ANDROID STATIC ANALYSIS REPORT

JYouPro (3.38.3)

File Name:	com.jaga.ibraceletplus.aigoband_613.apk
Package Name:	com.jaga.ibraceletplus.aigoband
Scan Date:	Aug. 30, 2025, 10:17 p.m.

App Security Score:	40/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
6	16	1	1	5

FILE INFORMATION

File Name: com.jaga.ibraceletplus.aigoband_613.apk
Size: 14.64MB
MD5: cd96fdd062a57b571351ece5b7f0b85d
SHA1: b3d436f06c68fedb99440871bb2571f74f0bd372
SHA256: 601c7561c4a38ce2a6c90d31a7bda69a47bef7c860e0b28696a910ef17ac01f2

APP INFORMATION

App Name: JYouPro
Package Name: com.jaga.ibraceletplus.aigoband
Main Activity: com.jaga.ibraceletplus.aigoband.sign.SplashActivity
Target SDK: 34
Min SDK: 21
Max SDK:
Android Version Name: 3.38.3
Android Version Code: 613

APP COMPONENTS

Activities: 76
Services: 7
Receivers: 2
Providers: 5
Exported Activities: 2
Exported Services: 1
Exported Receivers: 0
Exported Providers: 1

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=CN, ST=guangdong, L=shenzhen, O=keeprapid, OU=keeprapid, CN=keeprapid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-09-11 09:43:37+00:00
Valid To: 2042-01-27 09:43:37+00:00
Issuer: C=CN, ST=guangdong, L=shenzhen, O=keeprapid, OU=keeprapid, CN=keeprapid
Serial Number: 0x43ded068
Hash Algorithm: sha256
md5: 7eeb76a0cc2e15fc5f6307d8c561f0de
sha1: 08d6c912f0f08d9902e7e545e8c9131bb68537ad
```

sha256: c7486419f1c312ef1874df208ce8187d45b7bc6d8e6135396e0ea696df08d08c
sha512: 298d2b2a4c86590a38af44f90b7970d6bbda380758ca0894d32f6a38e14acfa7eccd5c536c0c86d5346a4cfc38656a77c59f15a8e528c967b139b4376e42e4ff
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 870f8518fec6e6e12de40a1efe23fcf7aea68350eb96994ae39982c22bcc1b57
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.READ_CALL_LOG	dangerous	grants read access to the user's call log.	Allows an application to read the user's call log.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.ANSWER_PHONE_CALLS	dangerous	permits an app to answer incoming phone calls.	Allows the app to answer an incoming phone call.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_CONNECTED_DEVICE	normal	enables foreground services with connected device use.	Allows a regular application to use Service.startForeground with the type "connectedDevice".
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.DISABLE_KEYGUARD	normal	disable keyguard	Allows applications to disable the keyguard if it is not secure.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_MEDIA_AUDIO	dangerous	allows reading audio files from external storage.	Allows an application to read audio files from external storage.
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.MEDIA_CONTENT_CONTROL	normal	allows control over media content playback.	Allows an application to know what content is playing and control its playback.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.BRAND check
Build.DEVICE check
Build.PRODUCT check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.BOARD check
possible Build.SERIAL check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.jaga.ibraceletplus.aigoband,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **1** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS

HIGH: **2** | WARNING: **5** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Activity (com.jaga.ibraceletplus.aigoband.main.DupMainActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Content Provider (com.facebook.FacebookContentProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

HIGH: **4** | WARNING: **8** | INFO: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				butterknife/ButterKnife.java c/b.java c/c.java c/d.java c/e.java c/g.java com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/ImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/dlazaro66/qrcodereaderview/QRCodeReaderView.java com/gaoxin/a/s.java com/gaoxin/proxy/a.java com/gaoxin/proxy/controller/EcgDspProxy.java com/github/paolorotolo/appintro/AppIntroBase.java com/j256/ormlite/android/AndroidLog.java com/j256/ormlite/android/apptools/OrmLiteConfigUtil.java com/j256/ormlite/logger/LocalLog.java com/jaga/ibraceletplus/aigoband/AppMng.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/jaga/ibraceletplus/aigoband/BaseActivity.java com/jaga/ibraceletplus/aigoband/BaseFragment.java com/jaga/ibraceletplus/aigoband/IBraceletplusSQLiteHelper.java com/jaga/ibraceletplus/aigoband/camera/CameraActivity.java com/jaga/ibraceletplus/aigoband/camera/DecoderActivity.java com/jaga/ibraceletplus/aigoband/camera/Preview.java com/jaga/ibraceletplus/aigoband/detail/DetailActivity.java com/jaga/ibraceletplus/aigoband/detail/DetailBloodActivity.java com/jaga/ibraceletplus/aigoband/detail/DetailBodyTemperatureActivity.java com/jaga/ibraceletplus/aigoband/detail/DetailHeartActivity.java com/jaga/ibraceletplus/aigoband/detail/DetailOxygenActivity.java com/jaga/ibraceletplus/aigoband/detail/DetailSleepActivity.java com/jaga/ibraceletplus/aigoband/detail/DetailSportActivity.java com/jaga/ibraceletplus/aigoband/detail/DetailWalkActivity.java com/jaga/ibraceletplus/aigoband/dslv/DragSortListView.java com/jaga/ibraceletplus/aigoband/ecg/EcgHistoryActivity.java com/jaga/ibraceletplus/aigoband/ecg/EcgHistoryHeartActivity.java com/jaga/ibraceletplus/aigoband/ecg/EcgReportActivity.java com/jaga/ibraceletplus/aigoband/ecg/EcgSessionHistoryActivity.java com/jaga/ibraceletplus/aigoband/ecg/EcgShareActivity.java com/jaga/ibraceletplus/aigoband/ecg/EcgTestActivity.java com/jaga/ibraceletplus/aigoband/ecg/EcgXtTestActivity.java