# Security & Privacy Disclosure, Final Report

## FitPro for Android (cn.xiaofengkj.fitpro)

A payment order endpoint and a WebSocket on plain HTTP in an app that tells 100 million installers their data is encrypted, with no reply since the notice.

**PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026.**

| | |
|---|---|
| **Target** | Shenzhen Well Fitness Management Technology Co,LTD (FitPro), operator named in policy: Shenzhen Jusheng Intelligent Technology Co., Ltd |
| **Versions Audited** | 2.10.8 / versionCode 208 (Play update 2026-07-16, analysed 2026-08-23) |
| **Notice / Publication** | 2026-08-23 / 2026-11-21 (90 days, unchanged) |
| **Findings** | 11: 1 High, 5 Medium, 3 Low, 1 observation (R1 labels reassessed, see status table) |
| **Status** | NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026 |
| **SHA-256 (base APK)** | `c33b6f05b2ecf83ccbfe5e58ec4add202320d00746f0cc61473afe4b6124e180` |

security@rfi-irfos.com • rfi-irfos.com

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

## Contents


1 Executive Summary 3

2 Finding Status at a Glance 5

3 Subject & Operator Analysis 5

4 Architecture & Data Flow 6

5 Engagement Summary 6

6 Findings 7

6.1 C1: Cleartext override, a ws:// WebSocket and an http:// payment order endpoint against a label that says data is encrypted in transit . . . 7

6.2 C2: About 60 own activities and services exported without a permission, including health, payment and debug screens . . . 9

6.3 C3: Two companies are named as operator, and the operator describes itself as a white-label platform vendor . . . 11

6.4 H1: Four SDK providers initialise before any consent screen, and no consent platform is wired in . . . 12

6.5 H2: The policy names five third-party SDKs and the binary ships at least a dozen more . . . 13

6.6 H3: Messages and Contacts may be shared with third parties per the Play label, against the policy . . . 14

6.7 H4: The policy says third-party applications can obtain paired device, sleep, movement and identifier data . . . 15

6.8 H5: Signature-level permissions and persistent=true requested by a consumer app . . . 16

6.9 M1: Test and debug artifacts compiled into the production build . . . 16

6.10 M2: PEGI 3 rating, date of birth collection and no age gate found in the resources 17

6.11 M3: The only official contact channels are two personal Gmail addresses . . . 17

7 Impact Analysis 18

8 The Complete Chain 18

9 Shared Platform and Chipset Fingerprint 19

10 Data Protection: Article by Article 20

11 Platform Accountability & DSA 20

12 Regulatory & Legal Landscape 21

13 Indicators of Compromise & Reproducible Evidence 22

14 Disclosure Timeline & Outcome 23

15 What Was Done Well 23

16 Residual Risk & Recommendations 24

## Executive Summary

FitPro (package cn.xiaofengkj.fitpro) is a companion app for smart watches and bands with more than 100 million installs on Google Play, 461 thousand reviews and a rating of 3.3. It syncs health readings such as ECG, blood pressure, heart rate, temperature and sleep, mirrors messages and call notifications to the band, and sells collections as in-app purchases. The Play listing carries PEGI 3. The developer of record is Shenzhen Well Fitness Management Technology Co,LTD. The privacy policy names another company, Shenzhen Jusheng Intelligent Technology Co., Ltd, as the operator. On 23 August 2026 RFI-IRFOS sent a notice with REF FITPRO-2026-R1 to the two contact addresses of the developer page, with the Austrian Datenschutzbehörde and the European Data Protection Supervisor in copy.

The root level code analysis of version 2.10.8 shows a global cleartext override, a persistent ws:// WebSocket to hiapi.jusonsmart.com:7780 and a payment order update endpoint at http://watch.jusonsmart.com/prod-api/pay/api/updateOrder, against a Google Play label and an operator policy that both promise encryption in transit (C1). About 60 activities and services of the app are exported without a permission, among them ECG, blood pressure, login, payment and raw Bluetooth debug screens (C2). Two companies are named as operator, and the operator describes itself as a white-label wearable and companion app platform vendor (C3). Four SDK providers start before any consent screen (H1). The policy names five SDKs against at least seventeen in the binary, including Yandex Mobile Ads (H2). The Play label and the policy disagree on whether messages and contacts reach third parties (H3). The policy admits that third-party applications can read paired device data (H4).

A reassessment by CVSS v4.0 band puts one finding at High, five at Medium and three at Low, with one observation left unrated. Every disclosed label that moves down does so because the package shows a configuration or a capability and not the runtime effect, or because the item is transparency and not exposure. The C1 label stays at High for the reasons stated in the finding. FitPro and the sibling app HiWatch Pro (REF HIWATCHPRO-2026-R1) are built from the same code base under the same developer account and use the same backend vendor.

The operator did not reply to the notice of 23 August 2026, the follow-up of 12 September 2026 or the follow-up of 17 October 2026. No bounce was received. This report is published on the embargo date of 21 November 2026 and records the state of the correspondence on 21 November 2026.

