Coordinated Security & Privacy Disclosure, Final Report

AliExpress for Android (com.alibaba.aliexpresshd)

Fourteen written notices, ninety days, zero findings answered on the merits, one manifest permission quietly dropped without explanation, and three misroutes to a card-fraud team

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL SIX FINDINGS UNADDRESSED ON THE MERITS AFTER FOURTEEN NOTICES

Target	Alibaba.com Singapore E-Commerce (Private) Limited / CAINIAO SMART LOGISTICS (HK) LIMITED
Product audited	AliExpress for Android, com.alibaba.aliexpresshd, v8.173.3
Disclosure reference	REF ALIEXPRESS-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	HIGH (C2 MediaProjection screen capture / C3 ByteDance pipeline / H1 Facebook Conversions API, CVSS v4.0 8.7, all un-addressed)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of the production AliExpress Android application and identified three CRITICAL and three HIGH findings: a hardcoded Firebase key, a full-device-screen recording capability (WhiteScreenRecorder, built on Android's MediaProjection API) whose stated white-screen-detection purpose does not require full display capture, an embedded ByteDance shadowhook native-hooking framework alongside TikTok branding assets forming a second, undisclosed PRC data pipeline independent of Alibaba's own infrastructure, a Facebook Conversions API integration sending EU purchase data to Meta, unexplained calendar-read/write permissions, and the absence of any certificate pinning or explicit cleartext restriction.

Across fourteen written notices over ninety days, AliExpress never produced a single substantive, finding-specific reply. Two non-templated replies (27 July, 7 August) used generic corporate-security reassurance language naming zero findings; RFI-IRFOS's own contemporaneous characterization of the second is that it is 'an unfalsifiable review' that 'names no reviewer, no date, and no finding.' Three further messages, from AliExpress's Risk Control Team, misrouted the disclosure as a card-fraud complaint. Every other inbound message was an unmodified auto-reply, in several cases arriving fifteen seconds after RFI-IRFOS's own message.

RFI-IRFOS's independent re-verification against production version 8.173.3 on 7 September 2026 found the Firebase key still hardcoded and unrotated 78 days after disclosure, the ByteDance/TikTok integration unchanged, and the Facebook Conversions API, calendar permissions, and absent certificate pinning all unchanged. The one partial change found was that the FOREGROUND_SERVICE_MEDIA_PROJECTION manifest permission is no longer declared, while the WhiteScreenRecorder class and its MediaProjection API calls remain fully present in the code, a change RFI-IRFOS explicitly flagged as an open technical question, a real fix or dormant code that could resume operating as a foreground service, that was never answered.

Scope: Static analysis of the publicly downloaded production AliExpress Android APK (re-verified against v8.173.3), on an authorized test device, only. No AliExpress account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to dataprotection.ae@aliexpress.com (privacy@aliexpress.com bounced), cc the Austrian DSB and EDPS. Across fourteen written notices over ninety days, every substantive reply was a generic corporate-security reassurance naming zero specific findings, and three separate messages misrouted the disclosure to AliExpress's card-fraud Risk Control team. No human ever addressed a single finding on its technical merits.

ID	Severity	Title
C1	CRITICAL	Hardcoded Firebase API key, unrotated 78 days after disclosure

ID	Severity	Title
C2	CRITICAL	Full-device-screen recording capability (WhiteScreenRecorder / MediaProjection), manifest permission dropped, code unchanged
C3	CRITICAL	ByteDance shadowhook SDK and TikTok assets, a second undisclosed PRC data pipeline
H1	HIGH	Facebook Conversions API sends EU purchase data to Meta
H2	HIGH	READ_CALENDAR / WRITE_CALENDAR permissions with no justification
H3	HIGH	No network_security_config.xml, no certificate pinning, no explicit cleartext restriction

Subject & Operator Analysis

AliExpress is operated by Alibaba.com Singapore E-Commerce (Private) Limited with logistics handled by CAINIAO SMART LOGISTICS (HK) LIMITED, both part of Alibaba Group Holding Limited. The Dutch Autoriteit Persoonsgegevens is the proposed lead supervisory authority; noyb's January 2025 GDPR complaints against AliExpress were cited as regulatory context in R1.