com/jaga/ibraceletplus/aigoband/googlefit/GoogleFitActivity.java com/jaga/ibraceletplus/aigoband/guide/BirthFragment.java com/jaga/ibraceletplus/aigoband/guide/GoalFragment.java com/jaga/ibraceletplus/aigoband/guide/GuideActivity.java com/jaga/ibraceletplus/aigoband/guide/HeightFragment.java com/jaga/ibraceletplus/aigoband/guide/WeightFragment.java com/jaga/ibraceletplus/aigoband/main/DupMainActivity.java com/jaga/ibraceletplus/aigoband/main/FragmentMain.java com/jaga/ibraceletplus/aigoband/main/FragmentPerson.java com/jaga/ibraceletplus/aigoband/main/FragmentSetting.java com/jaga/ibraceletplus/aigoband/ota/BluetoothGattReceiver.java com/jaga/ibraceletplus/aigoband/ota/BluetoothManager.java com/jaga/ibraceletplus/aigoband/ota/Callback.java com/jaga/ibraceletplus/aigoband/ota/DeviceConnectTask.java com/jaga/ibraceletplus/aigoband/ota/File.java com/jaga/ibraceletplus/aigoband/ota/OtaActivity.java com/jaga/ibraceletplus/aigoband/ota/OtaWallpaperActivity.java com/jaga/ibraceletplus/aigoband/ota/SuCallback.java com/jaga/ibraceletplus/aigoband/ota/SuotaManager.java com/jaga/ibraceletplus/aigoband/service/LocationService.java com/jaga/ibraceletplus/aigoband/service/MusicControlService.java com/jaga/ibraceletplus/aigoband/service/NLService.java com/jaga/ibraceletplus/aigoband/service/SampleBleService.java com/jaga/ibraceletplus/aigoband/sign/ForgetPwdActivity.java com/jaga/ibraceletplus/aigoband/sign/LoginActivity.java com/jaga/ibraceletplus/aigoband/sign/RegisterActivity.java com/jaga/ibraceletplus/aigoband/sport/WechatSportActivity.java com/jaga/ibraceletplus/aigoband/theme/dup/ChangePasswordActivity.java com/jaga/ibraceletplus/aigoband/theme/dup/CustomWallpaperA

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/jaga/ibraceletplus/aigoband/theme/dup/CustomWallpaperActivity.java com/jaga/ibraceletplus/aigoband/theme/dup/DialMarketActivity.java com/jaga/ibraceletplus/aigoband/theme/dup/ECardSimpleActivity.java com/jaga/ibraceletplus/aigoband/theme/dup/NotifyActivity.java com/jaga/ibraceletplus/aigoband/theme/dup/SmsRspSimpleActivity.java com/jaga/ibraceletplus/aigoband/theme/dup/UserInfoActivity.java com/jaga/ibraceletplus/aigoband/util/CheckUtil.java com/jaga/ibraceletplus/aigoband/util/EcgUtil.java com/jaga/ibraceletplus/aigoband/util/RomUtil.java com/jaga/ibraceletplus/aigoband/util/SoundPlayUtil.java com/jaga/ibraceletplus/aigoband/util/SysUtil.java com/jaga/ibraceletplus/aigoband/util/WeatherUtil.java com/jaga/ibraceletplus/aigoband/widget/HeartPolylineView.java com/keeprapid/serverdataload/server/ServerDataLoad.java com/king/zxing/util/LogUtils.java com/loopj/android/http/ConscryptSSLProvider.java com/loopj/android/http/LogHandler.java com/luck/picture/lib/loader/LocalMediaPageLoader.java com/luck/picture/lib/thread/PictureThreadUtils.java com/luck/picture/lib/utils/PSEglUtils.java com/luck/picture/lib/utils/PictureFileUtils.java com/sxr/sdk/ble/keepfit/ecg/EcgUtil.java com/sxr/sdk/ble/keepfit/ecg/EcgView.java com/sxr/sdk/ble/keepfit/service/BluetoothLeService.java com/sxr/sdk/ble/keepfit/service/OtaDial.java com/sxr/sdk/ble/keepfit/service/a.java com/yalantis/ucrop/UCropActivity.java com/yalantis/ucrop/task/BitmapCropTask.java com/yalantis/ucrop/task/BitmapLoadTask.java com/yalantis/ucrop/util/BitmapLoadUtils.java com/yalantis/ucrop/util/EglUtils.java com/yalantis/ucrop/util/FileUtils.java com/yalantis/ucrop/util/ImageHeaderParser.java com/yalantis/ucrop/view/TransformImageView.java cz/msebera/android/httpclient/conn/util/PublicSuffixMatcherLoader.java cz/msebera/android/httpclient/extras/HttpClientAndroidLog.java cz/msebera/android/httpclient/extras/PRNGFixes.java cz/msebera/android/httpclient/impl/conn/DefaultClientConnection.java cz/msebera/android/httpclient/impl/conn/LoggingManagedHttpClientConnection.java cz/msebera/android/httpclient/impl/execchain/MainClientExec.java d/e.java d/g.java ezy/boost/update/UpdateUtil.java lecho/lib/hellocharts/formatter/ValueFormatterHelper.java lecho/lib/hellocharts/view/BubbleChartView.java lecho/lib/hellocharts/view/ColumnChartView.java lecho/lib/hellocharts/view/ComboLineColumnChartView.java lecho/lib/hellocharts/view/LineChartView.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				lecho/lib/hellocharts/view/LineChartView.java lecho/lib/hellocharts/view/PieChartView.java lecho/lib/hellocharts/view/PreviewColumnChartView.java lecho/lib/hellocharts/view/PreviewLineChartView.java net/grandcentrix/tray/core/AbstractTrayPreference.java net/grandcentrix/tray/core/Preferences.java net/grandcentrix/tray/core/SharedPreferencesImport.java net/grandcentrix/tray/core/TrayLog.java net/grandcentrix/tray/provider/ContentProviderStorage.java net/grandcentrix/tray/provider/TrayContentProvider.java net/grandcentrix/tray/provider/TrayContract.java net/grandcentrix/tray/provider/TrayDBHelper.java no/nordicsemi/android/dfu/DfuBaseService.java top/zibin/luban/Checker.java top/zibin/luban/Luban.java top/zibin/luban/LubanUtils.java top/zibin/luban/io/LruArrayPool.java
2	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/jaga/ibraceletplus/aigoband/util/ConvertUtil.java com/jaga/ibraceletplus/aigoband/util/MD5Util.java com/jaga/ibraceletplus/aigoband/util/SysUtil.java com/luck/picture/lib/loader/SandboxFileLoader.java cz/msebera/android/httpclient/impl/auth/NTLMEngineImpl.java d/g.java ezy/boost/update/UpdateUtil.java