**Scope:** Root level code analysis of the Google Play release 2.10.8 (versionCode 208). The package was obtained as an XAPK from the APKPure mirror, with package name, version and developer cross-checked against the live Google Play listing before download. Work done: decoded manifest, resources and network security configuration (apktool, no source decode), a full string pass across the ten classes*.dex files and the two embedded Audience Network dex files (691,637 lines, about 19 MB of string pool) and the native library inventory. The Google Play listing, the Data Safety panel and the operator policy and corporate site were read on 23 August 2026. The app was not installed, no account was created, no feature was exercised, no operator server was called and no traffic was captured. No bytecode control-flow pass and no dynamic instrumentation were done. Findings that depend on runtime behaviour are marked as such. The signing certificate read from the mirror copy is not usable as a correlation key (see the Indicators section).

| ID | Severity | Title |
|---|---|---|
| C1 | HIGH | Cleartext override, a ws:// WebSocket and an http:// payment order endpoint against a label that says data is encrypted in transit |
| C2 | MEDIUM | About 60 own activities and services exported without a permission, including health, payment and debug screens |
| C3 | MEDIUM | Two companies are named as operator, and the operator describes itself as a white-label platform vendor |
| H1 | MEDIUM | Four SDK providers initialise before any consent screen, and no consent platform is wired in |
| H2 | MEDIUM | The policy names five third-party SDKs and the binary ships at least a dozen more |
| H3 | MEDIUM | Messages and Contacts may be shared with third parties per the Play label, against the policy |
| H4 | MEDIUM | The policy says third-party applications can obtain paired device, sleep, movement and identifier data |
| H5 | INFO | Signature-level permissions and persistent=true requested by a consumer app |
| M1 | LOW | Test and debug artifacts compiled into the production build |
| M2 | LOW | PEGI 3 rating, date of birth collection and no age gate found in the resources |
| M3 | LOW | The only official contact channels are two personal Gmail addresses |

| ID | Disclosed | This report | State on 14 November 2026 |
|---|---|---|---|

## Finding Status at a Glance

| ID | Disclosed | This report | State on 14 November 2026 |
|---|---|---|---|
| C1 | CRITICAL | HIGH | No reply. Configuration and endpoint strings read in 2.10.8. |
| C2 | CRITICAL | MEDIUM | No reply. Effect after a component start not tested. |
| C3 | CRITICAL | MEDIUM | No reply. Two operator names, no stated relationship. |
| H1 | HIGH | MEDIUM | No reply. Four providers with initOrder. |
| H2 | HIGH | MEDIUM | No reply. Policy names five SDKs. |
| H3 | HIGH | MEDIUM | No reply. Third parties behind the Play label not identified. |
| H4 | HIGH | MEDIUM | No reply. Authorisation screen not seen. |
| H5 | HIGH (provenance) | INFO | Not rated. Inert on a stock device. |
| M1 | MEDIUM | LOW | No reply. Test artifacts read in 2.10.8. |
| M2 | MEDIUM | LOW | No reply. Age gate not found in resources. |
| M3 | MEDIUM | LOW | No reply. Two personal mailboxes. |

## Subject & Operator Analysis

The Google Play developer of record is Shenzhen Well Fitness Management Technology Co,LTD, Room B901, Xinghe WORLD Building, No.1 Yabao Road, Nankeng Community, Bantian Subdistrict, Longgang District, Shenzhen, Guangdong, China 518129. The listed contacts are chenfengwellfitness@gmail.com, ygh13544039219@gmail.com and the phone number +86 135 4403 9219. The privacy policy at app.jusonsmart.com names Shenzhen Jusheng Intelligent Technology Co., Ltd, brand Juson Smart, as the operator and gives no address. The policy exists in English and Chinese.

The corporate site jusonsmart.com describes a supplier of smart watch, band and children's watch solutions with companion apps and device platforms for enterprises. FitPro is therefore one branded output of a platform business. The sibling app HiWatch Pro is built from the same code base, as the HiWatch Pro report of this package documents.

No Article 27 representative in the Union is named. A controller without an establishment in the Union is not covered by the one-stop-shop mechanism. The Austrian Datenschutzbehörde receives the notice in copy.

## Architecture & Data Flow

FitPro is a native Android app with ten classes*.dex files and two embedded Audience Network dex files, minSdk 26 and targetSdk 35. The first-party namespace is xfkj.fitpro. The app talks to a primary API under fpapi2.jusonsmart.com, a WebSocket host hiapi.jusonsmart.com on port 7780 and a payment path under watch.jusonsmart.com. A configuration call at https://tomato.gulaike.com/api/v1/config/app takes the app name, a type, the version and the platform as query parameters, which fits a backend that serves several differently named apps. Remote logging goes to cn-guangzhou.log.aliyuncs.com through the Alibaba Cloud Log Service SDK.

The band side is a multi-vendor client. The package bundles reference SDKs from Realtek, Jieli, OnMicro, Telink and Nordic Semiconductor (see the cluster section). Notifications reach the band through NotifyService (H3). RECORD_AUDIO is not requested and no AudioRecord, MediaRecorder or audio classification code was found, so the microphone question that this programme asks of every app is closed for this package.

## Engagement Summary

The notice REF FITPRO-2026-R1 was sent on 23 August 2026 at 00:28 UTC from rfi.irfos@gmail.com to chenfengwellfitness@gmail.com and ygh13544039219@gmail.com with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It carried the three critical findings C1 to C3, the high items H1 to H5 and the medium items M1 to M3 as short entries, a statement of what the app does well and three questions. A follow-up of 12 September 2026 restated the findings and set a date of 26 September 2026 for the three questions. A second follow-up of 17 October 2026 came from security@rfi-irfos.com. No inbound message from the operator exists in the mailbox and no delivery failure was returned for either address.

