ANDROID STATIC ANALYSIS REPORT

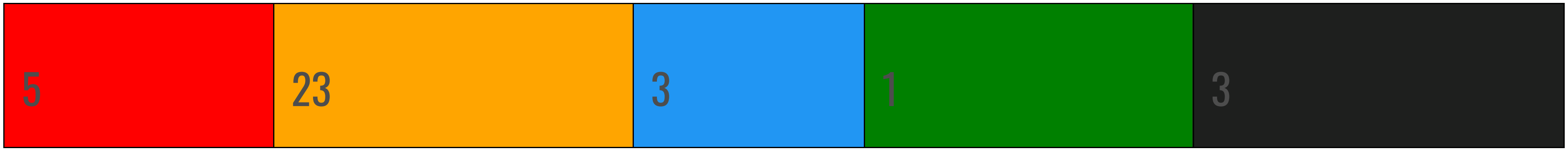
iHealth (4.10.0)

File Name:	com.ihealthlabs.MyVitalsPro_4100009.apk
Package Name:	com.ihealthlabs.MyVitalsPro

Scan Date:	Aug. 30, 2025, 10:06 p.m.
App Security Score:	43/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT



FILE INFORMATION

File Name: com.ihealthlabs.MyVitalsPro_4100009.apk
Size: 113.66MB
MD5: e235e29bcc9de21aaec336958a7bce51
SHA1: cf6442f6212b71d0e69579fdb2452cac910295a5
SHA256: 870a1516c7c807bbfb30fc81c793d840d2effff2e68f980d2950854966c7c8ff

APP INFORMATION

App Name: iHealth
Package Name: com.ihealthlabs.MyVitalsPro
Main Activity: com.ihealth.business.common.welcome.WelcomeActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 4.10.0
Android Version Code: 4100009

APP COMPONENTS

Activities: 227
Services: 15
Receivers: 8
Providers: 8
Exported Activities: 3
Exported Services: 5
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-09-16 09:51:21+00:00
Valid To: 2050-09-16 09:51:21+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x3078995368ba4ebefdfba8d09e49485337d16dc8
Hash Algorithm: sha256
md5: 47ca7812966ff90be500eadf7207039b
sha1: e25f0fe7d3c6125d860c285053c14f6dc45c66af
sha256: e42d0dfeca87b09f8f794e6c25d55ffba156cbaafde504ae5feddd7cb28149c9
sha512: 92a6f6c3579a530de26050b3dd2af681b3b1c1a3117fb3bda2ddc481b32431c34f48fd5b080c6ce1c9bce5e0f0be4f607f5c320128c8db836843b4d9047c27de
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 8ff874e3f06ed14e7630c196eb48ef8826e29cd4fbe2fea950924b0adc58c87d
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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.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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.CHANGE_WIFI_MULTICAST_STATE	normal	allow Wi-Fi Multicast reception	Allows an application to receive packets not directly addressed to your device. This can be useful when discovering services offered nearby. It uses more power than the non-multicast mode.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.READ_LOGS	dangerous	read sensitive log data	Allows an application to read from the system's various log files. This allows it to discover general information about what you are doing with the phone, potentially including personal or private information.
android.permission.PERMISSION_GRANTED	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.FOREGROUND_SERVICE_REMOTE_MESSAGING	normal	allows foreground services for remote messaging.	Allows a regular application to use Service.startForeground with the type "remoteMessaging".
android.permission.FOREGROUND_SERVICE_PHONE_CALL	normal	enables foreground services during phone calls.	Allows a regular application to use Service.startForeground with the type "phoneCall".
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.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
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.ANSWER_PHONE_CALLS	dangerous	permits an app to answer incoming phone calls.	Allows the app to answer an incoming phone call.