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/manager/RequestManagerRetriever.java com/hjq/permissions/StartActivityManager.java com/jaga/ibraceletplus/aigoband/camera/Preview.java com/jaga/ibraceletplus/aigoband/util/WeatherUtil.java com/keeprapid/serverdataload/model/Key.java com/king/zxing/Intents.java com/luck/picture/lib/config/PictureConfig.java cz/msebera/android/httpclient/impl/client/cache/FailureCacheValue.java net/grandcentrix/tray/core/SharedPreferencesImport.java net/grandcentrix/tray/provider/TrayContract.java net/grandcentrix/tray/provider/TrayDBHelper.java
4	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	com/loopj/android/http/MySSLSocketFactory.java cz/msebera/android/httpclient/conn/ssl/SSLConnectionSocketFactory.java cz/msebera/android/httpclient/conn/ssl/SSLSocketFactory.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/jaga/ibraceletplus/aigoband/camera/CameraActivity.java com/jaga/ibraceletplus/aigoband/dslv/DragSortListView.java com/jaga/ibraceletplus/aigoband/ota/File.java com/jaga/ibraceletplus/aigoband/sport/WechatSportActivity.java com/jaga/ibraceletplus/aigoband/theme/dup/CustomWallpaperActivity.java com/jaga/ibraceletplus/aigoband/theme/dup/UserInfoActivity.java com/jaga/ibraceletplus/aigoband/util/SysUtil.java com/luck/lib/camerax/utils/FileUtils.java com/luck/picture/lib/manager/PictureCacheManager.java com/luck/picture/lib/utils/DownloadFileUtils.java com/luck/picture/lib/utils/FileDirMap.java com/luck/picture/lib/utils/MediaStoreUtils.java com/luck/picture/lib/utils/PictureFileUtils.java com/sxr/sdk/ble/keepfit/service/a.java com/yalantis/ucrop/util/FileUtils.java d/g.java ezy/boost/update/UpdateDownloader.java ezy/boost/update/UpdateUtil.java top/zibin/luban/LubanUtils.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/loopj/android/http/MySSLSocketFactory.java cz/msebera/android/httpclient/conn/ssl/SSLContextBuilder.java cz/msebera/android/httpclient/ssl/SSLContextBuilder.java
7	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/j256/ormlite/android/AndroidCompiledStatement.java com/j256/ormlite/android/AndroidDatabaseConnection.java com/j256/ormlite/android/compat/ApiCompatibility.java com/j256/ormlite/android/compat/BasicApiCompatibility.java com/j256/ormlite/android/compat/JellyBeanApiCompatibility.java com/jaga/ibraceletplus/aigoband/IBraceletplusSQLiteHelper.java net/grandcentrix/tray/provider/TrayDBHelper.java
8	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/jaga/ibraceletplus/aigoband/camera/Preview.java com/loopj/android/http/FileAsyncHttpResponseHandler.java com/luck/lib/camerax/CustomCameraView.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/hjq/permissions/PermissionFragment.java com/jaga/ibraceletplus/aigoband/main/FragmentMain.java com/loopj/android/http/SimpleMultipartEntity.java com/scwang/smartrefresh/header/FunGameBattleCityHeader.java com/scwang/smartrefresh/header/TaurusHeader.java com/scwang/smartrefresh/header/storehouse/StoreHouseBarItem.java cz/msebera/android/httpclient/entity/mime/MultipartEntityBuilder.java cz/msebera/android/httpclient/impl/auth/NTLMEngineImpl.java
10	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	cz/msebera/android/httpclient/impl/auth/NTLMEngineImpl.java cz/msebera/android/httpclient/impl/client/cache/BasicIdGenerator.java
11	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/jaga/ibraceletplus/aigoband/theme/dup/HtmlContentActivity.java
12	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	cz/msebera/android/httpclient/conn/params/ConnRouteParams.java
13	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	lecho/lib/hellocharts/BuildConfig.java
14	Weak Encryption algorithm used	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	cz/msebera/android/httpclient/impl/auth/NTLMEngineImpl.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libhello.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
2	arm64-v8a/libnative-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
3	arm64-v8a/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86_64/libnative-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
5	x86_64/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	True info Symbols are stripped.
6	armeabi-v7a/libhello.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	armeabi-v7a/libnative-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
8	armeabi-v7a/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
9	armeabi/libhello.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	armeabi/liblocSDK5.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
11	x86/libnative-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
12	x86/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	arm64-v8a/libhello.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
14	arm64-v8a/libnative-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
15	arm64-v8a/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	x86_64/libnative-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
17	x86_64/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	True info Symbols are stripped.
18	armeabi-v7a/libhello.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	armeabi-v7a/libnative-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
20	armeabi-v7a/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
21	armeabi/libhello.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	armeabi/liblocSDK5.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
23	x86/libnative-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
24	x86/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00183	Get current camera parameters and change the setting.	camera	com/jaga/ibraceletplus/aigoband/camera/Preview.java com/king/zxing/CaptureHelper.java com/king/zxing/DecodeHandler.java com/king/zxing/camera/CameraConfigurationManager.java com/king/zxing/camera/CameraManager.java