## Findings

### C1: Cleartext override, a ws:// WebSocket and an http:// payment order endpoint against a label that says data is encrypted in transit

**MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), disclosed as CRITICAL on 23 August 2026, rated HIGH by blast-radius escalation**

res/xml/network_security_config.xml of version 2.10.8 sets cleartextTrafficPermitted to true in a base-config that covers every host not scoped otherwise, trusts only the system certificate store and pins nothing. AndroidManifest.xml additionally sets android:usesCleartextTraffic to true, although the app targets API level 35, where cleartext is refused by default. Two hard-coded endpoint strings in the dex string pool use the plain scheme. The first is a persistent ws:// WebSocket to the operator backend, backed by the exported service xfkj.fitpro.websocket.JWebSocketClientService (C2). The second is http://watch.jusonsmart.com/prod-api/pay/api/updateOrder, a production path that updates the state of a payment order in an app that declares com.android.vending.BILLING and sells in-app purchases. The Google Play Data Safety panel says Data is encrypted in transit and Your data is transferred over a secure connection. Section 3 of the operator policy says the operator will use Secure Sockets Layer to encrypt this information in the two stages of data transmission and data storage. Whether these endpoints are reached at runtime with real payloads and whether TLS is enforced in front of the host names was not tested, and no traffic was captured. The configuration and the scheme of the strings are unconditional. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.3 to HIGH because the payment order endpoint is a hard-coded production path, the Google Play label and the operator policy both promise encryption in transit, and the app has more than 100 million installs

```
<network-security-config>
    <domain-config cleartextTrafficPermitted="true">
        <domain includeSubdomains="true">127.0.0.1</domain>
    </domain-config>
    <domain-config>
        <domain includeSubdomains="true">c.adsplus.cn</domain>
        <domain includeSubdomains="true">adsplus.cn</domain>
    </domain-config>
    <base-config cleartextTrafficPermitted="true">
        <trust-anchors>
            <certificates src="system" />
        </trust-anchors>
    </base-config>
</network-security-config>

android:usesCleartextTraffic="true"  (application element)
```

```
ws://hiapi.jusonsmart.com:7780/websocket/%1$s/%2$s
http://watch.jusonsmart.com/prod-api/pay/api/updateOrder
```

Operator privacy policy, section 3, as quoted in the findings file: we will use Secure Sockets Layer (SSL) to encrypt these information [sic]. In the two stages of data transmission and data storage, we will protect the information you submit to us. Policy URL: https://app.jusonsmart.com/public/privacy_en_fitpro.html

**Impact:** A person who bought a collection in the app has the state of that purchase updated over a plain HTTP request on the production API path, on the same shared Wi-Fi networks and public hotspots that every mobile payment model treats as hostile. Both Google Play and the operator tell that person in writing that the data is encrypted in transit. The app has more than 100 million installs.

**Fix:** Remove the base-config and the application-level cleartext flag, move the WebSocket to wss and the payment endpoint to https, pin the first-party hosts and correct the Data Safety declaration until that is done.

### C2: About 60 own activities and services exported without a permission, including health, payment and debug screens

**MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 4.8 (CVSS-B), disclosed as CRITICAL on 23 August 2026**

Essentially the whole xfkj.fitpro component surface of version 2.10.8 is declared with android:exported set to true and no android:permission. The manifest counts 154 exported components in total. The list below is the part owned by the app, without AndroidX and WorkManager boilerplate. Any app on the same device can start such a component through an explicit Intent without holding a permission. That is documented Android behaviour and needs no test to establish. The one correctly protected service is NotifyService, which carries the system permission BIND_NOTIFICATION_LISTENER_SERVICE. What a co-installed app gains after it starts a component was not tested. Whether BluetoothCommandActivity accepts Intent extras that become raw BLE commands for the paired wearable, whether UploadDataService can be made to upload early and whether the debug activities expose more than their own screen are open questions that need a runtime test.

```
Health data screens
xfkj.fitpro.activity.ecg.ECGHistoryActivity
xfkj.fitpro.activity.ecg.ECGMeasureActivity
xfkj.fitpro.activity.measure.BloodMeasureActivity
xfkj.fitpro.activity.measure.HeartMeasureActivity
xfkj.fitpro.activity.TempHistoryActivity
xfkj.fitpro.activity.log.SleepLogActivity
xfkj.fitpro.activity.HealthReportActivity

Account, payment and contacts screens
xfkj.fitpro.activity.login.LoginActivity
xfkj.fitpro.activity.login.RegisterActivity
xfkj.fitpro.activity.ModifyPasswordActivity
xfkj.fitpro.activity.personinfo.PersonalInfoActivity
xfkj.fitpro.activity.pay.PayQrcodeActivity
xfkj.fitpro.activity.pay.PayChoiseActivity
xfkj.fitpro.activity.SynContractsActivity
xfkj.fitpro.activity.Camera2Activity

Debug and test tooling in the production build
xfkj.fitpro.activity.debug.BluetoothCommandActivity
xfkj.fitpro.activity.debug.DebugFunctionActivity
xfkj.fitpro.activity.debug.LocalFunctionTestActivity
xfkj.fitpro.activity.debug.ApiDebugActivity
xfkj.fitpro.activity.debug.OtherBluetoothDebugActivity
xfkj.fitpro.activity.debug.WatchTimeCheckActivity
xfkj.fitpro.activity.debug.ClockDialListDebugActivity
xfkj.fitpro.activity.debug.PictureCropTestActivity
xfkj.fitpro.activity.DebugUIActivity
xfkj.fitpro.activity.test.FileSendFilesActivity
```

```
<service android:exported="true" android:foregroundServiceType="connectedDevice"
    android:name="xfkj.fitpro.service.LeService">
<service android:exported="true" android:name="xfkj.fitpro.bluetooth.
    BluetoothLeService"/>
<service android:exported="true" android:name="xfkj.fitpro.websocket.
    JWebSocketClientService"/>
<service android:exported="true" android:name="xfkj.fitpro.service.
    TelinkOtaUpgradeService"/>
<service android:exported="true" android:name="xfkj.fitpro.service.UploadDataService
    "/>
```