A Note on Scope

An earlier draft of this investigation's working notes referenced a TLS trust-any-user-certificate and cleartext police-domain-whitelist finding. That finding, on verification, belongs to a separate, sibling disclosure case against a different Alibaba Group app, Alibaba.com for Android, and is published there under REF ALIBABA-2026-R1. It is excluded from this AliExpress report to avoid attributing a finding to the wrong application.

Findings

C1: Hardcoded Firebase API key, unrotated 78 days after disclosure

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

Firebase API key AIzaSyCTzZFRA_8aPgjz5-T31q1F7YWquB55cLM, project aliexpress-eabcc, hardcoded in plaintext in res/values/google-services.xml.

RFI-IRFOS's 7 September 2026 independent re-verification of v8.173.3 confirmed: "the same Firebase key, AIzaSyCTzZFRA_8aPgjz5-T31q1F7YWquB55cLM, still hardcoded, unrotated, 78 days after disclosure." No reply of any kind addressed this finding on its merits.

Impact: A production credential remains exposed and unrotated across the entire embargo period, with no confirmation of any access restriction.

Fix: Rotate the key and apply documented Firebase security rules restricting its scope.

C2: Full-device-screen recording capability (WhiteScreenRecorder / MediaProjection), manifest permission dropped, code unchanged

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

The app contains a full WhiteScreenRecorder implementation (com.aliexpress.framework.base.detect.WhiteScreenRecorder$a/$b/$c) built on android.media.projection.MediaProjectionManager, capable of capturing the complete device display, not just the app's own UI.

The stated purpose, white-screen/hang detection, does not require full display capture; StrictMode, ANRWatchDog, or Firebase Performance achieve the same diagnostic goal without screen access. RFI-IRFOS's 7 September re-verification of v8.173.3 found the FOREGROUND_SERVICE_MEDIA_PROJECTION manifest permission declaration no longer present, while the WhiteScreenRecorder class and its MediaProjectionManager API calls remain fully present in the code. RFI-IRFOS flagged this explicitly as an open question, whether this is a real fix or dormant code that could resume operating as a foreground service, in its final follow-up. No reply of any kind answered it.

Impact: A screen-capture capability broader than its stated diagnostic purpose remains present in the compiled code, with its activation path narrowed but not demonstrably removed.

Fix: Remove the WhiteScreenRecorder class and its MediaProjection dependency entirely, or publish a DPIA justifying its retained code path.

C3: ByteDance shadowhook SDK and TikTok assets, a second undisclosed PRC data pipeline

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

ByteDance's shadowhook native function-hooking framework (com.bytedance.shadowhook.ShadowHook, ShadowHook$Mode, ShadowHook$RecordItem) is embedded alongside TikTok branding and integration assets, forming a data pipeline into ByteDance independent of Alibaba's own infrastructure.

ByteDance is not disclosed as a data recipient anywhere in AliExpress's privacy documentation, and the integration allows EU consumer AliExpress behavior to potentially be linked to TikTok user identities. Unchanged as of RFI-IRFOS's 7 September 2026 re-verification. No reply of any kind addressed this finding.

Impact: EU consumer shopping behavior is exposed to a second PRC-based data recipient never disclosed in the app's privacy documentation, with no Transfer Impact Assessment referenced or produced.

Fix: Disclose the ByteDance shadowhook integration explicitly as a data recipient, or remove it, and publish a Transfer Impact Assessment covering this specific data flow.

H1: Facebook Conversions API sends EU purchase data to Meta

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

The Facebook Conversions API integration transmits EU consumer purchase data directly to Meta's advertising infrastructure.

Unchanged as of the 7 September 2026 re-verification. No reply of any kind addressed this finding on its merits.

Impact: EU consumer purchase behavior is exposed to a third-party advertising platform without a named technical or contractual safeguard.