00177	Check if permission is granted and request it	permission	com/jaga/ibraceletplus/aigoband/main/DupMainActivity.java com/jaga/ibraceletplus/aigoband/util/CheckUtil.java
00022	Open a file from given absolute path of the file	file	com/j256/ormlite/android/apptools/OrmLiteConfigUtil.java com/jaga/ibraceletplus/aigoband/camera/CameraActivity.java com/jaga/ibraceletplus/aigoband/camera/Preview.java com/jaga/ibraceletplus/aigoband/theme/dup/CustomWallpaperActivity.java com/jaga/ibraceletplus/aigoband/theme/dup/UserInfoActivity.java com/luck/lib/camerax/CustomCameraView.java com/luck/lib/camerax/utils/FileUtils.java com/luck/picture/lib/basic/PictureCommonFragment.java com/luck/picture/lib/entity/LocalMedia.java com/luck/picture/lib/loader/SandboxFileLoader.java com/luck/picture/lib/manager/PictureCacheManager.java com/luck/picture/lib/utils/DownloadFileUtils.java com/luck/picture/lib/utils/MediaStoreUtils.java com/luck/picture/lib/utils/MediaUtils.java com/luck/picture/lib/utils/PictureFileUtils.java com/yalantis/ucrop/UCropMultipleActivity.java top/zibin/luban/Luban.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/hjq/permissions/PermissionUtils.java com/jaga/ibraceletplus/aigoband/BaseActivity.java com/jaga/ibraceletplus/aigoband/camera/Preview.java com/jaga/ibraceletplus/aigoband/main/DupMainActivity.java com/jaga/ibraceletplus/aigoband/main/FragmentMain.java com/jaga/ibraceletplus/aigoband/theme/dup/UserInfoActivity.java com/luck/lib/camerax/CustomCameraView.java com/luck/picture/lib/basic/PictureCommonFragment.java com/luck/picture/lib/utils/IntentUtils.java com/yalantis/ucrop/UCropMultipleActivity.java no/nordicsemi/android/dfu/DfuBaseService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/hjq/permissions/PermissionUtils.java com/jaga/ibraceletplus/aigoband/main/DupMainActivity.java com/luck/lib/camerax/utils/FileUtils.java com/luck/picture/lib/utils/IntentUtils.java com/luck/picture/lib/utils/PictureFileUtils.java net/grandcentrix/tray/provider/TrayContract.java
00013	Read file and put it into a stream	file	c/e.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/hjq/permissions/PhoneRomUtils.java com/j256/ormlite/android/apptools/OrmLiteSqliteOpenHelper.java com/jaga/ibraceletplus/aigoband/ota/File.java com/jaga/ibraceletplus/aigoband/ota/OtaActivity.java com/jaga/ibraceletplus/aigoband/ota/OtaDialActivity.java com/jaga/ibraceletplus/aigoband/theme/dup/CustomWallpaperActivity.java com/jaga/ibraceletplus/aigoband/util/MD5Util.java com/jaga/ibraceletplus/aigoband/util/SysUtil.java com/loopj/android/http/JsonStreamerEntity.java com/loopj/android/http/SimpleMultipartEntity.java com/luck/lib/camerax/CustomCameraView.java com/luck/picture/lib/basic/PictureCommonFragment.java com/luck/picture/lib/utils/DownloadFileUtils.java com/luck/picture/lib/utils/MediaUtils.java com/luck/picture/lib/utils/PictureFileUtils.java com/luck/picture/lib/utils/SandboxTransformUtils.java com/sxr/sdk/ble/keepfit/service/OtaDial.java com/yalantis/ucrop/util/FileUtils.java cz/msebera/android/httpclient/conn/util/PublicSuffixMatcherLoader.java cz/msebera/android/httpclient/entity/FileEntity.java cz/msebera/android/httpclient/entity/mime/content/FileBody.java cz/msebera/android/httpclient/extras/PRNGFixes.java cz/msebera/android/httpclient/impl/client/cache/FileResource.java cz/msebera/android/httpclient/ssl/SSLContextBuilder.java d/g.java ezy/boost/update/UpdateUtil.java no/nordicsemi/android/dfu/DfuBaseService.java okio/Okio.java top/zibin/luban/io/ArrayPoolProvide.java
00162	Create InetSocketAddress object and connecting to it	socket	cz/msebera/android/httpclient/conn/MultihomePlainSocketFactory.java cz/msebera/android/httpclient/conn/scheme/PlainSocketFactory.java cz/msebera/android/httpclient/conn/socket/PlainConnectionSocketFactory.java cz/msebera/android/httpclient/conn/ssl/SSLConnectionSocketFactory.java cz/msebera/android/httpclient/conn/ssl/SSLSocketFactory.java cz/msebera/android/httpclient/impl/pool/BasicConnFactory.java

RULE ID	BEHAVIOUR	LABEL	FILES
00163	Create new Socket and connecting to it	socket	cz/msebera/android/httpclient/conn/MultihomePlainSocketFactory.java cz/msebera/android/httpclient/conn/scheme/PlainSocketFactory.java cz/msebera/android/httpclient/conn/socket/PlainConnectionSocketFactory.java cz/msebera/android/httpclient/conn/ssl/SSLConnectionSocketFactory.java cz/msebera/android/httpclient/conn/ssl/SSLSocketFactory.java cz/msebera/android/httpclient/impl/pool/BasicConnFactory.java
00003	Put the compressed bitmap data into JSON object	camera	com/jaga/ibraceletplus/aigoband/theme/dup/UserInfoActivity.java
00054	Install other APKs from file	reflection	com/jaga/ibraceletplus/aigoband/theme/dup/UserInfoActivity.java com/luck/picture/lib/utils/IntentUtils.java ezy/boost/update/UpdateUtil.java
00192	Get messages in the SMS inbox	sms	com/jaga/ibraceletplus/aigoband/BaseActivity.java com/jaga/ibraceletplus/aigoband/dslv/SimpleDragSortCursorAdapter.java com/jaga/ibraceletplus/aigoband/theme/dup/UserInfoActivity.java com/luck/picture/lib/loader/LocalMediaPageLoader.java com/luck/picture/lib/utils/PictureFileUtils.java com/yalantis/ucrop/util/FileUtils.java top/zibin/luban/LubanUtils.java
00005	Get absolute path of file and put it to JSON object	file	com/jaga/ibraceletplus/aigoband/theme/dup/UserInfoActivity.java com/luck/picture/lib/basic/PictureCommonFragment.java com/yalantis/ucrop/UCropMultipleActivity.java