**Impact:** Screens with ECG, blood pressure, sleep, login and payment content, a raw Bluetooth command tool and an OTA firmware trigger can all be opened by another app on the phone. The reachability is shown and the harm after the start is not. The score reflects a local app, the user seeing the started screen, and a low confidentiality and integrity impact for that reason.

**Fix:** Set exported to false for every activity and service that no other app needs, add signature permissions where a component must stay reachable and remove the debug and test activities from the release build.

### C3: Two companies are named as operator, and the operator describes itself as a white-label platform vendor

**MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1 (CVSS-B), disclosed as CRITICAL on 23 August 2026**

The Google Play developer of record is Shenzhen Well Fitness Management Technology Co,LTD. Section 1 and section 13 of the privacy policy name a different company, Shenzhen Jusheng Intelligent Technology Co., Ltd, as the one that supports and operates the app and as the contact for questions on data processing, with a pointer to www.jusonsmart.com. Neither document says how the two companies relate. The corporate site of the second company, jusonsmart.com, presents itself under the brand Juson Smart and describes services for enterprises that cover smart watches, smart bands, children's watches, companion apps and smart device platforms, with long-term strategic partnerships with several leading enterprise companies. Its product breakdown lists the companion app as a product category. The text is in Chinese and the English wording is the findings file's translation. No Article 27 representative in the Union is named in the binary, the listing or the policy. The operator picture also matches the sibling app HiWatch Pro (report of this package), which is built from the same code base under the same developer account.

```
Play developer of record   Shenzhen Well Fitness Management Technology Co,LTD
Address (Play listing)      Room B901, Xinghe WORLD Building, No.1 Yabao Road, Nankeng
     Community,
                           Bantian Subdistrict, Longgang District, Shenzhen, Guangdong
    , China 518129
Support email              chenfengwellfitness@gmail.com
Contact email              ygh13544039219@gmail.com
Phone                      +86 135 4403 9219
Policy operator (s.1, 13)  Shenzhen Jusheng Intelligent Technology Co., Ltd, brand
    Juson Smart, www.jusonsmart.com
Policy URL (EN)            https://app.jusonsmart.com/public/privacy_en_fitpro.html
Policy URL (CN)            https://app.jusonsmart.com/public/privacy_cn_fitpro.html
Policy quote (s.1)         "The APP is supported and operated by Shenzhen Jusheng
    Intelligent Technology Co., Ltd. (hereinafter referred to as 'the Company')"
Policy quote (s.13)        "The operator of this APP is Shenzhen Jusheng Intelligent
    Technology Co., Ltd. If you have any questions or concerns about our privacy
    policy or data processing, please visit www.jusonsmart.com."
```

**Impact:** A person who reads the Google Play listing learns about one company and a person who reads the policy learns about another. Neither tells them who answers for their health and payment data. The platform vendor self-description also shows that the same code and backend are sold to other brands.

**Fix:** State the legal relationship of the two companies, name one controller with address and a corporate contact, and appoint an Article 27 representative.

### H1: Four SDK providers initialise before any consent screen, and no consent platform is wired in

**MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N, 5.1 (CVSS-B), disclosed as HIGH on 23 August 2026**

Four provider declarations carry android:initOrder, so Android starts them when the process is created and before a consent screen can run. The Firebase provider is also directBootAware. A search of the ten classes*.dex files and the two embedded Audience Network dex files found one plain label each for OneTrust or CookiePro, Didomi and Usercentrics, all inside the generic detector enum of one ad mediation SDK, and no integrated consent flow. The 137 hits for IABTCF and IABUSPrivacy keys are the standard preference key names that any TCF-aware ad SDK reads. They show that the SDKs can read a TCF string and do not show that the app produces one. No OneTrust, Didomi or Usercentrics SDK and no in-house consent screen was found in the resources or the manifest. Which identifiers the four SDKs read at start-up and when they send them was not measured. The TraminiContentProvider with the .initprovider authority naming is the same AnyThink or TopOn component seen in Wearfit Pro and WearFit2.0. It is a shared SDK choice and the report does not treat it as a platform link.

```
<provider android:authorities="cn.xiaofengkj.fitpro.firebaseinitprovider" android:
    directBootAware="true" android:exported="false" android:initOrder="100" android:
    name="com.google.firebase.provider.FirebaseInitProvider"/>
<provider android:authorities="cn.xiaofengkj.fitpro.initprovider" android:exported="
    false" android:initOrder="100" android:name="com.tramini.plugin.api.
    TraminiContentProvider"/>
<provider android:authorities="cn.xiaofengkj.fitpro.applovininitprovider" android:
    exported="false" android:initOrder="101" android:name="com.applovin.sdk.
    AppLovinInitProvider"/>
<provider android:authorities="cn.xiaofengkj.fitpro.vungle-provider" android:exported
    ="false" android:initOrder="102" android:name="com.vungle.ads.VungleProvider"/>
```

**Impact:** Advertising components start on a phone that is paired with a health band before the person has made a choice. The app has more than 100 million installs and carries a PEGI 3 rating.

