywhere in the game's privacy policy.

Six further findings followed the same pattern of a gap between what the privacy policy states and what the binary does: a Facebook client token hardcoded in plaintext, extractable by anyone who downloads the app; ThinkingData, a Shanghai-based analytics platform bridged directly with AppsFlyer attribution data, again with no EU adequacy decision for China; cleartext traffic permitted for all domains with no certificate pinning; AIHelp, a Chinese customer-support platform processing user conversations and account identifiers; an unexplained calendar-write capability in com.sdkmanager with no disclosed gameplay function; and leftover Chinese payment-SDK debug strings in the production release build.

The correspondence record itself became part of the case. Three automated Zendesk-style satisfaction-survey emails closed the disclosure thread without any human engagement, one of them quoting RFI-IRFOS's own escalation subject line while doing exactly what that subject asked it not to do. A substantive technical response finally arrived on 24 August from privacy@firstfun.com, addressing the Tencent and Meta SDK findings directly but, on review, not resolving the underlying Art. 44 transfer-mechanism question; RFI-IRFOS published a point-by-point technical rebuttal on 1 September. The same week, FunPlus's GC Office wrote separately to state that Last War: Survival Game is not a FunPlus title and asked to be removed from correspondence, a request made after FunPlus-affiliated staff and addresses had already engaged substantively with the app's own SDK configuration for over two months. No reply of any kind followed the 1 September rebuttal.

Twelve messages were sent across 70 days, to a rotating set of addresses as bounces and dead mailboxes (dpo@fun.co, compliance@firstfun.com, edps@europa.eu) were identified and worked around. The embargo, stated at various points as 19 September, then 23 September, then restated as 24 September in later correspondence, is treated here as 24 September, the latest date actually communicated to the target. This report and the accompanying closure notice publish one day after that date.

Scope: Root-level static analysis of the production Last War: Survival Game Android application (com.fun.lastwar.gp, built against SDK 35), pulled from Google Play and reviewed on 23 June 2026. No account was created, and no interaction with Tencent's, ThinkingData's, AIHelp's, or Facebook's backend infrastructure was performed.

Disposition

Seven findings were disclosed on 23 June 2026, re-scored under CVSS v4.0. Tencent GME's routing of in-game voice audio through PRC-subject infrastructure reaches HIGH/8.7 on its own computed band without escalation. A hardcoded Facebook client token, ThinkingData's Chinese analytics processing, unrestricted cleartext traffic, and AIHelp's Chinese customer-support processing all correct to MEDIUM. Unexplained calendar writes and leftover payment-SDK debug strings both correct to LOW/MEDIUM. Twelve messages were sent across 70 days. A substantive technical response arrived on 24 August, addressing the findings on the merits but not resolving the core Art. 44 transfer-mechanism question for Tencent; RFI-IRFOS rebutted it point by point on 1 September. The same week, FunPlus's GC Office disputed that the title is a FunPlus product and asked to be removed from correspondence, after FunPlus-affiliated addresses had already engaged substantively on the app's own SDK configuration for over two months.

ID	Severity	Title
C1	HIGH	In-Game Voice Audio Routed Through Tencent's PRC-Subject Infrastructure
C2	MEDIUM	Facebook Client Token Hardcoded in Plaintext
H1	LOW	Undisclosed Calendar Writes With No Gameplay Function
H2	MEDIUM	ThinkingData: Chinese Analytics Platform Bridged With Attribution Data
H3	MEDIUM	Cleartext Traffic Permitted for All Domains, No Certificate Pinning
H4	MEDIUM	AIHelp: Chinese Customer-Support Platform Processing User Conversations
M1	MEDIUM	Chinese Payment SDK Debug Strings Left in Production Binary

Subject & Operator Analysis

Last War: Survival Game is a mobile strategy war game with more than 60 million installs. Correspondence on this disclosure was conducted for over two months through privacyoffice@funplus.com, privacy@firstfun.com, legal@funplus.com, support@lastwar.com, and named FunPlus staff, all of whom engaged with the technical substance of the findings, including the app's own SDK configuration, before FunPlus's GC Office wrote on 1 September 2026 to state that the title is not a FunPlus product and asked to be removed from correspondence. This report attributes findings to the package and app as reviewed, and records the ownership dispute as part of the correspondence timeline without asserting a resolution either way.

Genuine positives are worth naming. Google Play Billing is properly integrated for in-app purchases. Firebase Crashlytics is present, indicating active quality monitoring. AD_ID is requested correctly through the Privacy Sandbox API, not read directly, reflecting awareness of current Google Play policy.

Twelve Messages: Three Survey Closures, One Rebutted Technical Reply, One Late Ownership Dispute

Three automated satisfaction-survey emails closed this disclosure thread without any human reading its content, one of them quoting RFI-IRFOS's own escalation subject line back while doing exactly what that subject asked it not to do. A substantive technical response arrived on 24 August 2026 from privacy@firstfun.com, addressing the Tencent GME and Meta SDK findings directly. RFI-IRFOS reviewed it on the merits and published a point-by-point rebuttal on 1 September: the response confirmed Tencent's regional server placement but did not answer which specific Art. 44-49 GDPR transfer mechanism covers Tencent as a processor, nor did it produce the underlying Art. 28 data processing agreement or standard contractual clauses. The same week, FunPlus's GC Office wrote separately to dispute publisher ownership of the title. No reply of any kind followed the 1 September rebuttal.

Findings

C1: In-Game Voice Audio Routed Through Tencent's PRC-Subject Infrastructure

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.

