Coordinated Privacy Disclosure, Final Report

iJoysoft ″Camera″ Android (photo.cam.filter.beauty.effect)

iJoysoft, Hong Kong corporate buffer over apparent mainland China operations, 10M+ downloads

SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, SIX DAYS AFTER THE STATED 19 SEPTEMBER EMBARGO, TWELVE MESSAGES, ZERO REPLY OF ANY KIND

Target	iJoysoft ″Camera″, a beauty-filter photo and camera app
Package	photo.cam.filter.beauty.effect, version 2.1.9
Operator	iJoysoft, Hong Kong corporate buffer over apparent mainland China operations, 10M+ downloads across its app network
Initial Disclosure	2026-06-25
Stated Embargo	2026-09-19, as communicated directly to the target in the initial disclosure
Report Published	2026-09-25, six days after the stated date
Regulators	Austrian DSB, CERT.at, EDPS
Total Outbound Messages	12, across 79 days, all to smartchen2015@gmail.com, the single generic contact address iJoysoft uses across its app network.
Inbound Replies	0. No reply, automated or human, was ever received.

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 iJoysoft, using the single generic Gmail contact address the company uses across its entire app network instead of a corporate domain, that its Camera app contains fully wired image-upload machinery, bitmap compression feeding multipart/form-data JPEG requests over OkHttp, integrated and pointed at infrastructure that includes Chinese and Alibaba Cloud endpoints. RFI-IRFOS was precise about what could and could not be statically proven: the relevant code is obfuscated and the destination URL is constructed at runtime, so the disclosure does not assert that photos are uploaded, only that the capability is built, integrated, and connected to that infrastructure, placing the burden of disclosure on iJoysoft to state what image data is transmitted, when, and to which endpoints. No on-device biometric or face-recognition SDK was found, and the disclosure explicitly does not claim biometric processing.

A second finding names the advertising identifier's exposure to Chinese ad networks, Pangle (ByteDance), Mintegral, and Tencent/QQ, with configuration and content served from Alibaba Cloud storage and a .cn host, a third-country transfer with no evident adequacy decision or Art. 46 safeguard. Two further findings compound this: an explicit android:usesCleartextTraffic="true" override, re-enabling cleartext HTTP traffic Android blocks by default since API 28, alongside a hardcoded developer LAN IP left in the shipped network security config; and Facebook Audience Network and Google Ads both registering ContentProviders that initialize before any consent step, with RFI-IRFOS noting explicitly that Google's own consent management platform being present does not necessarily gate the separate Pangle, Mintegral, and Tencent integrations.

A final finding names a permission footprint, camera, microphone, fine location, and photo geolocation, that a beauty-filter camera app does not self-evidently require, alongside AdMob and Firebase identifiers extractable from the public APK. RFI-IRFOS noted for the record that iJoysoft's operational pattern, a Hong Kong corporate buffer over apparent mainland operations, a single generic contact address across a 10-million-plus-download app network instead of a corporate domain, and a prior researcher flag for bundling adware into its desktop tooling, forms the context in which a regulator would read these findings.

Twelve messages were sent across 79 days, all to the same single generic address, cc'ing the Austrian DSB, CERT.at, and the EDPS throughout. Not one reply, automated or human, was ever received. The 90-day embargo, stated directly to the target in the initial disclosure, 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 iJoysoft Camera Android application (photo.cam.filter.beauty.effect, version 2.1.9, SHA-256 0637a308f3d56159d60f6961b6c65b3f857352fad5ca53f92fb6d0cf1d1bef80), pulled from Google Play and reviewed on 25 June 2026. No account was created, no dynamic instrumentation was performed, and no interaction with iJoysoft's, Pangle's, Mintegral's, Tencent's, or Alibaba's backend infrastructure was performed; the image-upload destination named in C2 was not, and could not be, dynamically confirmed from this static review.

Disposition

Five findings were disclosed on 25 June 2026, re-scored under CVSS v4.0. Fully wired but obfuscated-destination image-upload machinery in a camera app, capability built and integrated but with the exact upload trigger and target statically unresolvable due to obfuscation, reaches HIGH/8.2 on its own computed band without escalation. Third-country advertising-identifier exposure to Chinese ad networks, an explicit cleartext-traffic override, pre-consent ad SDK initialization, and a permission footprint with extractable API keys all correct to MEDIUM. Twelve messages were sent across 79 days. Not one reply of any kind was ever received.

ID	Severity	Title
C2	HIGH	Fully Wired Image-Upload Machinery, Obfuscated Destination, Pointed at Chinese Infrastructure
C1	MEDIUM	Advertising Identifier Exposed to Chinese Ad Networks, Alibaba/.cn Infrastructure
H1	MEDIUM	Explicit Cleartext Override With a Hardcoded Developer LAN IP in Production
H2	MEDIUM	Ad SDKs Initialize Before Any Consent Step
M1	MEDIUM	Permission Footprint Exceeds a Beauty-Filter Camera App, Extractable Keys

Subject & Operator Analysis

iJoysoft operates a corporate buffer in Hong Kong over apparent mainland China operations, uses a single generic Gmail contact address across an app network with 10 million-plus downloads instead of a corporate domain, and has previously been flagged by other researchers for bundling adware into its desktop tooling. That operational pattern is named here as context, not as an additional finding.

Twelve Messages, Zero Reply

All twelve messages in this case's correspondence record were delivered to smartchen2015@gmail.com, the single address iJoysoft provides across its app network, across 79 days, cc'ing the Austrian DSB, CERT.at, and the EDPS throughout. Not one reply, automated or human, was ever received on that address at any point.