**Fix:** Gate every advertising and analytics SDK on a recorded consent decision and add a consent management platform.

### H2: The policy names five third-party SDKs and the binary ships at least a dozen more

**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 (CVSS-B), disclosed as HIGH on 23 August 2026**

Section 9 of the policy names Google Maps, Qiniu Cloud, Sina Weibo, WeChat and Facebook with purposes and links. The table below lists components in the compiled binary that the section does not name. The hit counts are class-string matches in the string pool and measure presence, not use. The Yandex integration adds a Russian Federation signal that the policy does not address anywhere. The policy holds no Russia specific text.

| SDK or namespace | Hits | Observed purpose |
|---|---|---|
| com.applovin.* | 594 | Ad mediation |
| com.vungle.* | 49 | Video ads |
| com.inmobi.* | 1,380 | Ad mediation |
| sg.bigo.* (BIGO Ads) | 1,638 | Ad mediation |
| com.thinkup.*, com.smartdigimkt.* (AnyThink/TopOn rebrand) | 802 + 2,349 | Ad mediation, largest SDK in the app |
| com.unad.sdk.* (second wrapper over AdMob, AppLovin, Meta, Mintegral, Pangle, TopOn adapters) | 128 | Ad mediation layer |
| com.mbridge.* (Mintegral) | 200 | Ad mediation |
| com.bytedance.*, com.pgl.* (ByteDance Pangle) | 151 + 76 | Ad mediation, native libpglarmor.so, libbuffer_pgl.so, libtt_ugen_layout.so, libapminsighta.so, libapminsightb.so |
| com.yandex.* (Yandex Mobile Ads) | 1,312 + 71 | Ad mediation |
| com.baidu.* (Baidu Maps) | 139 | Location SDK, native liblocSDK8b.so |
| com.aliyun.sls.* (Alibaba Cloud Log Service) | provider present | Remote logging, native libsls_producer.so, endpoint cn-guangzhou.log.aliyuncs.com |
| com.facebook.ads.* (Meta Audience Network) | 48 | Ad mediation |

**Impact:** The user reads a list of five and installs an app that talks to many more companies in the United States, the People’s Republic of China, the Russian Federation and Singapore. Nothing tells them who receives what.

**Fix:** List every component that receives or processes personal data with its operator and

country, address the Russian and Chinese recipients under Chapter V and remove components that no feature uses.

### H3: Messages and Contacts may be shared with third parties per the Play label, against the policy

**MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 4.8 (CVSS-B), disclosed as HIGH on 23 August 2026**

The manifest declares no READ_SMS, RECEIVE_SMS or SEND_SMS. It registers xfkj.fitpro.service.NotifyService, a NotificationListenerService with the permission BIND_NOTIFICATION_LISTENER_SERVICE, which mirrors incoming SMS, call and other apps' message notifications to the paired wearable. The operator policy describes this as reading short messages and calls to synchronise them to the Bluetooth device and states: Not used for any other purpose. The Google Play Data Safety panel says that Messages (SMS or MMS and other in-app messages) and Contacts may be shared with other companies or organisations. The two statements pull apart. The identity of the third parties and the mechanism behind the label were not determined. They may be the advertising and analytics SDKs of H2 or a separate integration.

```
<service android:exported="true" android:foregroundServiceType="connectedDevice"
    android:label="@string/app_name"
  android:name="xfkj.fitpro.service.NotifyService" android:permission="android.
    permission.BIND_NOTIFICATION_LISTENER_SERVICE">
  <intent-filter>
    <action android:enabled="true" android:name="android.service.notification.
    NotificationListenerService" android:priority="1000" android:process="system"/>
  </intent-filter>
</service>
```

**Impact:** A listener that sees who messages a person, how often and through which app builds a communication pattern of the user and of every person who writes to them, none of whom agreed to it. The Play label suggests that some of this may reach other companies.

**Fix:** State in the policy and in the Data Safety declaration which message and contact data leaves the device, to whom and why, and keep notification content on the Bluetooth link.

### H4: The policy says third-party applications can obtain paired device, sleep, movement and identifier 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 (CVSS-B), disclosed as HIGH on 23 August 2026**

The device-management section of the policy states that after a wearable is paired, third-party applications interacting with paired wearable devices can obtain data such as the random identifier, device name and hardware information and status, and can send messages to the paired device. According to the explicit authorisation, these third-party applications can access sensor data, sleep status, movement type, pedometer data, log information, location information and equipment information that includes system basic information, equipment name and identifier, IMEI, Mac address, system log, IMSI, AndroidID, Android advertising ID, OAID, hardware serial number and SIM card identification. The policy names a category of recipients and no recipient. The wording echoes the multi-tenant statement in the Wearfit Pro policy, from a second operator. The report treats this as two instances of one business pattern and not as one platform. The consent screen a third-party application sees before it gets such access is a user interface question that the package does not answer.

```
"... third-party applications can access the device's sensor data, sleep status, and
    movement type [walking, running], pedometer status data, log information, location
     information, equipment information (system basic information, equipment name,
    equipment identifier, IMEI, Mac address, system log, system use information,
    equipment use information, IMSI, AndroidID, Android advertising ID, OAID, hardware
     serial number, SIM card identification, etc.)."
```

**Impact:** A person who pairs a band is told that other applications may read their sleep, movement, location and device identifiers. The policy does not say which applications or on which basis.