00091	Retrieve data from broadcast	collection	com/jaga/ibraceletplus/aigoband/camera/CameraActivity.java com/jaga/ibraceletplus/aigoband/camera/Preview.java com/jaga/ibraceletplus/aigoband/service/SampleBleService.java com/jaga/ibraceletplus/aigoband/theme/dup/UserInfoActivity.java com/luck/lib/camerax/CustomCameraView.java com/yalantis/ucrop/UCropMultipleActivity.java
00009	Put data in cursor to JSON object	file	com/jaga/ibraceletplus/aigoband/theme/dup/UserInfoActivity.java
00121	Create a directory	file command	com/jaga/ibraceletplus/aigoband/camera/CameraActivity.java com/jaga/ibraceletplus/aigoband/ota/OtaActivity.java com/jaga/ibraceletplus/aigoband/ota/OtaDialActivity.java com/jaga/ibraceletplus/aigoband/theme/dup/CustomWallpaperActivity.java com/jaga/ibraceletplus/aigoband/theme/dup/UserInfoActivity.java com/yalantis/ucrop/UCropMultipleActivity.java top/zibin/luban/Luban.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/jaga/ibraceletplus/aigoband/BaseActivity.java com/jaga/ibraceletplus/aigoband/main/DupMainActivity.java com/jaga/ibraceletplus/aigoband/theme/dup/UserInfoActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00125	Check if the given file path exist	file	com/jaga/ibraceletplus/aigoband/camera/CameraActivity.java com/jaga/ibraceletplus/aigoband/main/FragmentSetting.java com/jaga/ibraceletplus/aigoband/ota/OtaActivity.java com/jaga/ibraceletplus/aigoband/ota/OtaDialActivity.java com/jaga/ibraceletplus/aigoband/ota/OtaWallpaperActivity.java com/jaga/ibraceletplus/aigoband/theme/dup/CustomWallpaperActivity.java com/jaga/ibraceletplus/aigoband/theme/dup/DialMarketActivity.java com/jaga/ibraceletplus/aigoband/theme/dup/UserInfoActivity.java com/luck/picture/lib/basic/PictureCommonFragment.java com/yalantis/ucrop/UCropMultipleActivity.java top/zibin/luban/Luban.java
00191	Get messages in the SMS inbox	sms	com/jaga/ibraceletplus/aigoband/theme/dup/UserInfoActivity.java com/luck/picture/lib/utils/MediaUtils.java
00104	Check if the given path is directory	file	com/jaga/ibraceletplus/aigoband/camera/CameraActivity.java top/zibin/luban/Luban.java
00112	Get the date of the calendar event	collection calendar	com/jaga/ibraceletplus/aigoband/util/DateUtil.java com/sxr/sdk/ble/keepfit/service/BluetoothLeService.java
00014	Read file into a stream and put it into a JSON object	file	com/jaga/ibraceletplus/aigoband/ota/OtaActivity.java com/jaga/ibraceletplus/aigoband/ota/OtaDialActivity.java com/loopj/android/http/JsonStreamerEntity.java com/luck/picture/lib/basic/PictureCommonFragment.java
00004	Get filename and put it to JSON object	file collection	com/jaga/ibraceletplus/aigoband/main/FragmentSetting.java com/jaga/ibraceletplus/aigoband/ota/OtaActivity.java com/jaga/ibraceletplus/aigoband/ota/OtaDialActivity.java com/jaga/ibraceletplus/aigoband/ota/OtaWallpaperActivity.java com/loopj/android/http/JsonStreamerEntity.java
00096	Connect to a URL and set request method	command network	ezy/boost/update/UpdateChecker.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java ezy/boost/update/UpdateChecker.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java ezy/boost/update/UpdateChecker.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java ezy/boost/update/UpdateChecker.java ezy/boost/update/UpdateDownloader.java
00204	Get the default ringtone	collection	com/jaga/ibraceletplus/aigoband/camera/Preview.java com/jaga/ibraceletplus/aigoband/util/SoundPlayUtil.java

RULE ID	BEHAVIOUR	LABEL	FILES
00056	Modify voice volume	control	com/jaga/ibraceletplus/aigoband/util/SoundPlayUtil.java
00080	Save recorded audio/video to a file	record file	com/jaga/ibraceletplus/aigoband/camera/Preview.java
00002	Open the camera and take picture	camera	com/jaga/ibraceletplus/aigoband/camera/Preview.java
00101	Initialize recorder	record	com/jaga/ibraceletplus/aigoband/camera/Preview.java
00195	Set the output path of the recorded file	record file	com/jaga/ibraceletplus/aigoband/camera/Preview.java
00199	Stop recording and release recording resources	record	com/jaga/ibraceletplus/aigoband/camera/Preview.java
00198	Initialize the recorder and start recording	record	com/jaga/ibraceletplus/aigoband/camera/Preview.java
00136	Stop recording	record command	com/jaga/ibraceletplus/aigoband/camera/Preview.java
00194	Set the audio source (MIC) and recorded file format	record	com/jaga/ibraceletplus/aigoband/camera/Preview.java
00090	Set recroded audio/video file format	record	com/jaga/ibraceletplus/aigoband/camera/Preview.java
00007	Use absolute path of directory for the output media file path	file	com/jaga/ibraceletplus/aigoband/camera/Preview.java
00006	Scheduling recording task	record	com/jaga/ibraceletplus/aigoband/camera/Preview.java
00138	Set the audio source (MIC)	record	com/jaga/ibraceletplus/aigoband/camera/Preview.java
00196	Set the recorded file format and output path	record file	com/jaga/ibraceletplus/aigoband/camera/Preview.java
00133	Start recording	record command	com/jaga/ibraceletplus/aigoband/camera/Preview.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/jaga/ibraceletplus/aigoband/camera/Preview.java
00041	Save recorded audio/video to file	record	com/jaga/ibraceletplus/aigoband/camera/Preview.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java
00012	Read data and put it into a buffer stream	file	com/luck/picture/lib/utils/PictureFileUtils.java com/yalantis/ucrop/util/FileUtils.java
00047	Query the local IP address	network collection	cz/msebera/android/httpclient/impl/SocketHttpClientConnection.java cz/msebera/android/httpclient/impl/SocketHttpServerConnection.java

RULE ID	BEHAVIOUR	LABEL	FILES