Fix: Disclose the Conversions API data fields explicitly and offer an opt-out that does not degrade core app function.

H2: READ_CALENDAR / WRITE_CALENDAR permissions with no justification

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 app requests full READ_CALENDAR and WRITE_CALENDAR access, giving it visibility into personal schedule data with no clear justification for a shopping app.

RFI-IRFOS's suggested remediation, replacing this with the scoped Intent.ACTION_INSERT, was never adopted. Unchanged as of the 7 September 2026 re-verification.

Impact: Personal schedule data is exposed to an app whose core function does not require it.

Fix: Replace direct calendar-provider access with the scoped Intent.ACTION_INSERT for the specific feature that needs it.

H3: No network_security_config.xml, no certificate pinning, no explicit cleartext restriction

HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 7.1

No network_security_config.xml is declared anywhere in the app: no certificate pinning and no explicit restriction on cleartext traffic for any AliExpress endpoint.

Unchanged as of the 7 September 2026 re-verification. No reply of any kind addressed this finding.

Impact: An attacker positioned on the network path, a malicious access point or a compromised router, can intercept or manipulate traffic without pinning to detect it.

Fix: Declare a network_security_config.xml with certificate pinning on all AliExpress and CAINIAO endpoints.

A Denial Without a Finding, Three Times, and a Card-Fraud Misroute

Two of AliExpress's fourteen replies were not machine auto-replies, but neither named a single finding. On 27 July 2026: "AliExpress maintains robust security standards and continuously monitors its infrastructure to ensure the protection of user data." On 7 August 2026, after RFI-IRFOS explicitly asked which findings had been reviewed, by whom, and on what basis: "we have not identified any security vulnerabilities or data breaches requiring notification under applicable laws," again with no reviewer, date, or finding named.

Three further messages, on 17 August, 1 September, and 7 September 2026, arrived from AliExpress's Risk Control Team and treated the disclosure as a card-fraud or chargeback complaint. RFI-IRFOS's reply to the first: "we are not a customer, and we do not want to become one." The misroute recurred twice more after that.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32	Hardcoded, unrotated production credential
C2	GDPR Art. 5(1)(c), Art. 9, Art. 13, Art. 35(3)(b)	Full-device screen-capture capability broader than its stated purpose
C3	GDPR Art. 13(1)(e), Art. 44, Art. 46	Undisclosed second PRC data recipient (ByteDance)
H1	GDPR Art. 5(1)(a), Art. 13	Undisclosed EU purchase-data egress to Meta
H2	GDPR Art. 5(1)(c)	Unjustified calendar-data access
H3	GDPR Art. 32	No certificate pinning or cleartext restriction

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 delivered to dataprotection.ae@aliexpress.com (privacy@aliexpress.com bounced), cc Austrian DSB/EDPS, 3 CRITICAL + 3 HIGH findings
2026-07-27	First non-auto reply: generic 'robust security standards' reassurance, names no finding
2026-08-07	Second non-auto reply: 'no vulnerabilities identified,' no reviewer, date, or finding named
2026-08-17 / 09-01 / 09-07	Three identical misroutes from AliExpress Risk Control Team treating the disclosure as card fraud
2026-08-24	RFI-IRFOS invokes GDPR Art. 33(4), the 72-hour supervisory-notification clock
2026-09-07	RFI-IRFOS's final independent re-verification of v8.173.3: C1/C3/H1/H2/H3 unchanged, C2's manifest permission dropped but WhiteScreenRecorder code unchanged
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Answer, on the technical merits, whether the WhiteScreenRecorder / MediaProjection code path in C2 is dead code or can still be reactivated.
- Rotate the Firebase key named in C1, unrotated for the entire embargo period.
- Disclose the ByteDance shadowhook integration as a data recipient or remove it, and produce the Transfer Impact Assessment RFI-IRFOS requested and never received.

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, 9, 13, 32, 33, 35, 44, 46. REF ALIEXPRESS-2026-R1.