Security & Privacy Disclosure, Final Report

HiWatch Pro for Android (com.legend.hiwatchpro.app)

A Play label that says no data is collected, a shared nine-brand backend and global cleartext in a smartwatch app with 50 million installs, 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 (HiWatch Pro), backend vendor behind jusonsmart.com and gulaike.com not identified
Versions Audited	1.3.72 / versionCode 49 (analysed 2026-08-23)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	12: 1 High, 6 Medium, 4 Low, 1 observation (R1 labels re-assessed, see status table)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`3e340dc48c896698418706973b3399733da257b50cb640e3955c910e6d89022a`

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: One code base, one backend and at least nine brand identities, with the controller not identifiable from the Play listing . . . 7

6.2 C2: The Data Safety panel says no data is collected and the package reads SMS, contacts, call log, location and notifications . . . 8

6.3 C3: More than fifteen advertising and analytics SDKs with no consent management platform, in a persistent process . . . 9

6.4 H1: Baidu and Google Maps keys in the manifest . . . 10

6.5 H2: Compiled endpoints on Alibaba, Tencent, AutoNavi, Baidu and Umeng infrastructure for location and health related data . . . 11

6.6 H3: SMS content and notification metadata are processed for people who never installed the app . . . 12

6.7 H4: Ten debug, test and Bluetooth command activities exported without a permission in the production release . . . 13

6.8 H5: Cleartext traffic permitted for the whole app and user-installed certificates trusted with a pin override, on an app with 50 million installs . . . 14

6.9 H6: allowBackup is true and both backup rule files are empty . . . 15

6.10 M1: Test backend endpoint compiled into the production release . . . 15

6.11 M2: The agreement string says Default Consent, which suggests a pre-ticked checkbox . . . 16

6.12 M3: The English privacy policy URL is named default and shared across the brand cluster . . . 16

7 Impact Analysis 17

8 The Complete Chain 17

9 Shared Chipset or Platform Fingerprint 18

10 Data Protection: Article by Article 18

11 Platform Accountability & DSA 19

12 Regulatory & Legal Landscape 19

13 Indicators of Compromise & Reproducible Evidence 20

14 Disclosure Timeline & Outcome 21

15 What Was Done Well 21

16 Residual Risk & Recommendations 21

Executive Summary

HiWatch Pro (package com.legend.hiwatchpro.app) is the companion app of a smartwatch line. It is published on Google Play by Shenzhen Well Fitness Management Technology Co,LTD, has more than 50 million installs, a rating of 3.6 stars from 154 thousand reviews and PEGI 3. RFI-IRFOS sent a notice with REF HIWATCHPRO-2026-R1 first to 866589978@qq.com, which bounced permanently because the mailbox does not exist. The identical notice was redelivered on 23 August 2026 at 11:35 UTC to legend_wgl@yeah.net, the contact address published on the backend vendor's site jusonsmart.com, with the Austrian Datenschutzbehörde and the European Data Protection Supervisor in copy.

The Google Play Data Safety card states that the developer says the app does not collect user data, and on the same card that Contacts may be shared with third parties. The root level code analysis of version 1.3.72 finds SMS, contacts, call log, location and notification access in app-owned classes (C2). The application class is that of the FitPro code base, and the APK carries callback components for seven package identities, a string for an eighth and a privacy policy for a ninth, all served by one configuration backend (C1). More than fifteen advertising and analytics SDKs ship with no consent management platform (C3). Cleartext traffic is permitted for the whole app and user certificates are trusted with a pin override, which makes it the one finding that stays at High (H5). Ten debug and test activities are exported without a permission (H4).

A reassessment by CVSS v4.0 band puts six findings at Medium, four at Low and one at High, with one observation left unrated. The three findings disclosed as Critical move to Medium because the package shows the permissions, the classes and the shared backend and does not show a data flow. HiWatch Pro is built from the same code base and shares the backend with FitPro (REF FITPRO-2026-R1).

The operator did not reply to the redelivered notice of 23 August 2026, the follow-up of 12 September 2026 or the follow-up of 17 October 2026. No bounce was received on the redelivery address. 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 version 1.3.72 (versionCode 49, 104,847,852 bytes) of the Google Play app, obtained from a download mirror and matched to the live Google Play listing on package ID, developer name and version. Work done: manifest and resources decoded without a source decode (apktool), a string pass across the eight primary classes dex files and the native library inventory. A shielding artifact (ijiami_1011.VData and libijiami_1011.so) is present, and the primary dex files are full-sized, so the string-level evidence is readable. The Google Play listing and the Data Safety card 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. Anything that depends on runtime behaviour is marked as such.

