Coordinated Security & Privacy Disclosure, Final Report

Alibaba.com for Android (com.alibaba.intl.android.apps.poseidon)

One CRITICAL finding genuinely fixed and independently confirmed, one CRITICAL finding partially fixed then moved server-side and made unverifiable, five findings and a legal question never answered on the merits across eleven notices and three months

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ONE FIX CONFIRMED, ONE FIX MADE UNVERIFIABLE, FIVE FINDINGS UNANSWERED

Target	Alibaba Group Holding Limited / Alibaba.com Europe B.V., Netherlands
Product audited	Alibaba.com for Android, com.alibaba.intl.android.apps.poseidon, v26.25.0 / v26.31.0
Disclosure reference	REF ALIBABA-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2, server-moved and unverifiable, CVSS v4.0 8.8); five HIGH/MEDIUM findings unaddressed

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 Alibaba.com Android application, a global B2B trade-sourcing platform, and identified two CRITICAL, four HIGH, and one MEDIUM finding, plus an unresolved legal question tied to the PRC National Intelligence Law. Alibaba.com's Data Protection Team, across five substantive replies distinct from its standard auto-reply template, self-reported fixing the two CRITICAL findings by 3 August 2026.

RFI-IRFOS independently re-pulled and verified the production APK on 7 September 2026. C1, a production TLS configuration trusting any user-installed certificate authority, was confirmed genuinely fixed. C2 was only partially fixed: the two named Chinese Public Security Bureau domains were removed from the static cleartext whitelist, but the underlying cleartextTrafficPermitted flag remains globally set, and the whitelist logic itself moved into a new interceptor class wired to Alibaba's own server-delivered remote-configuration system, meaning the same or other domains could be re-added at runtime for any version, region, or user population with no way to verify this from the app binary alone.

Four further HIGH findings, a hardcoded Firebase key, an undisclosed Facebook Conversions API integration exposing B2B trade behavior to Meta's advertising infrastructure, a subsidiary WebView component with a documented history of IMEI/IMSI exfiltration, and a dual-jurisdiction analytics pipeline, plus a MEDIUM finding on unaddressed permission scope, were never answered on their technical merits. Alibaba's final substantive reply (7 September 2026) states verbatim: 'For the rest of the queries, we will not comment nor respond as they are beyond our disclosure duty under the applicable law.' A direct question on whether Alibaba disputes that PRC National Intelligence Law Art. 7 can compel disclosure of data transiting the C2 infrastructure received the same refusal.

Scope: Static analysis of the publicly downloaded production Alibaba.com Android APK (v26.25.0, re-verified against v26.31.0), on an authorized test device, only. No Alibaba account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to Alibaba.com's Data Protection Team, cc the Austrian DSB, EDPS, EDPB, the Dutch Autoriteit Persoonsgegevens (lead SA, both delivery attempts bounced), and CERT.at. Across eleven written notices, Alibaba's Data Protection Team sent five substantive replies distinct from its standard auto-reply. C1 was independently confirmed fixed. C2 was partially fixed, then its whitelist logic moved to a server-delivered runtime configuration RFI-IRFOS cannot verify by static analysis. Five further findings and a PRC National Intelligence Law Art. 7 question were explicitly refused as 'beyond our disclosure duty.'

ID	Severity	Title
C2	CRITICAL	Cleartext HTTP whitelist partially removed, then moved to an unverifiable server-delivered runtime configuration

ID	Severity	Title
H1	HIGH	Hardcoded Firebase API key, restriction claims unverified
H2	HIGH	Facebook Conversions API receives EU B2B trade-sourcing behavior
H3	HIGH	UC WebView (Alibaba subsidiary), documented IMEI/IMSI exfiltration history, never addressed
H4	HIGH	Dual analytics pipeline, Alibaba internal (China) and Firebase Analytics (US), simultaneously
M1	MEDIUM	Broad permission scope, never technically addressed

Subject & Operator Analysis

Alibaba Group Holding Limited operates Alibaba.com, a global B2B trade-sourcing platform, through Alibaba.com Europe B.V. in the Netherlands, whose lead supervisory authority is the Dutch Autoriteit Persoonsgegevens.

Positive Observations

- Alibaba's Data Protection Team sent five genuinely substantive, apparently human/legal-drafted replies across eleven notices, a real engagement rate compared to many targets in this research series.
- C1, the production TLS configuration trusting any user-installed certificate authority, was fixed and RFI-IRFOS independently confirmed the fix on re-verification, without relying on Alibaba's self-report alone.