00065	Get the country code of the SIM card provider	collection	com/jaga/ibraceletplus/aigoband/util/SysUtil.java
00055	Query the SMS content and the source of the phone number	sms collection	com/jaga/ibraceletplus/aigoband/service/SampleBleService.java
00048	Query the SMS contents	sms collection	com/jaga/ibraceletplus/aigoband/service/SampleBleService.java
00049	Query the phone number from SMS sender	sms collection	com/jaga/ibraceletplus/aigoband/service/SampleBleService.java
00193	Send a SMS message	sms	com/jaga/ibraceletplus/aigoband/main/DupMainActivity.java
00018	Get JSON object prepared and fill in location info	location collection	com/jaga/ibraceletplus/aigoband/main/DupMainActivity.java
00137	Get last known location of the device	location collection	com/jaga/ibraceletplus/aigoband/main/DupMainActivity.java
00115	Get last known location of the device	collection location	com/jaga/ibraceletplus/aigoband/main/DupMainActivity.java
00031	Check the list of currently running applications	reflection collection	com/jaga/ibraceletplus/aigoband/main/DupMainActivity.java
00092	Send broadcast	command	com/jaga/ibraceletplus/aigoband/main/DupMainActivity.java
00113	Get location and put it into JSON	collection location	com/jaga/ibraceletplus/aigoband/main/DupMainActivity.java
00040	Send SMS	sms	com/jaga/ibraceletplus/aigoband/main/DupMainActivity.java
00016	Get location info of the device and put it to JSON object	location collection	com/jaga/ibraceletplus/aigoband/main/DupMainActivity.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	14/25	android.permission.VIBRATE, android.permission.READ_CALL_LOG, android.permission.READ_CONTACTS, android.permission.GET_ACCOUNTS, android.permission.READ_PHONE_STATE, android.permission.CAMERA, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.WAKE_LOCK, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	8/44	android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.CHANGE_NETWORK_STATE, android.permission.FOREGROUND_SERVICE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.FLASHLIGHT, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION
download.keeprapid.com	IP: 120.27.122.248 Country: China Region: Zhejiang City: Hangzhou
api.keeprapid.com	IP: 115.28.137.190 Country: China Region: Zhejiang City: Hangzhou
www.mob.com	IP: 180.188.26.28 Country: China Region: Zhejiang City: Taizhou
openapi.keeprapid.com	IP: 139.129.212.113 Country: China Region: Zhejiang City: Hangzhou

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
example.com	ok	**IP:** 23.220.75.245 **Country:** Colombia **Region:** Antioquia **City:** Medellin **Latitude:** 6.251840 **Longitude:** -75.563591 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
download.keeprapid.com	ok	**IP:** 120.27.122.248 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
twitter.com	ok	**IP:** 162.159.140.229 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
paolorotolo.github.io	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
api.openweathermap.org	ok	**IP:** 38.143.66.114 **Country:** United States of America **Region:** Utah **City:** Salt Lake City **Latitude:** 40.760780 **Longitude:** -111.891052 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
api.keeprapid.com	ok	**IP:** 115.28.137.190 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
line.me	ok	**IP:** 147.92.243.206 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
www.mob.com	ok	**IP:** 180.188.26.28 **Country:** China **Region:** Zhejiang **City:** Taizhou **Latitude:** 28.666668 **Longitude:** 121.349998 **View:** Google Map
openapi.keeprapid.com	ok	**IP:** 139.129.212.113 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
api.waqi.info	ok	**IP:** 139.162.71.178 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
github.com	ok	**IP:** 140.82.114.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70

HARDCODED SECRETS

POSSIBLE SECRETS
"ssdk_cmcc_login_one_key" : "□□□□□□□□□"
"ssdk_weibo_oauth_regiseter" : "Authorization"
"com_facebook_device_auth_instructions" : "□□<b>facebook.com/device</b>□□□□□□□□□□□□□"
"demo_user" : "Неизвестно"
"demo_user" : "Невідомий"
"wechat_auth" : "WeChat-godkendelse"
"demo_user" : "Unbekannt"
"app_getback_pwd_success" : "□□□□□□□"
"Ecg_Session_List_Count" : "Evidence"
"ssdk_instapaper_pwd" : "□□"
"Ecg_Session_List_Count" : "Podatki"
"Ecg_Session_List_Count" : "Записи"
"sport_hockey" : "□□"
"demo_user" : "Desconocido"
"demo_user" : "Άγνωστο"

POSSIBLE SECRETS
"Ecg_Session_List_Count" : "Zapisi"
"demo_user" : "Unknown"
"app_getback_pwd_success" : "■■■■■■■■■■■■■■■"
"demo_user" : "■■■■■■■"
"Ecg_Session_List_Count" : "Sessionslista"
"wechat_auth" : "WeChat-valtuutus"
"Sport_IceHockey" : "□□"
"com_facebook_device_auth_instructions" : "<b>facebook.com/device</b>□□□□□□□□□□□□□□□□□□□□□□□□"
"wechat_auth" : "□□□□"
"wechat_auth_retry" : "Переавторизуйте"
"demo_user" : "Bilinmeyen"
"Ecg_Session_List_Count" : "Records"
"sport_hockey" : "Jääkiekko"
"sport_hockey" : "hokej"
"demo_user" : "□□"
"sport_hockey" : "Hóquei"
"Ecg_Session_List_Count" : "Sessionsliste"
"sport_hockey" : "Hokej"
"demo_user" : "Sconosciuto"
"Ecg_Session_List_Count" : "□□□□□"
"sport_hockey" : "Jégkorong"

POSSIBLE SECRETS
"demo_user" : "□□□□"
"sport_hockey" : "Hockey"
"wechat_auth_fail" : "□□□□□□□□□□"
"Ecg_Session_List_Count" : "□□□"
"Ecg_Session_List_Count" : "■■■■■■■"
"sport_hockey" : "□□□□"
"demo_user" : "Desconhecido"
"wechat_auth" : "□□□□"
"Sport_FieldHockey" : "FieldHockey"
"demo_user" : "مجهول"
"sport_hockey" : "Hokey"
"demo_user" : "Tuntematon"
"Ecg_Session_List_Count" : "Øktliste"
"wechat_auth_retry" : "□□□□"
"sport_hockey" : "хокей"