**Fix:** Name the third-party applications or their categories with purposes, show the authorisation screen and state the legal basis.

### H5: Signature-level permissions and persistent=true requested by a consumer app

**INFO, no CVSS v4.0 score assigned, observation, not rated, disclosed as HIGH (provenance) on 23 August 2026**

The manifest requests android.permission.READ_PRIVILEGED_PHONE_STATE, android.permission.READ_LOGS and android.permission.MOUNT_UNMOUNT_FILESYSTEMS and sets android:persistent to true on the application element. The first two are signature or system protected and cannot be granted to a Play-distributed app on a stock device. The third has no effect on current Android versions. persistent is a hint that matters for preinstalled system apps. None of this is exploitable on a standard consumer device. The combination fits a template meant for manufacturers who sign the app as a system app, and it supports the picture of FitPro as one branded output of a shared platform build. The report records it as provenance and does not rate it.

```
<uses-permission android:name="android.permission.READ_PRIVILEGED_PHONE_STATE"/>
<uses-permission android:name="android.permission.READ_LOGS"/>
<uses-permission android:name="android.permission.MOUNT_UNMOUNT_FILESYSTEMS"/>
<application ... android:persistent="true" ...>
```

**Impact:** No processing capability follows from the declarations on a non-rooted device.

**Fix:** Remove permissions that have no function on the target platform.

### M1: Test and debug artifacts compiled into the production build

**LOW, CVSS v4.0 AV:L/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.1 (CVSS-B), disclosed as MEDIUM on 23 August 2026**

res/values/strings.xml holds admob_mine_native_ad_unit_id with the value ca-app-pub-3940256099942544/2247696110, which is the sample native ad unit published by Google for test ads, used as the placement for the profile screen of a release build. The dex string pool holds two test endpoints on plain HTTP, a payment test host and a PRC domain IoT push manager for a third-party cloud integration. Test and staging artifacts should not reach production. The test endpoints use the same plaintext default as the production ones in C1.

```
admob_mine_native_ad_unit_id = ca-app-pub-3940256099942544/2247696110
http://pay.test.hyjk.top
https://iot-test.wasumedia.cn/thirdCloud/connect/manager/open/push
```

**Impact:** A release build that carries test endpoints shows weak separation between test and production. The test payment host is plain HTTP.

**Fix:** Remove test identifiers and endpoints from release builds and add a release check for them.

### M2: PEGI 3 rating, date of birth collection and no age gate found in the resources

**LOW, CVSS v4.0 AV:L/AC:H/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.0 (CVSS-B), disclosed as MEDIUM on 23 August 2026**

The Play listing carries PEGI 3 and APKPure lists Everyone. Section 12.2 of the policy says that account setup collects gender and date of birth to give better sports suggestions. No age gate, parental consent flow, date-of-birth validation logic or minors section was found in strings.xml or the manifest. The date of birth field is confirmed by the policy text. Whether an enforced minimum age check exists on it was not established, since the decode covered resources and strings and not the code.

```
Google Play content rating: PEGI 3 (APKPure: Everyone)
Policy s.12.2: account setup collects "gender and date of birth"
```

**Impact:** A child can create an account in a product that is rated for everyone and that collects a date of birth without a check the package shows.

**Fix:** Add an age gate with a parental consent path or state that the app is for adults, and align the rating.

### M3: The only official contact channels are two personal Gmail addresses

**LOW, CVSS v4.0 AV:L/AC:H/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.0 (CVSS-B), disclosed as MEDIUM on 23 August 2026**

Both contact addresses of the Play developer of record are free webmail accounts. The local part of the second one appears to embed a mobile phone number, which matches the phone number on the listing. The operator controls the domains iwellfitness.com and jusonsmart.com, according to the findings file, and uses neither for a contact address on the listing. No corporate address was found in the app materials.

```
chenfengwellfitness@gmail.com   (Support email)
ygh13544039219@gmail.com       (Contact email)
+86 135 4403 9219              (Phone)
```

**Impact:** A person who wants access or deletion of health data has a private mailbox as the only written channel.

**Fix:** Publish a corporate privacy contact on a company domain in the listing and the policy.

## Impact Analysis

The people affected are the users of a 100 million install health and fitness companion. They hold ECG, blood pressure, heart rate, temperature and sleep readings in the app, they pair a band that mirrors their messages and calls, and some of them pay inside the app. Minors are among them, since the Play rating is PEGI 3.

The weight of the case sits on the transport layer. A payment order endpoint and a WebSocket that use plain schemes (C1) are the clearest contradiction between what the platform label tells users and what the code can do. The exported surface (C2) matters for health and debug screens, and the harm after a start is not shown. The operator split (C3), the SDK table (H2) and the third-party application statement (H4) decide whether a user can find out who holds their data.

The package shows configuration and capability. No health reading, payment detail or message was observed leaving a device and the report asserts no such flow.

## The Complete Chain

Step 1, install: a user installs the app from Google Play after reading a Data Safety label that says data is encrypted in transit. Four SDK providers start at process creation (H1).

Step 2, account: the user registers, enters gender and date of birth and sees a policy that names a different company from the listing (C3, M2).

Step 3, pairing: the user pairs a band, which can mirror messages through a notification listener (H3), and the policy says third-party applications may read device data (H4).

Step 4, operation: the app talks to its API, a WebSocket and a payment endpoint over a configuration that permits plain HTTP, and two of those endpoints use the plain scheme (C1). Health and payment screens are reachable by other apps (C2).