ID	Severity	Title
C1	MEDIUM	One code base, one backend and at least nine brand identities, with the controller not identifiable from the Play listing
C2	MEDIUM	The Data Safety panel says no data is collected and the package reads SMS, contacts, call log, location and notifications
C3	MEDIUM	More than fifteen advertising and analytics SDKs with no consent management platform, in a persistent process
H1	LOW	Baidu and Google Maps keys in the manifest
H2	MEDIUM	Compiled endpoints on Alibaba, Tencent, AutoNavi, Baidu and Umeng infrastructure for location and health related data
H3	MEDIUM	SMS content and notification metadata are processed for people who never installed the app
H4	MEDIUM	Ten debug, test and Bluetooth command activities exported without a permission in the production release
H5	HIGH	Cleartext traffic permitted for the whole app and user-installed certificates trusted with a pin override, on an app with 50 million installs
H6	LOW	allowBackup is true and both backup rule files are empty
M1	LOW	Test backend endpoint compiled into the production release
M2	LOW	The agreement string says Default Consent, which suggests a pre-ticked checkbox
M3	INFO	The English privacy policy URL is named default and shared across the brand cluster

Finding Status at a Glance

ID	Disclosed	This report	State on 14 November 2026
C1	CRITICAL	MEDIUM	No reply. Controller of the shared backend not identified.
C2	CRITICAL	MEDIUM	No reply. Contents leaving the device not shown.
C3	CRITICAL	MEDIUM	No reply. Start order of the SDKs not traced.
H1	HIGH	LOW	No reply. Restriction state of the keys not visible.
H2	HIGH	MEDIUM	No reply. Runtime routing by region not tested.
H3	HIGH	MEDIUM	No reply. Upload of message content not shown.
H4	HIGH	MEDIUM	No reply. Behaviour after start not tested.
H5	HIGH	HIGH	No reply. Kept at High by blast-radius escalation, computed band Medium.
H6	HIGH	LOW	No reply. Data stays in the user account.
M1	MEDIUM	LOW	No reply. Test host in release.
M2	MEDIUM	LOW	No reply. Checkbox state not established.
M3	MEDIUM	INFO	Not rated. Policy text not read.

Subject & Operator Analysis

HiWatch Pro is published by Shenzhen Well Fitness Management Technology Co,LTD. A public business directory lists the company at Room 908, Xinghe World, B Block Building, Yabao Road, Bantian, Buji Town, Longgang District, Shenzhen, and names it as a wearables manufacturer established in 2010. Both statements are UNVERIFIED against the package, which does not show a company address. A string in the resources names the QQ mailbox 866589978@qq.com in the feedback flow, and this is UNVERIFIED as the support contact. That mailbox bounced permanently as a delivery address.

The backend vendor operates jusonsmart.com and gulaike.com. Its legal identity was not found in the package or in public sources. The notice was redelivered to legend_wgl@yeah.net, which jusonsmart.com publishes as its contact. No data protection officer and no Article 27 representative was found.

A controller without an establishment in the Union is not covered by the one-stop-shop mechanism. The Austrian Datenschutzbehörde received the notice in copy.

Architecture & Data Flow

HiWatch Pro is a native Android app with eight primary classes dex files and 37 native libraries for each of arm64-v8a and armeabi-v7a, targeting API level 35 with a minimum of API level 26. The code lives under xfkj.fitpro, the namespace of the FitPro code base. The application element sets persistent to true, allowBackup to true and usesCleartextTraffic to true.

The app talks to its own backend on jusonsmart.com and gulaike.com, among them the configuration endpoint tomato.gulaike.com, and to a large set of advertising and analytics networks (C3) and Chinese cloud endpoints (H2). The endpoints tomato.gulaike.com/api/v1/convert/8bit and /convert/dial convert watch dial images, which suggests that a photo chosen as a watch face goes to the backend. Whether it does was not tested. A person in such a photo has no consent path of their own. The manifest holds exported debug activities (H4).

Engagement Summary

The notice REF HIWATCHPRO-2026-R1 was first sent to 866589978@qq.com and bounced permanently because the mailbox does not exist. The identical, unedited notice was redelivered on 23 August 2026 at 11:35 UTC from rfi.irfos@gmail.com to legend_wgl@yeah.net with dsb@dsb.gv.at and edps@edps.europa.eu in copy. It carried three critical findings, further high findings and three questions. A follow-up of 12 September 2026 restated the open findings and set 19 September 2026 as the date 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 the redelivery address.