Findings

C2: Cleartext HTTP whitelist partially removed, then moved to an unverifiable server-delivered runtime configuration

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 8.8

The static cleartext whitelist named www.hzpolice.gov.cn (Hangzhou Public Security Bureau), www.sxgajj.gov.cn (Shaanxi Public Security Department), and 100+ other domains including people.com.cn. The two named police domains are now removed from the local network_security_config.xml, but cleartextTrafficPermitted remains globally true, and whitelist control moved to a new CleartextUpgradeInterceptor class wired to Alibaba's own Orange remote-config system (com.taobao.orange.ConfigCenter, namespace securityguard_orange_namespace).

Alibaba's position, verbatim (7 September 2026): "The cleartext whitelist entries for www.hzpolice.gov.cn and www.sxgajj.gov.cn have been removed. This is notwithstanding that any whitelisted domains that existed on Alibaba.com were mainly for the purpose of facilitating users to access the relevant websites which did not result in Alibaba.com transmitting users' data thereto." RFI-IRFOS's independent re-verification of v26.31.0 the same day found the fix real but incomplete: the two named domains are gone from the static binary, but the mechanism that whitelisted them was replaced with a server-controlled equivalent, not removed. RFI-IRFOS cannot confirm or rule out that the same or other domains, including government domains, are present in the live server-delivered configuration for any version, region, or user population.

Impact: A cleartext-HTTP capability that previously named Chinese government and judicial domains explicitly was moved from a static, auditable configuration into a dynamic, server-controlled one that cannot be verified by external static analysis, for a platform carrying EU business trade-sourcing, purchase-order, and payment data.

Fix: Set cleartextTrafficPermitted to false globally, and if any cleartext exception is operationally required, publish the exact current server-delivered domain list so it can be independently audited, rather than leaving it opaque.

H1: Hardcoded Firebase API key, restriction claims unverified

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 AIzaSyDopCbRuKAAkP3-rmeLx9MqHuhSq1OjtNQ, project 'alisourcingproject', GCP project #314775841274, hardcoded in the app binary.

Alibaba's only response (3 August 2026), verbatim: "our Firebase API Key is configured based on the minimum necessary permissions with appropriate access restrictions in place." No permission scope, console configuration, or restriction rule was named or evidenced, and none has been offered since.

Impact: The claimed access restriction on this key cannot be independently verified from outside Alibaba's own Firebase console.

Fix: Publish the actual Firebase security rules and API key restrictions applied to this key, or rotate it behind a backend proxy.

H2: Facebook Conversions API receives EU B2B trade-sourcing behavior

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 integrates Facebook's Conversions API, meaning EU business users' trade-sourcing behavior on a B2B platform is reported to Meta's advertising infrastructure.

Alibaba's only response (3 August 2026), verbatim: "all data processing activities conducted by Alibaba.com are carried out in accordance with applicable data protection laws." No technical rebuttal, scope limitation, or remediation was offered, and none has been offered since.

Impact: Business sourcing behavior, which can reveal a company's supply-chain strategy and negotiating position, is exposed to a third-party advertising platform without a named technical or contractual safeguard.

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

H3: UC WebView (Alibaba subsidiary), documented IMEI/IMSI exfiltration history, never addressed

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 ships UC WebView / WindVane, an Alibaba-subsidiary WebView component with a publicly documented history of IMEI/IMSI exfiltration, operating as a second, largely opaque data-collection layer alongside the app's own telemetry.

Alibaba's only response (3 August 2026), verbatim: "we use UC WebView to facilitate our users' web browsing activities. It does not result in UC WebView collecting any personal data... we carefully assess our service providers." No technical evidence was offered, and none has been offered since.

Impact: A WebView component with a documented history of collecting device identifiers operates as an unaudited second data-collection surface.

Fix: Publish a technical audit of what UC WebView actually collects in this app's configuration, or replace it with the platform-standard Android WebView.

H4: Dual analytics pipeline, Alibaba internal (China) and Firebase Analytics (US), simultaneously

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

Two parallel analytics pipelines run concurrently: Alibaba's own internal analytics infrastructure, subject to PRC National Intelligence Law Art. 7, and Google Firebase Analytics in the US, meaning the same behavioral dataset is visible in both jurisdictions simultaneously.

No disclosed Art. 13 notice or consent gate distinguishes this dual egress from a single-destination analytics disclosure. Alibaba's only response (3 August 2026) was a generic reference to compliance with applicable data protection laws, unaddressed on the specific j urisdictional-duplication point since.

Impact: The same behavioral dataset is fully exposed to two separate legal jurisdictions with materially different government-access regimes, without a specific disclosure distinguishing this from ordinary single-destination analytics.