Step 5, rights: a person who wants to ask what is held finds two company names and two personal mailboxes (C3, M3).

## Shared Platform and Chipset Fingerprint

FitPro does not share the Bluetrum abpartool fingerprint of HryFine, Wearfit Pro and Fere Fit. A search of all dex files for bluetrum and abpartool returned no hit. FitPro is a multi-vendor client, which fits a hub build for hardware from several chip platforms sold under many brands. The same naming convention for the AnyThink or TopOn provider as in Wearfit Pro and WearFit2.0 is a shared SDK choice. The libapminsighta.so and libapminsightb.so file names also appear in HryFine and are generic ByteDance components. Neither signal is treated as a platform link.

| Vendor SDK | Class-string hits | Corroborating evidence |
|---|---|---|
| Realtek (Realsil) | 929 | com.realsil.ota.*, com.realsil.sdk.dfu.* DFU stack, string rtksdk_copyright ″Copyright 2019 Realtek Semiconductor Corp.″ |
| Zhuhai Jieli Technology | 514 | Native libjl_ota_auth.so, strings company_name ″Zhuhai jili technology co., LTD″ and copy_right ″Copyright@2019www.zh-jieli.com All Rights Reserved″ |
| OnMicro | 157 | com.onmicro.omtoolbox.dfu6620.Dfu6620Manager, reference http://www.onmicroapp.com.cn/Onmicro/public/index.php/ |
| Telink | present, count not isolated | xfkj.fitpro.service.TelinkOtaUpgradeService, Lcom/telink/ota/ble/Device$DeviceStateCallback |
| Nordic Semiconductor (open-source DFU) | 132 | Lno/nordicsemi/android/dfu/*, also found in WearFit2.0 |

The strongest first-party evidence of a shared multi-brand backend is the configuration call that passes the app name to https://tomato.gulaike.com/api/v1/config/app. The same path shape exists under a second domain, jusonsmart.com. The relationship between gulaike.com and jusonsmart.com was not resolved and is an open lead. The sibling report HiWatch Pro shows the same call inside a package that carries artifacts of at least nine differently branded products. The pair of operator statements, here and in the Wearfit Pro report, shows that the white-label model is not confined to one supplier. It does not show that the two suppliers share infrastructure.

## Data Protection: Article by Article

Article 4(7), controller: engaged by C3 as the open question of which company is the controller.

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1, H2 and H3.

Article 5(1)(b), purpose limitation: engaged by H3 and H4.

Article 5(1)(c), data minimisation: engaged by M2.

Article 5(1)(f), integrity and confidentiality: engaged by C1.

Article 6(1): engaged by H1, H3 and H4.

Article 7(1), conditions for consent: engaged by H1.

Article 8, children: engaged by M2.

Article 12(1), Article 13(1)(a) and 13(1)(e) and Article 14: engaged by C1, C3, H2, H4 and M3.

Article 25: engaged by C2 and M2.

Article 27: engaged by C3. No representative is named.

Article 32(1)(a) and (b): engaged by C1 and C2.

Articles 44 and 46: engaged by H2 as an open question for the Russian, Chinese and Singapore recipients. No transfer is asserted.

## Platform Accountability & DSA

The Google Play Data Safety panel of FitPro says that data is encrypted in transit and that Contacts, Messages and App activity may be shared with other companies, and it lists Device IDs and app performance data as collected. The encryption statement conflicts with the shipped configuration and the two endpoint strings (C1). The sharing statement for Messages and Contacts conflicts with the policy (H3). The Contains ads badge agrees with the advertising stack of H2.

Google Play is an online platform under Regulation (EU) 2022/2065. Any person can submit a notice about the Data Safety declaration under the notice and action mechanism of Art. 16 of that Regulation. RFI-IRFOS records the contradiction here and treats the notice as a decision for the publication stage.

## Regulatory & Legal Landscape

Shenzhen Well Fitness Management Technology Co,LTD and Shenzhen Jusheng Intelligent Technology Co., Ltd offer the app to users in the Union through Google Play, so Art. 3(2) of the GDPR applies. No main establishment in the Union is identified for either company, so the one-stop-shop mechanism does not apply and the supervisory authority of each Member State where users are affected is competent under Art. 55. The Austrian Datenschutzbehörde (dsb@dsb.gv.at) and the European Data Protection Supervisor (edps@edps.europa.eu) received the notice in copy.

Infringements of Art. 5, 6, 7 and 9, of Art. 12 to 22 and of Art. 44 to 49 fall under the upper fine tier of Art. 83(5). Infringements of Art. 25, 27 and 32 fall under Art. 83(4). Data subjects can complain under Art. 77 and claim damages under Art. 82. Art. 5(3) of the ePrivacy Directive covers access to information on the user’s device.

The disclosure follows ISO/IEC 29147 and Art. 17 StGG. RFI-IRFOS acts under ZVR 1015608684 and GISA 39261441.