Findings

C1: One code base, one backend and at least nine brand identities, with the controller not identifiable from the Play listing

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 application class is xfkj.fitpro.application.MyApplication and not a hiwatchpro namespace. The manifest declares WeChat callback activities for seven package identities in the same APK: cn.xiaofengkj.fitpro, com.majia.alading.watch, com.majia.daku.sports.watch, com.legend.youhuo.watch, com.legend.superband.watch, com.legend.hiwatchpro.app and com.legend.hiwtchMax.app. The dex strings name an eighth, com.legend.mywatch.commonlib, which matches MyWatch+ on Google Play under the same publisher. A remote configuration URL serves settings per brand and takes the brand as the name parameter, so one backend host answers for every brand registered against it. A ninth identity, FontaFitPlus, appears through a privacy policy URL on a German domain. The privacy policy URLs sit on the backend vendor's domain app.jusonsmart.com and not on the publisher's own site, and the English one is named privacy_en_default.html while the Chinese one is named for HiWatch Pro. The Google Play publisher of record is Shenzhen Well Fitness Management Technology Co,LTD. Which company operates jusonsmart.com and gulaike.com, and whether it is a joint controller with the publisher, is not shown by any file. The sibling app FitPro (cn.xiaofengkj.fitpro, see the FitPro report of this package) is built from the same code base and uses the same backend.

```
android:name="xfkj.fitpro.application.MyApplication"

<activity android:name="cn.xiaofengkj.fitpro.wxapi.WXEntryActivity" .../>
<activity android:name="com.majia.alading.watch.wxapi.WXEntryActivity" .../>
<activity android:name="com.majia.daku.sports.watch.wxapi.WXEntryActivity" .../>
<activity android:name="com.legend.youhuo.watch.wxapi.WXEntryActivity" .../>
<activity android:name="com.legend.superband.watch.wxapi.WXEntryActivity" .../>
<activity android:name="com.legend.hiwatchpro.app.wxapi.WXEntryActivity" .../>
<activity android:name="com.legend.hiwtchMax.app.wxapi.WXEntryActivity" .../>

com.legend.mywatch.commonlib   (dex string)
https://tomato.gulaike.com/api/v1/config/app?name=%1$s&type=1&version=%2$s&platform=%3
    $d

https://d-parts.de/privacy_fontafitplus
https://www.d-parts.de/fontafitplus_help

<string name="privacy_cn">https://app.jusonsmart.com/public/privacy_cn_hiwatchpro.html
    </string>
<string name="privacy_en">https://app.jusonsmart.com/public/privacy_en_default.html</
    string>
```

Impact: A person who wants to ask who holds their data is shown one company on Google Play and finds that the app and its policy belong to a backend vendor under another domain, shared with at least eight other brands.

Fix: Name the controller of the shared backend, state whether the publisher and the vendor are joint controllers and publish a policy for each brand.

C2: The Data Safety panel says no data is collected and the package reads SMS, contacts, call log, location and notifications

---

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 CRITICAL on 23 August 2026

The Google Play Data Safety card for com.legend.hiwatchpro.app states that the app may share Contacts with third parties and, on the same card, that the developer says the app does not collect user data. The two statements contradict each other before the package is opened. The manifest requests READ_CONTACTS, READ_CALL_LOG, READ_SMS, RECEIVE_SMS, CALL_PHONE, ANSWER_PHONE_CALLS, READ_PHONE_STATE, READ_PRIVILEGED_PHONE_STATE, CAMERA, ACCESS_FINE_LOCATION, READ_LOGS and AD_ID. App-owned classes use the data: xfkj.fitpro.receiver.SmsObserver and xfkj.fitpro.service.SmsService, direct ContactsContract references and the notification listener xfkj.fitpro.service.NotifyService. Whether the contents leave the device is not shown. The label speaks of collection, and reading the data is already collection in the sense of the Android definition.

```
READ_CONTACTS  READ_CALL_LOG  READ_SMS  RECEIVE_SMS  CALL_PHONE  ANSWER_PHONE_CALLS
READ_PHONE_STATE  READ_PRIVILEGED_PHONE_STATE  CAMERA  ACCESS_FINE_LOCATION  READ_LOGS
      com.google.android.gms.permission.AD_ID

Lxfkj/fitpro/receiver/SmsObserver;
Lxfkj/fitpro/service/SmsService;
android.provider.ContactsContract$Contacts, $CommonDataKinds$Phone, $PhoneLookup

<service android:name="xfkj.fitpro.service.NotifyService"
    android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE">
  <intent-filter><action android:name="android.service.notification.
    NotificationListenerService" .../></intent-filter>
</service>
```

Impact: The label is the place where a user decides whether to install. A person who reads that nothing is collected installs an app that reads their messages, contacts and call history.