PERMISSION	STATUS	INFO	DESCRIPTION
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.health.READ_ACTIVE_CALORIES_BURNED	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_ACTIVE_CALORIES_BURNED	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_BASAL_METABOLIC_RATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_BASAL_METABOLIC_RATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_BLOOD_GLUCOSE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_BLOOD_GLUCOSE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_BLOOD_PRESSURE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_BLOOD_PRESSURE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_BODY_FAT	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_BODY_FAT	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_BODY_TEMPERATURE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_BODY_TEMPERATURE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_BODY_WATER_MASS	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_BODY_WATER_MASS	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_BONE_MASS	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_BONE_MASS	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.health.READ_DISTANCE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_DISTANCE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_HEART_RATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_HEART_RATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_HEIGHT	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_HEIGHT	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_LEAN_BODY_MASS	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_LEAN_BODY_MASS	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_OXYGEN_SATURATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_OXYGEN_SATURATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_SLEEP	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_SLEEP	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_STEPS	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_STEPS	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.READ_WEIGHT	unknown	Unknown permission	Unknown permission from android reference
android.permission.health.WRITE_WEIGHT	unknown	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH_ADVERTISE	dangerous	required to advertise to nearby Bluetooth devices.	Required to be able to advertise to 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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.ihealthlabs.MyVitalsPro.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>e235e29bcc9de21aaec336958a7bce51.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes4.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>possible Build.SERIAL check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table></td></tr>
<tr><td>classes5.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.BOARD check
SIM operator check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table></td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.ihealth.business.common.welcome.WelcomeActivity	Schemes: myvitalspro://, Hosts: ihealthlabs.com, Path Prefixes: /v4,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.

CERTIFICATE ANALYSIS

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

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **13** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. 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	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Service (com.ihealth.service.MyAWSMessagingService) is not Protected. [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.
5	Activity (com.ihealth.business.common.trampoline.TrampolineActivity) 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.
6	Broadcast Receiver (com.ihealth.broadcastReceiver.LanguageReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver 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.jiuan.project.rulai.business.service.Am6Service) is not Protected. [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.
8	Service (com.jiuan.project.rulai.business.service.NotificationService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NOTIFICATION_LISTENER_SERVICE [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.
9	Activity (com.neutral.kit.model.healthconnect.HealthConnectPrivacyPolicy) 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.
10	Activity-Alias (com.neutral.kit.ViewPermissionUsageActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.START_VIEW_PERMISSION_USAGE [android:exported=true]	warning	An Activity-Alias 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.

NO	ISSUE	SEVERITY	DESCRIPTION
11	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.
12	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver 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.
13	Service (androidx.health.platform.client.impl.sdkservice.HealthDataSdkService) is not Protected. [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.
14	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver 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.
15	High Intent Priority (1000) - {2} Hit(s) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

CODE ANALYSIS

HIGH: **3** | WARNING: **7** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				butterknife/ButterKnife.java com/alibaba/android/arouter/utils/DefaultLogger.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/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java 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/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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				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/gif/GifDrawableEncoder.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/module/ManifestParser.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/contrarywind/view/WheelView.java com/example/smartlinklib/MainActivity.java com/example/smartlinklib/SmartLinkManipulator.java com/ido/ble/bluetooth/b/a.java com/ido/ble/business/sync/k.java com/ido/ble/business/sync/l.java com/ido/ble/common/c.java com/ido/ble/common/l.java com/ido/ble/common/m.java com/ido/ble/dfu/b/l.java com/ido/ble/dfu/c/a.java com/ido/ble/dfu/c/b.java com/ido/ble/dfu/c/c.java com/ido/ble/dfu/c/d.java com/ido/ble/dfu/m.java com/ido/ble/logs/LogTool.java com/ihealth/analysis/manager/YDAnalysisManager.java com/ihealth/analysis/manager/YDAnalyticsDeviceManager.java com/ihealth/communication/base/a/a.java com/ihealth/communication/base/audio/AudioTrack