Fix: Disclose the dual-pipeline architecture explicitly in the privacy policy, naming both destinations and their respective legal regimes.

M1: Broad permission scope, never technically addressed

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

Full RECORD_AUDIO, Bluetooth, GET_TASKS, GET_ACCOUNTS, and READ_PHONE_STATE permission scope, logged in RFI-IRFOS's 7 September 2026 independent re-verification.

None of these five permissions has received a technical justification or answer from Alibaba in any round of correspondence.

Impact: Permission scope broader than the app's stated B2B trade-sourcing purpose, unexplained.

Fix: Justify each permission against a specific in-app feature, or remove the ones that are not load-bearing.

A Genuine Fix, and a Fix That Moved Out of View

This case is recorded here in full because it is not a simple silence case, and treating it as one would be inaccurate. C1 is a real, independently confirmed fix: RFI-IRFOS pulled v26.31.0 itself on 7 September 2026 and verified the user-installed CA trust anchor is gone, rather than accepting Alibaba's 3 August self-report at face value.

C2 is more complicated, and RFI-IRFOS states plainly what it can and cannot confirm. The two named Chinese Public Security Bureau domains are gone from the static, auditable configuration file. But the mechanism that whitelisted them was not removed, it was relocated to a server-delivered configuration RFI-IRFOS has no way to inspect from outside Alibaba's own infrastructure. A fix that cannot be verified going forward is not the same as a fix, and Alibaba's refusal to publish the current server-delivered whitelist, or to answer whether the same domains remain present in it for any version, region, or user population, leaves this finding open rather than resolved.

Data Protection, Article by Article

Finding	Provision	Concern
C2	GDPR Art. 25, 32, 46; NIS2 Art. 21	Cleartext capability moved server-side, unverifiable, prior scope included Chinese government domains
H1	GDPR Art. 32	Hardcoded credential, restriction claims unverified
H2	GDPR Art. 5(1)(a), Art. 13	Undisclosed B2B behavioral data egress to Meta
H3	GDPR Art. 5(1)(a), Art. 28	Unaudited subsidiary WebView with documented exfiltration history
H4	GDPR Art. 13, Art. 44-49	Simultaneous dual-jurisdiction analytics exposure, undisclosed
UNRESOLVED-LEGAL	GDPR Ch. V; PRC NIL Art. 7	Transfer Impact Assessment and NIL Art. 7 exposure question explicitly refused

The PRC National Intelligence Law Question

Across three explicit written requests (18 August, 4 September, 7 September 2026), RFI-IRFOS asked whether Alibaba Group Holding Limited disputes that PRC National Intelligence Law Art. 7 can compel disclosure of data transiting the infrastructure named in C2, and whether a GDPR Chapter V Transfer Impact Assessment covering that infrastructure has been conducted and reviewed by a DPO. Alibaba's verbatim final position (7 September 2026): "we will not comment nor respond as they are beyond our disclosure duty under the applicable law." This question remains completely unanswered as of the embargo date.

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to DataProtection@service.alibaba.com (privacy@alibaba-inc.com bounced), cc Austrian DSB/EDPS/EDPB/Dutch AP (bounced)/CERT.at, 2 CRITICAL + 4 HIGH findings
2026-07-02	Alibaba redirects to its bug-bounty program, not a substantive reply
2026-07-10	Alibaba Cloud abuse-bot auto-closes and redirects to a counterfeit-goods portal
2026-08-03	First substantive reply: C1 and C2 self-reported fixed, H1-H4 answered only with generic compliance language
2026-08-11 / 08-18	RFI-IRFOS rebuttals; Alibaba explicitly stonewalls: "not obliged to supplement anything else"
2026-09-04	RFI-IRFOS sets a 3-question deadline of 11 September, restates 19 September disclosure date as unchanged
2026-09-07, 09:20 UTC	Alibaba confirms C1 fixed, partial C2 fix, refuses DPIA/TIA/NIL Art.7 questions as "beyond our disclosure duty"
2026-09-07, 10:54 UTC	RFI-IRFOS independently verifies v26.31.0: C1 genuinely fixed, C2 only partially fixed and moved server-side
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Publish the current server-delivered domainWhiteList / cleartextUpgradeWhiteList so the C2 fix can be independently verified rather than taken on trust.
- Answer the PRC National Intelligence Law Art. 7 / Transfer Impact Assessment question directly rather than declining to comment.
- Address H1 through H4 and M1 on their technical merits rather than with a blanket compliance assertion.

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, 13, 25, 32, 44-49; NIS2 Art. 21. REF ALIBABA-2026-R1.