Fix: Correct the Data Safety declaration to the permissions and classes in the package and explain each data type in the policy.

C3: More than fifteen advertising and analytics SDKs with no consent management platform, in a persistent process

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 CRITICAL on 23 August 2026

The application element sets android:persistent to true and android:usesCleartextTraffic to true. The manifest and native libraries hold the SDKs in the table below, among them ByteDance Pangle, Alimama TANX, Kuaishou, Tencent Klevin and GDT, Umeng, Alibaba SLS, Mintegral, TopOn, Sigmob and the advertising channels of Xiaomi, Huawei, OPPO and vivo. A search of the decoded resources for OneTrust, Didomi, Usercentrics and IABTCF returned no match. The launcher flow shows UserProtocolActivity before MenusActivity and MainActivity. Whether the SDKs start before or after that screen is not established, since no bytecode control-flow pass was done, and no SDK component carries a consent-gating attribute in the manifest. The package holds no billing library, so the product is ad financed. The vector models a local pre-consent collection with a low confidentiality impact.

SDK	Vendor	Evidence
Pangle / openadsdk	ByteDance	TT_PANGOLIN permission, ZEUS_PLUGIN_PANGLE meta-data, libpangleflipped.so
Douyin live plugin	ByteDance	com.byted.live.lite.*, com.bytedance.android.openliveplugin.*
TANX	Alimama / Alibaba	com.alimm.tanx.*, libtanx.so
Kwad	Kuaishou	com.kwad.sdk.api.proxy.app.*
Klevin, GDT	Tencent	com.tencent.klevin.*, com.qq.e.*
Weibo SDK	Sina	libweibosdkcore.so, com.sina.weibo.sdk.*
Mobads	Baidu	com.baidu.mobads.sdk.api.*
Umeng, SLS, AMap	Alibaba	UMENG_CHANNEL = hiwatchProCN, SLSContentProvider, libsls_producer.so, libAMapSDK_MAP_v8_1_0.so
Bugly	Tencent	libBugly_Native.so
Mintegral, AnyThink / TopOn, Sigmob	Mintegral, TopOn, Sigmob	com.mbridge.msdk.*, com.anythink.*, com.sigmob.sdk.*
Mimo, TapAd, JD ads	Xiaomi, TapTap, JD.com	com.miui.zeus.mimo.sdk.*, com.tapsdk.tapad.*, com.jd.ad.sdk.*
Huawei, OPPO, vivo ads	Huawei, OPPO, vivo	com.huawei.openalliance.ad.*, com.opos.*, com.heytap.msp.mobad.*, com.vivo.mobilead.*, libvivoantisdk.so

Impact: The people who wear the watch are users of a product that is paid for by advertising.

They meet more than fifteen advertising networks in the binary and no consent platform that would let them decline before those networks run.

Fix: Add a consent management platform, start advertising and analytics SDKs only after the choice and drop the persistent flag.

H1: Baidu and Google Maps keys in the manifest

LOW, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:P/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N, 2.3 (CVSS-B), disclosed as HIGH on 23 August 2026

The manifest carries a Baidu LBS key and a Google geo key as plain meta-data values. Both ship in every install of an app with 50 million installs. The restriction state of the keys cannot be seen from the package, and the burden of showing it lies with the operator under Art. 5(2). The exposure is availability of the map and location functions through quota use. No request was made with either key.

```
<meta-data android:name="com.baidu.lbsapi.API_KEY" android:value="
    Rb9C4HCwYC6dhUhHKFhX3Z9mD20lfPu5"/>
<meta-data android:name="com.google.android.geo.API_KEY" android:value="
    AIzaSyDeKF6XaKcF2EErEHxlCpLB-72m44k4U30"/>
```

Impact: A third party can use the operator’s map quota, which affects availability for all users and does not expose user data.

Fix: Restrict the Google key by package name and signing certificate, restrict the Baidu key and rotate both.