"wechat_auth" : "Wechat-autorisasjon"
"demo_user" : "Okänd"
"ssdk_cmcc_auth" : "□□□□□□□□□□□□□"
"library_appintro_authorWebsite" : "http://paolorotolo.github.io/"
"Ecg_Session_List_Count" : "Aufzeichnungen"
"demo_user" : "□□"

POSSIBLE SECRETS
"wechat_auth" : "Wechat-auktorisering"
"Ecg_Session_List_Count" : "Dokumentacja"
"Ecg_Session_List_Count" : "□□"
"sport_hockey" : "Χακί"
"demo_user" : "Ukjent"
"Sport_FieldHockey" : "□□□"
"sport_hockey" : "Хокей"
"ssdk_weibo_oauth_regiseter" : "□□□□"
"wechat_auth_retry" : "Reauthorization"
"demo_user" : "Neznámé"
"wechat_auth_retry" : "Преупълномощаване"
"Sport_IceHockey" : "Хокей"
"demo_user" : "Nepoznato"
"ssdk_instapaper_pwd" : "Password"
"demo_user" : "Ukendt"
"demo_user" : "Nieznany"
"Sport_IceHockey" : "IceHockey"
"demo_user" : "Onbekend"
"sport_hockey" : "Хоккей"
"sport_hockey" : "■■■■■■"
"wechat_auth_retry" : "□□□□"

POSSIBLE SECRETS
"wechat_auth_fail" : "□□□□□□□□□□□□"
"Ecg_Session_List_Count" : "Istuntoluettelo"
"app_getback_pwd_success" : "□□□□□□□□□□□□□□□□"
"sport_hockey" : "□□□"
"demo_user" : "Inconnu"
"demo_user" : "Неизвестен"
"demo_user" : "Neznáme"
"wechat_auth_retry" : "Reautoriser"
"demo_user" : "Neznano"
"Ecg_Session_List_Count" : "□□□"
"sport_hockey" : "الهوكي"
"facebook_client_token" : "4243f419b385008eb84549d44719d75a"
"Ecg_Session_List_Count" : "Podaci"
"tray__authority" : "legacyTrayAuthority"
"wechat_auth_retry" : "□□□"
"sport_hockey" : "■■■■"
"app_getback_pwd_success" : "□□□□□□□"
"demo_user" : "Ismeretlen"
61C8849C-F639-4765-946E-5C3419BEBB2A
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
sha1/VRmyeKyygdftp6vBg5nDu2kEJLU=

POSSIBLE SECRETS
sha1/PANDaGiVHPNpKri0Jtq6j+ki5b0=
6c53db25-47a1-45fe-a022-7c92fb334fd4
sha1/u8I+KQuzKHcdrT6iTb30I70GsD0=
sha1/sYEIGhmkwJQf+uiVKMEkyZs0rMc=
8082caa8-41a6-4021-91c6-56f9b954cc34
sha1/aDMOYTWFIVkpg6PI0tLhQG56s8E=
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
sha1/7WYxNdMb1OymFMQp4xkGn5TBJlA=
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
B7DE1EEA-823D-43BB-A3AF-C4903DFCE23C
c56fb7d591ba6704df047fd98f535372fea00211
sha1/nKmNAK90Dd2BgNITRaWLjy6UONY=
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
357e248a6873302426f1ccdcf258e0c9
724249f0-5eC3-4b5f-8804-42345af08651
9b8f518b086098de3d77736f9458a3d2f6f95a37
308203523082023aa00302010202044fd0006b300d06092a864886f70d0101050500306b310b3009060355040613025553310b300906035504081302434131163014060355040713 0d53616e204672616e636973636f3110300e060355040a130754776974746572310f300d060355040b13064d6f62696c65311430120603550403130b4a6f6e617468616e204c65301e170d3132303630373031313431395a170d3339313032343031313431395a306b310b3009060355040613025553310b300906035504081302434131163014060355040713 0d53616e204672616e636973636f3110300e060355040a130754776974746572310f300d060355040b13064d6f62696c65311430120603550403130b4a6f6e617468616e204c6530820122300d06092a864886f70d01010105000382010f003082010a028201010089e6cbdfed4288a9c0a215d33d4fa978a5bdd20be426ef4b497d358a9fd1c6efec9684f059f6955e60e5fda1b5910bb2d097e7421a78f9c81e95cd8ef3bf50add7f8d9f073c0478736a6c7fd38c5871559783a76420d37f3f874f2114ec02532e85587791d24037485b1b95ec8cbc75b52042867988b51c7c3589d5b5972fd20a2e8a7c9ced986873f5008a418b2921daa7cfb78afc174eecdb8a79dc0961bea9740d09c4656ac9b8c86263a788e35af1d4a3f86ce053a1aefb5369def91614a390219f896f378712376baa05934a341798950e229f4f735b86004952b259f23cc9fc3b8c1bc8171984884dc92940e91f2e9a78a84a78f0c2946b7e37bbf3b9b0203010001300d06092a864886f70d01010505000382010100 1cf15250365e66cc87bb5054de1661266cf87907841016b20dfa1f9f59842020cbc33f9b4d41717db0428d11696a0bade6a4950a48cc4fa8ae56c850647379a5c2d977436b644162c453dd36b7745ccb9ff0b5fc070125024de73dab6dcda5c69372e978a49865f569927199ed0f61d7cbee1839079a7da2e83f8c90f7421a8c81b3f17f1cc05d52aedac9acd6e092ffd9ad572960e779a5b91a78e1aeb2b3c7b24464bd223c745e40abd74fc586310809520d183443fcca3c6ade3be458afedbd3325df9c0e552636e35bb55b240eb8c0ba3973c4fb81213f22363be2d70e85014650c2f4fc679747a7ec31ea7b08da7dd9b9ba279a7fbbc1bd440fbe831bf4
64B4E8B5-0DE5-401B-A21D-ACC8DB3B913A

POSSIBLE SECRETS
0b94731c9428eccb6a21ca9ab52a58bf6a3f8995
457871e8-d516-4ca1-9116-57d0b17b9cb2
9d84b9a3-000c-49d8-9183-855b673fda31
sha1/GiG0lStik84Ys2XsnA6TTLOB5tQ=
3082025d308201c6a00302010202044bd76cce300d06092a864886f70d01010505003073310b3009060355040613025553310b3009060355040813024341311630140603550407130d53616e204672616e636973636f31163014060355040a130d547769747465722c20496e632e310f300d060355040b13064d6f62696c65311630140603550403130d4c656c616e642052656368697330 1e170d3130303432373233303133345a170d3438303832353233303133345a307331 0b3009060355040613025553310b3009060355040813024341311630140603550407130d53616e204672616e636973636f31163014060355040a130d547769747465722c20496e632e310f300d060355040b13064d6f62696c65311630140603550403130d4c656c616e642052656368697330819f300d06092a864886f70d010101050003818d003081890281810086233c2e51c62232d49cc932e470713d63a6a1106b38f9e442e01bc79ca4f95c72b2cb3f1369ef7dea6036bff7c4b2828cb3787e7657ad83986751ced5b131fcc6f413efb7334e32ed9787f9e9a249ae108fa66009ac7a7932c25d37e1e07d4f9f66aa494c270dbac87d261c9668d321c2fba4ef2800e46671a597ff2eac5d7f0203010001300d06092a864886f70d0101050500038181003e1f01cb6ea8be8d2cecef5cd2a64c97ba8728aa5f08f8275d00508d64d139b6a72c5716b40a040df0eeeda04de9361107e123ee8d3dc05e70c8a355f46dbadf1235443b0b214c57211afd4edd147451c443d49498d2a7ff27e45a99c39b9e47429a1dae843ba233bf8ca81296dbe1dc5c5434514d995b0279246809392a219b
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
sha1/IvGeLsbqzPxdI0b0wuj2xVTdXgc=
sha1/wHqYaI2J+6sFZAwRfap9ZbjKzE4=
sha1/1S4TwavjSdrotJWU73w4Q2BkZr0=