## Indicators of Compromise & Reproducible Evidence

No indicators of compromise were found and none are claimed. The values below are the identifiers needed to reproduce each finding. All values are given in full.

```
Package            cn.xiaofengkj.fitpro
Version            2.10.8 (versionCode 208), updated 2026-07-16, minSdk 26, targetSdk
    35
XAPK SHA-256       b855000ad8865b0b8e2489c3d7cf52edf9d0c444d1e4c23e21a1d4a0db121474
base APK SHA-256   c33b6f05b2ecf83ccbfe5e58ec4add202320d00746f0cc61473afe4b6124e180
arm64-v8a split SHA-256 3
    a61e1e6d53d8e351dd296cda22d4220dad9028eb9ba52f1c6de5e06b54c0c68
Mirror copy signer  CN=Android, OU=Android, O=Google Inc., L=Mountain View, ST=
    California, C=US
Mirror signer SHA-256 c724d5d6683572a3ac1e66c60fadff09ee3feeceafc735b587be4d1e2f91b9d4
Audit device       none, the app was not installed
Acquisition        APKPure mirror, 2026-08-23
```

The signing identity read from the mirror copy is a generic Android debug-style identity for both the main signer and the source stamp. It is most likely an artifact of how the mirror repackages Play-delivered split APKs and is not the operator's own certificate. It was not checked against a device install and is not used as a correlation key.

```
Primary API        fpapi2.jusonsmart.com
WebSocket          ws://hiapi.jusonsmart.com:7780/websocket/%1$s/%2$s
Payment update     http://watch.jusonsmart.com/prod-api/pay/api/updateOrder
Config API         https://tomato.gulaike.com/api/v1/config/app?name=%1$s&type=1&
    version=%2$s&platform=%3$d
Test payment host  http://pay.test.hyjk.top
Test IoT endpoint  https://iot-test.wasumedia.cn/thirdCloud/connect/manager/open/push
Log endpoint       cn-guangzhou.log.aliyuncs.com
Policy (EN)        https://app.jusonsmart.com/public/privacy_en_fitpro.html
Policy (CN)        https://app.jusonsmart.com/public/privacy_cn_fitpro.html
Sample AdMob unit  ca-app-pub-3940256099942544/2247696110
Contacts           chenfengwellfitness@gmail.com, ygh13544039219@gmail.com, +86 135
    4403 9219
```

```
C1  res/xml/network_security_config.xml, AndroidManifest.xml (usesCleartextTraffic),
    dex string pool (ws:// and http:// endpoints), Play Data Safety panel, policy s.3
C2  AndroidManifest.xml (exported activities and services)
C3  Google Play About the developer panel, policy s.1 and s.13, jusonsmart.com
H1  AndroidManifest.xml (four initOrder providers), dex string pool
H2  policy s.9 against dex namespaces and native library inventory
H3  AndroidManifest.xml (NotifyService), Play Data Safety panel, policy s.8 and s.10
H4  policy device management section
H5  AndroidManifest.xml
M1  res/values/strings.xml, dex string pool
M2  Google Play listing, policy s.12.2
M3  Google Play About the developer panel
```

Reproduction: obtain cn.xiaofengkj.fitpro 2.10.8 (208), check the SHA-256 values above, de-

code the manifest and resources with apktool and extract the dex string pools with strings. No device, account or network access is needed.

## Disclosure Timeline & Outcome

2026-08-23 Notice REF FITPRO-2026-R1 at 00:28 UTC to chenfengwellfitness@gmail.com and ygh13544039219@gmail.com, CC dsb@dsb.gv.at and edps@edps.europa.eu. Findings, three questions, response requested within 30 days.

2026-09-12 Follow-up at 16:56 UTC, 20 days after the notice. It restated the findings and asked three questions on the Data Safety statement about encryption in transit, the controller for EU users and the SDK disclosure, with answers due on 26 September 2026.

2026-10-17 Second follow-up from security@rfi-irfos.com at 19:04 UTC, 35 days before publication, with the three questions reframed on the encryption statement, the controller and the pre-consent initialisation.

2026-11-14 No reply of any kind and no delivery failure. The mailbox holds no inbound message from either address.

2026-11-21 Embargo date, 90 days after delivery of the notice of 23 August 2026.

## What Was Done Well

The Google Play Data Safety panel is filled with specific categories and is not boilerplate. The problem is the encryption statement and not the absence of a panel. A real, substantive privacy policy is linked from the app, names a responsible company and describes each permission with a usage scenario in section 8. An account deletion path is documented as My, Personal Information, Cancel and is described as deleting the account and the associated information on the server. RECORD_AUDIO is not requested, and no AudioRecord, MediaRecorder or audio classification code was found in the strings or class inventory.

## Residual Risk & Recommendations

Open at the date of publication: all findings except the observation. The operator has not replied and the build analysed is version 2.10.8 of 16 July 2026. A final APK diff before 21 November 2026 determines the state that the published report records.

Recommendations in order of effect. First, remove the global cleartext override and the application-level flag, move the WebSocket to wss and the payment endpoint to https and correct the Data Safety statement (C1). Second, close the exported surface and remove the debug and test activities from the release build (C2). Third, name the controller, the relationship of the two companies and a corporate contact, and appoint an Article 27 representative (C3, M3). Fourth, gate the advertising SDKs on consent and publish the complete SDK and recipient list with countries (H1, H2). Fifth, state which message and contact data leaves the device and name the third-party applications that may read paired device data (H3, H4). Sixth, remove test artifacts and add an age gate (M1, M2).

**RFI-IRFOS** security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria RFI-IRFOS research focus institute · ZVR 1015608684 ·

GISA 39261441 · Graz, Austria. Coordinated disclosure under ISO/IEC 29147, Art. 17 StGG (freedom of science) and Art. 89 GDPR. Root level code analysis of the published application only. CVSS values are CVSS v4.0 Base (CVSS-B) and model technical exposure, so transparency findings fit the scale only approximately. Labels above the computed band carry a blast-radius escalation statement in the finding. Final report, published 21 November 2026. REF FITPRO-2026-R1.