H2: Compiled endpoints on Alibaba, Tencent, AutoNavi, Baidu and Umeng infrastructure for location and health related 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 dex strings hold endpoints on Alibaba Cloud SLS in Guangzhou, Tencent Cloud Bugly, AutoNavi location, Baidu map and Umeng. The app has screens for ECG, SpO2, heart rate and temperature (ECGMeasureActivity, SpoMeasureActivity, HeartMeasureActivity, TempHistoryActivity). The endpoints are compiled into reachable code. Whether traffic of a user in the Union goes to the Chinese endpoints at runtime or to a regional equivalent was not tested, and the resources hold no logic that routes by user region. The beian.miit.gov.cn host in the list is the Chinese ICP registry and is not a data endpoint. The report does not assess PRC law. The finding is the absence of a named transfer mechanism for a stack of Chinese cloud endpoints.

```
https://cn-guangzhou.log.aliyuncs.com          (Alibaba Cloud SLS, log ingestion)
https://astat.bugly.qcloud.com                 (Tencent Cloud crash and behaviour
    telemetry)
https://apilocate.amap.com   https://abroad.apilocate.amap.com   (AutoNavi location)
https://api.map.baidu.com   https://client.map.baidu.com        (Baidu)
https://alogsus.umeng.com   https://ccs.umeng.com               (Umeng analytics)
https://beian.miit.gov.cn                                      (ICP registry)
```

Impact: Health and location data of people in the Union may meet Chinese cloud platforms with no mechanism named in front of the user.

Fix: Name each recipient with country and transfer mechanism and publish the transfer impact assessment.

H3: SMS content and notification metadata are processed for people who never installed the app

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 app registers its own SMS receiver and service pair, the intent android.provider. Telephony.SMS_RECEIVED and the notification listener NotifyService with priority 1000. The sender of an SMS or the counterpart in a messenger notification is not the account holder and saw no consent screen. The sender number identifies the person, and notification text can hold names. Whether the content stays on the Bluetooth link to the watch or also reaches UploadDataService and the backend is not shown, since the upload payload of that class was not read.

```
Lxfkj/fitpro/receiver/SmsObserver;
Lxfkj/fitpro/service/SmsService;
android.provider.Telephony.SMS_RECEIVED

<service android:name="xfkj.fitpro.service.NotifyService"
    android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE">
  <intent-filter><action android:name="android.service.notification.
    NotificationListenerService" android:priority="1000"/></intent-filter>
</service>
```

Impact: People who text the user or write in a messenger have their number, name and message text shown on a watch and possibly processed further, and they were never asked.

Fix: State that message content stays on the Bluetooth link, or name the recipient and the legal basis, and restrict the listener to the apps the user selects.

H4: Ten debug, test and Bluetooth command activities exported without a permission in the production release

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 HIGH on 23 August 2026

The manifest declares ten activities under xfkj.fitpro.activity.debug, xfkj.fitpro.activity and xfkj.fitpro.activity.test with exported true and no permission, among them BluetoothCommandActivity, ApiDebugActivity and DebugFunctionActivity. Any other app on the phone can start them by component name. The name BluetoothCommandActivity suggests that it issues commands to the paired watch. What it does after the start, and whether it takes Intent extras, was not tested. The list matches the debug screens of the FitPro report of this package, which shares the code base.

```
xfkj.fitpro.activity.debug.ClockDialListDebugActivity
xfkj.fitpro.activity.debug.WatchTimeCheckActivity
xfkj.fitpro.activity.debug.BluetoothCommandActivity
xfkj.fitpro.activity.debug.PictureCropTestActivity
xfkj.fitpro.activity.debug.LocalFunctionTestActivity
xfkj.fitpro.activity.debug.DebugFunctionActivity
xfkj.fitpro.activity.debug.OtherBluetoothDebugActivity
xfkj.fitpro.activity.debug.ApiDebugActivity
xfkj.fitpro.activity.DebugUIActivity
xfkj.fitpro.activity.test.FileSendFilesActivity
(all with android:exported="true" and no android:permission)
```

Impact: Developer tools of a health watch app can be opened by another app on the phone, and a build that ships them shows that the release process does not strip them.

Fix: Remove the debug and test activities from the release build or set exported to false.

H5: Cleartext traffic permitted for the whole app and user-installed certificates trusted with a pin override, on an app with 50 million installs