Findings

C2: Fully Wired Image-Upload Machinery, Obfuscated Destination, Pointed at Chinese Infrastructure

HIGH, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.2.

17 classes implement Bitmap.compress() (image to bytes), and 19 classes implement okhttp3 MultipartBody/RequestBody for multipart/form-data JPEG, PNG, and WebP uploads. Camera and AR endpoints (cameraarv2.ijoysoftconnect.com/cosmetic/, /image_r4/cosmetic/) are present. The exact destination URL and trigger condition are obfuscated and constructed at runtime, so this finding does not assert that photos are uploaded, only that the capability is built, integrated, and connected to infrastructure that includes Chinese and Alibaba Cloud endpoints. No on-device biometric or face-recognition SDK was found.

```
Bitmap.compress() present in 17 classes
okhttp3 MultipartBody/RequestBody present in 19 classes
cameraarv2.ijoysoftconnect.com/cosmetic/, /image_r4/cosmetic/
```

Impact: A camera app that processes user faces carries fully integrated, wired image-upload capability with an obfuscated destination and no disclosed purpose, and the burden falls on the operator to state what is actually transmitted, when, and to where.

Fix: Publish the specific destination, trigger condition, and purpose of the image-upload machinery, and remove it if unused. No confirmation that this has occurred was ever received.

C1: Advertising Identifier Exposed to Chinese Ad Networks, Alibaba/.cn Infrastructure

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.

Pangle (ByteDance), Mintegral, and Tencent/QQ ad SDKs are present. Configuration and content are served from Alibaba Cloud storage (oss-us-west-1/oss-us-east-1.aliyuncs.com) and a .cn host (tenfei03.cfp.cn). The Android advertising identifier is exposed via ACCESS_ADSERVICES_AD_ID and the standard Google Play Services AD_ID.

```
Chinese ad SDKs: Pangle (ByteDance), Mintegral (mBridge), Tencent/QQ
.cn endpoint: tenfei03.cfp.cn
Alibaba Cloud: *.oss-us-west-1/oss-us-east-1.aliyuncs.com, *.ijoysoftconnect.com
```

Impact: The advertising identifier and device data reach Chinese advertising networks with configuration served from Alibaba Cloud and a .cn host, a third-country transfer with no evident adequacy decision or Art. 46 safeguard for EU users.

Fix: Document the Art. 44 transfer mechanism covering all three Chinese ad networks, or remove them for EU users. No confirmation that this has occurred was ever received.

H1: Explicit Cleartext Override With a Hardcoded Developer LAN IP in Production

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.

android:usesCleartextTraffic is explicitly set to true, re-enabling cleartext HTTP traffic that Android blocks by default since API 28. The network security config additionally contains a hardcoded developer LAN IP (192.168.1.172) left in the shipped production build.

```
android:usesCleartextTraffic="true"
network_security_config.xml: cleartext permitted for 192.168.1.172 (developer LAN IP)
```

Impact: A deliberate override of Android's default cleartext protection lowers transport security, and the leftover developer LAN IP is a configuration-hygiene gap indicating the production config was not cleaned before release.

Fix: Remove the cleartext override and the hardcoded developer IP from the production network security config. No confirmation that this has occurred was ever received.

H2: Ad SDKs Initialize Before Any Consent Step

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.

Facebook Audience Network and Google Ads both register ContentProviders that auto-initialize on process start, before any consent step. Google's own User Messaging Platform (Funding Choices) is present, but a CMP covering Google's stack does not necessarily gate the separate Pangle, Mintegral, and Tencent integrations named in C1.

```
com.facebook.ads.AudienceNetworkContentProvider: auto-init on process start
com.google.android.gms.ads.MobileAdsInitProvider: auto-init on process start
```

Impact: Tracking infrastructure from at least two ad networks is active before any consent mechanism runs, and it remains unconfirmed whether the separate Chinese ad SDKs are consent-gated at all for EU users.

Fix: Confirm and document whether Pangle, Mintegral, and Tencent are consent-gated for EU users, and gate Facebook and Google Ads behind the existing CMP. No confirmation that this has occurred was ever received.

M1: Permission Footprint Exceeds a Beauty-Filter Camera App, Extractable Keys

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.

CAMERA, RECORD_AUDIO, ACCESS_FINE_LOCATION, ACCESS_MEDIA_LOCATION, and AD_ID are all declared. A beauty-filter camera app does not self-evidently need microphone access, precise location, or photo geolocation. AdMob and Firebase API keys are hardcoded and extractable from the production binary.

```
admob_app_id: ca-app-pub-6282254818375654~7628703842
google_api_key: AIzaSyBcI15RM10tlcspRXX4ARleZ0XjyIEy91w
```

Impact: Microphone and precise-location access on a photo-filter app, combined with extractable ad and analytics credentials, exceeds what the app's documented function requires.

Fix: Document a specific purpose for each named permission, or remove those without one, and restrict the extractable keys by package and certificate. 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. 5(1)(a), Art. 13, Art. 44	C2	Fully wired, obfuscated-destination image-upload machinery.
Art. 44	C1	Advertising identifier exposed to Chinese ad networks, Alibaba/.cn infrastructure.
Art. 32	H1	Explicit cleartext override, hardcoded developer LAN IP.
Art. 6(1), Art. 7	H2	Ad SDKs initializing before any consent step.
Art. 5(1)(c)	M1	Permission footprint exceeding a beauty-filter camera app's needs.

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, C2 corrects to HIGH on its own computed band. C1, H1, H2, and M1 correct to MEDIUM on their own computed bands. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: IJOYSOFT-R1.