Tencent GME (com.gme.GME.GMESDK, com.gme.trtc, com.gme.liteav.audio), 885 compiled classes, handles in-game voice chat and routes all captured audio through Tencent's real-time communication infrastructure. Tencent Holdings Limited is incorporated in the People's Republic of China and is subject to PRC National Security Law Art. 7, which compels cooperation with state intelligence operations on demand, without judicial review or notice to the data subject. Tencent is not named as a data recipient anywhere in the app's privacy policy.

```
com.gme.GME.GMESDK (Tencent Game Multimedia Engine)
com.gme.trtc (Tencent Real-Time Communication)
RECORD_AUDIO permission declared, 885 compiled classes
```

Impact: Every player who has used in-game voice chat has had their audio routed through infrastructure legally compellable by PRC state intelligence, with no disclosed EU adequacy decision or documented Art. 44-46 transfer mechanism, and no ability to have given informed consent for a transfer never disclosed to them.

Fix: Document a specific Art. 44-46 transfer mechanism covering Tencent, or route voice data through infrastructure outside PRC jurisdiction. No confirmation that this has occurred was ever received; the 24 August response addressed regional server placement but did not answer the underlying transfer-mechanism question.

C2: Facebook Client Token Hardcoded in Plaintext

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.

A Facebook app ID and client token are hardcoded in plaintext in res/values/strings.xml , extractable by anyone with apktool from the publicly distributed APK.

```
facebook_app_id = 870206494237573
facebook_client_token = 467ea067c13ad1661b8bafcf655e6dfb
```

Impact: The extractable token enables unauthorized calls to the Facebook Graph API on the app's behalf and user-data enumeration against the app's own Facebook application.

Fix: Rotate the token and restrict it server-side. No confirmation that this has occurred was ever received.

H1: Undisclosed Calendar Writes With No Gameplay Function

LOW, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 2.4.

com.sdkmanager reads the user's calendar list and inserts events and reminders via CalendarContract.Events.insert() and CalendarContract.Reminders.insert(), with READ_CALENDAR and WRITE_CALENDAR both declared. A strategy war game has no disclosed functional need to create calendar entries.

Impact: Calendar entries created by an undisclosed SDK component, combined with behavioral data from other SDKs, contribute to a detailed daily-routine profile with no data-minimisation basis.

Fix: Remove the calendar read/write scope from com.sdkmanager unless a specific, disclosed feature requires it. No confirmation that this has occurred was ever received.

H2: ThinkingData: Chinese Analytics Platform Bridged With Attribution Data

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.

ThinkingData (cn.thinkingdata.android, 160 compiled classes), headquartered in Shanghai, bridges directly with AppsFlyer attribution data, meaning install-attribution data merges with in-app behavioral and purchase data and routes to Chinese infrastructure with no EU adequacy decision.

```
cn.thinkingdata.thirdparty.AppsFlyerSyncData (attribution bridge)
cn.thinkingdata.android, 160 compiled classes, Shanghai HQ
```

Impact: In-app purchase events, session lengths, and feature engagement, merged with advertising-attribution data, are processed by a Chinese analytics platform with no adequacy decision for that jurisdiction.

Fix: Document the Art. 44 transfer mechanism covering ThinkingData, or route this data through an EU-based analytics processor. No confirmation that this has occurred was ever received.

H3: Cleartext Traffic Permitted for All Domains, No Certificate Pinning

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

network_security_config.xml sets cleartextTrafficPermitted="true" for all domains, with no certificate pinning present anywhere in the configuration.

Impact: Purchase data, session tokens, and behavioral events are all transmittable over unencrypted HTTP, and with no certificate pinning, the app has no defense against a network-level interception even over TLS.

Fix: Restrict cleartext exceptions to specific, justified domains, and implement certificate pinning. No confirmation that this has occurred was ever received.

H4: AIHelp: Chinese Customer-Support Platform Processing User Conversations

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.

AIHelp (net.aihelp, 1,618 compiled classes) processes user support conversations, account identifiers, and reported issues. It is a Chinese customer-support platform with no EU adequacy decision covering the jurisdiction.

Impact: Support-ticket content, which frequently includes account and payment troubleshooting detail, is processed by infrastructure in a jurisdiction with no EU adequacy decision.

Fix: Document the Art. 44 transfer mechanism covering AIHelp, or migrate support-ticket processing to an EU-adequate provider. No confirmation that this has occurred was ever received.

M1: Chinese Payment SDK Debug Strings Left in Production Binary

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3.

Alipay-adjacent payment infrastructure debug strings, including Chinese-language configuration error messages, remain in the production release binary, indicating incomplete build stripping.

```
□□
: □□□□PARTNER|APP_ID|RSA_PRIVATE|TARGET_ID
```

Impact: Debug configuration strings referencing partner credentials, app IDs, and RSA private-key configuration in a production release indicate the payment integration was not fully stripped of development scaffolding before shipping.

Fix: Strip all debug and development strings from the production release build. No confirmation that this has occurred was ever received.

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. 44, Art. 13(1)(e), PRC NSL Art. 7	C1	Voice audio routed through PRC-subject infrastructure, undisclosed.
Art. 32(1)(b)	C2	Hardcoded, extractable Facebook client token.
Art. 5(1)(c), Art. 13(1)(e)	H1	Undisclosed calendar writes with no gameplay function.
Art. 44, Art. 13(1)(e)	H2	Chinese analytics platform bridged with attribution data.
Art. 32	H3	Cleartext traffic permitted for all domains.
Art. 44	H4	Chinese customer-support platform processing user conversations.
Art. 32(1)(b)	M1	Payment SDK debug strings left in production.

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. In this report, C1 corrects to HIGH on its own computed band. C2, H2, H3, H4, and M1 correct to MEDIUM, and H1 corrects to LOW, all on their own computed bands. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: RFI-2026-OFT-LW01.