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 HIGH on 23 August 2026, rated HIGH by blast-radius escalation

res/xml/network_security_config.xml consists of a base-config with cleartextTrafficPermitted set to true and two trust anchors with overridePins true, one for the system store and one for the user store. The application element also sets usesCleartextTraffic to true. No domain-config exists, so this is the single policy for every endpoint. The app targets API level 35, where cleartext HTTP is refused by default. Any certificate authority that a user or an attacker adds to the device store can therefore intercept traffic that a pin would otherwise protect. Whether a given endpoint is called over plain HTTP was not tested and no traffic was captured. The score reflects an attacker on the same network path and the need for the app to use an http:// address. The sibling FitPro, built from the same code base, shows a plain HTTP payment endpoint and a plain WebSocket to the shared backend. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.3 to HIGH because the app is positioned to carry health readings, location, message content and account traffic, it has more than 50 million installs on Google Play, the override covers every host and the user trust anchor with pin override removes the protection of any pinning.

```
<network-security-config>
    <base-config cleartextTrafficPermitted="true">
        <trust-anchors>
            <certificates overridePins="true" src="system" />
            <certificates overridePins="true" src="user" />
        </trust-anchors>
    </base-config>
</network-security-config>

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

Impact: The app is positioned to carry health readings, precise location, text message content, contacts and account traffic. A plain HTTP request to any host travels in the open on a shared Wi-Fi network or a hostile access point. For a person who wears the watch all day, the data at stake is the most personal kind a phone holds.

Fix: Remove the base-config override and the application flag, remove the user trust anchor with pin override, pin the first-party hosts and verify that every endpoint in the dex strings uses https.

H6: allowBackup is true and both backup rule files are empty

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 HIGH on 23 August 2026

The application element sets android:allowBackup to true and references data_extraction_rules.xml and backup_rules.xml. The first holds an empty cloud-backup element and the second an empty full-backup-content element, so no exclusion rule exists. The private storage of the app, which can hold health measurements, cached contact and message derived data, auth tokens and Bluetooth pairing state, is therefore eligible for backup to the user's Google account. The data stays in the user's own account, which explains the low score. Which files the app writes was not examined.

```
<application android:allowBackup="true" android:dataExtractionRules="@xml/
    data_extraction_rules" android:fullBackupContent="@xml/backup_rules" ...>

<!-- data_extraction_rules.xml -->
<data-extraction-rules><cloud-backup /></data-extraction-rules>
<!-- backup_rules.xml -->
<full-backup-content />
```

Impact: No decision was made about which of the user's health and account files belong in a backup.

Fix: Set allowBackup to false or exclude tokens, pairing state and health data in the rule files.

M1: Test backend endpoint compiled into the production release

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

The dex strings hold the host iot-test.wasumedia.cn with the path of a third-party cloud push management integration. A test subdomain in a release with 50 million installs is either live traffic through a non-production environment or dead code. Both are release hygiene gaps. The same endpoint appears in the FitPro report of this package.

```
https://iot-test.wasumedia.cn/thirdCloud/connect/manager/open/push
```

Impact: A release that carries a test host shows weak separation between test and production.

Fix: Remove the test host from the release build.

M2: The agreement string says Default Consent, which suggests a pre-ticked checkbox

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

res/values/strings.xml holds the string agree_user_protocol with the wording Default Consent to the User Agreement. The wording fits a checkbox that starts in the agreed state. The layout file was not found in the resource decode, and the default state is most likely set in code, so the actual state of the checkbox is not established.

```
<string name="agree_user_protocol">Default Consent toUser Agreement</string>
```

Impact: A user who does not look at the box has agreed to the legal text, if the box starts ticked.

Fix: Start the checkbox unticked and require an active choice.

M3: The English privacy policy URL is named default and shared across the brand cluster

INFO, no CVSS v4.0 score assigned, observation, not rated, disclosed as MEDIUM on 23 August 2026

The resource privacy_en points to privacy_en_default.html on app.jusonsmart.com, while the Chinese policy is named for HiWatch Pro. The file name suggests an English text reused across the brands of C1. The policy text itself was not read in this analysis, so its specificity is not assessed, and the report records the file naming as an observation and does not rate it.