cc2751449a350f668590264ed76692694a80308a
5f78df94-798c-46f5-990a-b3eb6a065c88
sha1/gzF+YoVCU9bXeDGQ7JGQVumRueM=
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
sha1/cTg28gIxU0crbrplRqkQFVggBQk=
sha1/I0PRSKJViZuUfUYaeX7ATP7RcLc=
42C3DFDD-77BE-4D9C-8454-8F875267FB3B

PLAYSTORE INFORMATION

Title: JYouPro - Fitness Tracker

Score: 3.5522387 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.jaga.ibraceletplus.aigoband

Developer Details: Keeprapid Dev, Keeprapid+Dev, None, None, thinksth@qq.com,

Release Date: Sep 5, 2018 **Privacy Policy:** Privacy link

Description:

Keeping up with your health has never been as easy as it is with JYouPro App. Note: JYouPro application is compatible with the following JYouPro Smartwatches: - ZW01 Smartwatch - T18 Smartwatch - ZW27T Smartwatch - T100 Smartwatch - T100A Smartwatch - L21 Smartwatch - S050 Smartwatch - T95 Smartwatch - G12Pro Smartwatch This application will help you: 1. Push call notification to smart watch, and let your know who is calling. 2. Push SMS notification to smart watch and you can read text and detail of SMS on your wearable device. 3. Display your heart rate, sleeping and workout history tracked from your smart watch. 4. Sedentary reminders to help you reach your fitness goals. 5. Weather check so you can plan your days and workouts accordingly. 6. Alarm 7. Drink water reminders 8. Multiple watch face options

SCAN LOGS

Timestamp	Event	Error
2025-08-30 22:17:38	Generating Hashes	OK
2025-08-30 22:17:38	Extracting APK	OK
2025-08-30 22:17:38	Unzipping	OK
2025-08-30 22:17:38	Parsing APK with androguard	OK
2025-08-30 22:17:39	Extracting APK features using aapt/aapt2	OK
2025-08-30 22:17:39	Getting Hardcoded Certificates/Keystores	OK
2025-08-30 22:17:42	Parsing AndroidManifest.xml	OK
2025-08-30 22:17:42	Extracting Manifest Data	OK
2025-08-30 22:17:42	Manifest Analysis Started	OK
2025-08-30 22:17:42	Performing Static Analysis on: JYouPro (com.jaga.ibraceletplus.aigoband)	OK

2025-08-30 22:17:42	Fetching Details from Play Store: com.jaga.ibraceletplus.aigoband	OK
2025-08-30 22:17:42	Checking for Malware Permissions	OK
2025-08-30 22:17:42	Fetching icon path	OK
2025-08-30 22:17:42	Library Binary Analysis Started	OK
2025-08-30 22:17:42	Analyzing lib/arm64-v8a/libhello.so	OK
2025-08-30 22:17:42	Analyzing lib/arm64-v8a/libnative-lib.so	OK
2025-08-30 22:17:42	Analyzing lib/arm64-v8a/libimage_processing_util_jni.so	OK
2025-08-30 22:17:42	Analyzing lib/x86_64/libnative-lib.so	OK
2025-08-30 22:17:42	Analyzing lib/x86_64/libimage_processing_util_jni.so	OK
2025-08-30 22:17:42	Analyzing lib/armeabi-v7a/libhello.so	OK
2025-08-30 22:17:42	Analyzing lib/armeabi-v7a/libnative-lib.so	OK
2025-08-30 22:17:42	Analyzing lib/armeabi-v7a/libimage_processing_util_jni.so	OK
2025-08-30 22:17:42	Analyzing lib/armeabi/libhello.so	OK
2025-08-30 22:17:42	Analyzing lib/armeabi/liblocSDK5.so	OK
2025-08-30 22:17:42	Analyzing lib/x86/libnative-lib.so	OK

2025-08-30 22:17:42	Analyzing lib/x86/libimage_processing_util_jni.so	OK
2025-08-30 22:17:42	Analyzing apktool_out/lib/arm64-v8a/libhello.so	OK
2025-08-30 22:17:42	Analyzing apktool_out/lib/arm64-v8a/libnative-lib.so	OK
2025-08-30 22:17:42	Analyzing apktool_out/lib/arm64-v8a/libimage_processing_util_jni.so	OK
2025-08-30 22:17:42	Analyzing apktool_out/lib/x86_64/libnative-lib.so	OK
2025-08-30 22:17:42	Analyzing apktool_out/lib/x86_64/libimage_processing_util_jni.so	OK
2025-08-30 22:17:42	Analyzing apktool_out/lib/armeabi-v7a/libhello.so	OK
2025-08-30 22:17:42	Analyzing apktool_out/lib/armeabi-v7a/libnative-lib.so	OK
2025-08-30 22:17:42	Analyzing apktool_out/lib/armeabi-v7a/libimage_processing_util_jni.so	OK
2025-08-30 22:17:42	Analyzing apktool_out/lib/armeabi/libhello.so	OK
2025-08-30 22:17:42	Analyzing apktool_out/lib/armeabi/liblocSDK5.so	OK
2025-08-30 22:17:42	Analyzing apktool_out/lib/x86/libnative-lib.so	OK
2025-08-30 22:17:42	Analyzing apktool_out/lib/x86/libimage_processing_util_jni.so	OK
2025-08-30 22:17:42	Reading Code Signing Certificate	OK

2025-08-30 22:17:43	Running APKiD 2.1.5	OK
2025-08-30 22:17:47	Detecting Trackers	OK
2025-08-30 22:17:49	Decompiling APK to Java with JADX	OK
2025-08-30 22:26:12	Decompiling with JADX failed, attempting on all DEX files	OK
2025-08-30 22:26:12	Decompiling classes2.dex with JADX	OK
2025-08-30 22:26:24	Decompiling classes.dex with JADX	OK
2025-08-30 22:26:35	Decompiling classes2.dex with JADX	OK
2025-08-30 22:26:47	Decompiling classes.dex with JADX	OK
2025-08-30 22:26:57	Converting DEX to Smali	OK
2025-08-30 22:26:57	Code Analysis Started on - java_source	OK
2025-08-30 22:26:58	Android SBOM Analysis Completed	OK
2025-08-30 22:27:05	Android SAST Completed	OK
2025-08-30 22:27:05	Android API Analysis Started	OK
2025-08-30 22:27:12	Android API Analysis Completed	OK
2025-08-30 22:27:12	Android Permission Mapping Started	OK

2025-08-30 22:27:20	Android Permission Mapping Completed	OK
2025-08-30 22:27:21	Android Behaviour Analysis Started	OK
2025-08-30 22:27:28	Android Behaviour Analysis Completed	OK
2025-08-30 22:27:28	Extracting Emails and URLs from Source Code	OK
2025-08-30 22:27:30	Email and URL Extraction Completed	OK
2025-08-30 22:27:30	Extracting String data from APK	OK
2025-08-30 22:27:31	Extracting String data from SO	OK
2025-08-30 22:27:31	Extracting String data from Code	OK
2025-08-30 22:27:31	Extracting String values and entropies from Code	OK
2025-08-30 22:27:33	Performing Malware check on extracted domains	OK
2025-08-30 22:27:36	Saving to Database	OK

Report Generated by - MobSF v4.4.0

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.