```
<string name="privacy_cn">https://app.jusonsmart.com/public/privacy_cn_hiwatchpro.html
    </string>
<string name="privacy_en">https://app.jusonsmart.com/public/privacy_en_default.html</
    string>
```

Impact: A user in the Union who wants to learn about this one product reads a text with a name that does not mention it.

Fix: Publish a policy that names the product and the controller.

Impact Analysis

The people affected are the users of a smartwatch companion app with more than 50 million installs, which includes minors under the PEGI 3 rating. A search of the decoded resources for birth date, age gate, parental control and COPPA terms returned no match, so no mechanism that distinguishes a child from an adult was found. The app handles ECG, SpO2, heart rate and temperature screens, precise location, SMS, contacts and call log.

The weight of the case sits on three points. The Play label says that no data is collected while the package reads messages, contacts, call history and location (C2). The code base and the backend are shared with at least eight other brands, and the controller is not identified (C1). Cleartext traffic is permitted for every host and user certificates override pins (H5).

The package shows classes, endpoints, permissions and text. No message, contact or health reading was observed leaving a device, and the report asserts no such flow. The app declares no RECORD_AUDIO permission and the analysis found no audio capture path.

The Complete Chain

Step 1, install: a user installs the app after reading a Play label that says no data is collected (C2).

Step 2, start-up: the persistent process starts and more than fifteen advertising and analytics SDKs are present with no consent platform. The order of calls was not traced (C3).

Step 3, brand and configuration: the app asks the configuration backend for its settings by brand name (C1).

Step 4, features: SMS and notification content is mirrored to the watch (H3) and a watch face photo may go to the conversion endpoint.

Step 5, network: traffic goes to Chinese cloud and map endpoints (H2) and cleartext is allowed for all of them (H5).

Step 6, local exposure: other apps on the phone can open ten debug and test activities (H4) and a backup rule set that excludes nothing applies (H6).

Step 7, rights: a person who wants to ask who holds the data is shown one publisher and a policy on the domain of a different company (C1).

Shared Chipset or Platform Fingerprint

HiWatch Pro is one output of the FitPro code base. The application class, the debug activities, the test endpoint and the backend vendor match the FitPro report of this package. The Bluetooth service UUID is the cluster-detection key. The signing certificate is unique to HiWatch Pro and differs from the FitPro certificate, which each brand signs on its own. The multi-vendor chipset table of the FitPro report applies to the same code base. It was not re-derived for this package.

```
Application class       xfkj.fitpro.application.MyApplication
BLE service UUID        0000fee7-0000-1000-8000-00805f9b34fb
Signing cert SHA-256    1
    e60c0455d08f3c692347295bde9687be0bd708487a6590fbfd63871c17945cd
Signing DN              CN=hiwatchPro, OU=hiwatchPro, O=hiwatchPro, L=Shenzhen, ST=
    Guangdong, C=86
Brand packages          cn.xiaofengkj.fitpro, com.majia.alading.watch, com.majia.daku.
    sports.watch, com.legend.youhuo.watch, com.legend.superband.watch, com.legend.
    hiwatchpro.app, com.legend.hiwtchMax.app
Further brand strings   com.legend.mywatch.commonlib (MyWatch+), FontaFitPlus
Same-publisher apps     fitpro, AIXcore, SuperBand, FitPro2, Hyper watch, MyWatch+
Configuration backend   https://tomato.gulaike.com/api/v1/config/app?name=%1$s&type=1&
    version=%2$s&platform=%3$d
Policy host             app.jusonsmart.com
Shielding artifact      ijiami_1011.VData, libijiami_1011.so
```

Data Protection: Article by Article

Article 4(7) and Article 26, controller and joint controllers: engaged by C1.

Article 4(11) and Article 7(1), consent: engaged by C3 and M2.

Article 5(1)(a), lawfulness, fairness and transparency: engaged by C1, C2 and C3.

Article 5(1)(c), data minimisation: engaged by H3.

Article 5(2), accountability: engaged by C3 and H1.

Article 6: engaged by C3 and H3.

Articles 12(1), 13 and 14: engaged by C1, C2, H3 and M3. Article 13(1)(a) is engaged by C1.

Article 25: engaged by H1 and H6.

Article 32(1)(a) and (b): engaged by H1, H4, H5, H6 and M1.

Article 35: engaged by H2. A data protection impact assessment is not published.

Articles 44 and 46: engaged by H2. The package names no mechanism.

No Article 27 representative is named.

Platform Accountability & DSA

The Data Safety card of HiWatch Pro says that Contacts may be shared with third parties and, on the same card, that the developer says the app does not collect user data. It also says that data is encrypted in transit and that deletion can be requested. The package requests permissions for SMS, contacts, call log, camera and location, and the app-owned classes use SMS and contacts (C2). The statement on encryption in transit sits against a package that permits cleartext for every host (H5). A screenshot of the card is on file. The label was not re-read after 23 August 2026.

Google Play is an online platform under Regulation (EU) 2022/2065. Any person can submit a notice about the Data Safety declaration under 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

The publisher offers the app to users in the Union through Google Play with interface languages that include the major languages of the Union, so Art. 3(2) of the GDPR applies. No main establishment in the Union is identified, 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, 26, 27, 32 and 35 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 notice raised the access powers that PRC law gives to PRC-domiciled processors as a risk factor for Chapter V. The report records it as context and does not assess PRC law. 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            com.legend.hiwatchpro.app
Version            1.3.72 (versionCode 49), 104,847,852 bytes, minSdk 26, targetSdk 35
APK SHA-256        3e340dc48c896698418706973b3399733da257b50cb640e3955c910e6d89022a
Signing cert SHA-256  1e60c0455d08f3c692347295bde9687be0bd708487a6590fbfd63871c17945cd
Audit device       none, the app was not installed
```

```
Baidu LBS key        Rb9C4HCwYC6dhUhHKFhX3Z9mD20lfPu5
Google geo key       AIzaSyDeKF6XaKcF2EErEHxlCpLB-72m44k4U30
Config endpoint      https://tomato.gulaike.com/api/v1/config/app?name=%1$s&type=1&
    version=%2$s&platform=%3$d
Backend hosts        jusonsmart.com, gulaike.com, app.jusonsmart.com, tomato.gulaike.
    com, hiapi.jusonsmart.com
Dial conversion      tomato.gulaike.com/api/v1/convert/8bit, tomato.gulaike.com/api/v1/
    convert/dial
Chinese cloud        https://cn-guangzhou.log.aliyuncs.com, https://astat.bugly.qcloud.
    com, https://apilocate.amap.com, https://abroad.apilocate.amap.com, https://api.
    map.baidu.com, https://client.map.baidu.com, https://alogsus.umeng.com, https://
    ccs.umeng.com
Test host            https://iot-test.wasumedia.cn/thirdCloud/connect/manager/open/push
Policy URLs          https://app.jusonsmart.com/public/privacy_cn_hiwatchpro.html,
    https://app.jusonsmart.com/public/privacy_en_default.html, https://d-parts.de/
    privacy_fontafitplus
Contacts             legend_wgl@yeah.net (redelivery address), 866589978@qq.com (
    bounced)
```

```
C1  AndroidManifest.xml (WXEntryActivity list), dex string pool (config endpoint), res
    /values/strings.xml
C2  Google Play Data Safety card, AndroidManifest.xml (permissions), dex string pool (
    SmsObserver, SmsService)
C3  AndroidManifest.xml, lib/arm64-v8a, resource search for consent platforms
H1  AndroidManifest.xml (meta-data)
H2  dex string pool (endpoints)
H3  AndroidManifest.xml (NotifyService), dex string pool
H4  AndroidManifest.xml (exported activities)
H5  res/xml/network_security_config.xml, AndroidManifest.xml
H6  AndroidManifest.xml, res/xml/data_extraction_rules.xml, res/xml/backup_rules.xml
M1  dex string pool (iot-test.wasumedia.cn)
M2  res/values/strings.xml (agree_user_protocol)
M3  res/values/strings.xml (privacy_en, privacy_cn)
```

Reproduction: obtain com.legend.hiwatchpro.app 1.3.72 (49), check the SHA-256 value above, decode 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 HIWATCHPRO-2026-R1 first sent to 866589978@qq.com, which bounced permanently because the mailbox does not exist. The identical notice was redelivered on this date at 11:35 UTC to legend_wgl@yeah.net, CC dsb@dsb.gv.at and edps@edps.europa.eu. Three questions.

2026-09-12 Follow-up at 17:06 UTC, 20 days after the redelivery, with the open findings restated and the three questions due on 19 September 2026.

2026-10-17 Second follow-up from security@rfi-irfos.com at 19:05 UTC, 35 days before publication, with the three questions unchanged in substance.

2026-11-14 No reply of any kind and no delivery failure on the redelivery address.

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

What Was Done Well

The package declares no RECORD_AUDIO permission and holds no audio capture path, which is a verified negative for a wearable category where acoustic sensing is a documented pattern. A first-launch agreement screen (UserProtocolActivity) and a descriptive permission dialog for Bluetooth and device information exist. The Data Safety card states that deletion can be requested, and nothing found in the package contradicts it.

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 1.3.72. A final APK diff before 21 November 2026 determines the state that the published report records.

Recommendations in order of effect. First, correct the Data Safety declaration to the permissions and classes in the package (C2). Second, remove the global cleartext allowance and the user trust anchor with pin override (H5). Third, name the controller of the shared backend and publish a policy for each brand (C1). Fourth, add a consent management platform and start the SDKs after the choice (C3). Fifth, remove the debug and test activities and the test host from the release build (H4, M1). Sixth, name each Chinese recipient with country and transfer mechanism (H2) and state where message content goes (H3). Seventh, restrict the keys, set backup rules and start the agreement checkbox unticked (H1, H6, 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 HIWATCHPRO-2026-R1.