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	Manager.java com/ihealth/communication/base/audio/TunnerThread.java com/ihealth/communication/base/ble/BleUnPackageData.java com/ihealth/communication/base/ble/BleUnPackageData2.java com/ihealth/communication/base/ble/ScanRecord.java com/ihealth/communication/base/bt/BtCommThread.java com/ihealth/communication/base/bt/BtCommThreadEE.java com/ihealth/communication/base/bt/BtUnpackageData.java com/ihealth/communication/base/ecg/ECGOnline.java com/ihealth/communication/base/protocol/BtCommProtocol.java com/ihealth/communication/base/protocol/ECGUSBCommProtocol.java com/ihealth/communication/base/protocol/Hs3CommProtocol.java com/ihealth/communication/base/protocol/WifiCommProtocol.java com/ihealth/communication/base/statistical/litepal/util/LogUtil.java com/ihealth/communication/base/usb/Ecg3Usb.java com/ihealth/communication/base/usb/UsbUnpackageData.java com/ihealth/communication/base/wifi/WifiUnpackageData.java com/ihealth/communication/cloud/a/a.java com/ihealth/communication/cloud/a/c.java com/ihealth/communication/cloud/a/e.java com/ihealth/communication/cloud/data/AM_CommCloud.java com/ihealth/communication/control/BPControl.java com/ihealth/communication/control/Hs5ControlForBt.java com/ihealth/communication/ins/A1InSet_KD723.java com/ihealth/communication/ins/Bg1aInsSet.java com/ihealth/communication/ins/BgInsSet.java com/ihealth/communication/ins/Bpm1InsSet.java com/ihealth/communication/ins/Hs5InsSet.java com/ihealth/communication/ins/InsCallback.java com/ihealth/communication/manager/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/ihealth/communication/manager/e.java com/ihealth/communication/manager/f.java com/ihealth/communication/manager/i.java com/ihealth/communication/privatecontrol/AbiControlSubManager.java com/ihealth/communication/utils/AppUtils.java com/ihealth/communication/utils/ByteBufferUtil.java com/ihealth/communication/utils/DataThreadPoolManager.java com/ihealth/communication/utils/FileUtils.java com/ihealth/communication/utils/Logger.java com/ihealth/communication/utils/WifiAdmin.java com/ihealth/sdk/ble/BleManager.java com/ihealth/sdk/ble/BleScanner.java com/ihealth/sdk/command/AuthCommand.java com/ihealth/sdk/command/base/flow/ProtocolParser.java com/ihealth/sdk/command/base/flow/ProtocolWrapper.java com/ihealth/util/PublicMethod.java com/ihealth/util/TimeUtils.java com/ihealth/zxing/camera/CameraConfigurationUtils.java com/jakewharton/disklrucache/DiskLruCache.java com/jiuan/project/bailongma/base/b.java com/jiuan/project/bailongma/base/d.java com/jiuan/project/honghaierkit/base/a.java com/jiuan/project/honghaierkit/base/b.java com/just/agentweb/AgentWebUtils.java com/just/agentweb/AgentWebView.java com/just/agentweb/JsCallJava.java com/just/agentweb/JsCallback.java com/just/agentweb/LogUtils.java com/king/zxing/util/LogUtils.java com/lcodecore/tkrefreshlayout/TwinklingRefreshLayout.java com/neutral/kit/utils/AndonDateUtil.java com/neutral/kit/utils/AndonLogUtils.java com/samsung/android/sdk/healthdata/HealthDataStore.java com/samsung/android/sdk/internal/database/BulkCursorToCursorAdaptor.java com/samsung/android/sdk/internal/healthdata/HealthResultHolderImpl.java com/tencent/mars/BaseEvent.java com/tencent/mars/Mars.java com/tencent/mars/comm/Alarm.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/tencent/mars/comm/NetStatusUtil.java com/tencent/mars/sample/wrapper/remote/MarsServiceProxy.java com/tencent/mars/sample/wrapper/remote/NanoMarsTaskWrapper.java com/tencent/mars/sample/wrapper/service/MarsServiceStub.java com/tencent/mars/xlog/Log.java common/log/SimpleLogger.java dagger/android/AndroidInjection.java jxl/demo/WriteAccess.java org/greenrobot/eventbus/Logger.java org/greenrobot/greendao/AbstractDao.java org/greenrobot/greendao/DaoException.java org/greenrobot/greendao/DaoLog.java org/greenrobot/greendao/DbUtils.java org/greenrobot/greendao/internal/LongHashMap.java org/greenrobot/greendao/test/AbstractDaoTestSinglePk.java org/greenrobot/greendao/test/DbTest.java zendesk/belvedere/BelvedereFileProvider.java zendesk/belvedere/L.java zendesk/belvedere/Storage.java
2	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/jiuan/notification/ui/TB_InAppMessageTransparentActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/alibaba/fastjson/support/geo/Geometry.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/manager/RequestManagerRetriever.java com/example/smartlinklib/SmartLinkManipulator.java com/ihealth/communication/base/statistical/litepal/util/cipher/CipherUtil.java com/ihealth/constants/ConstantsAnalytics.java com/ihealth/constants/ConstantsCommon.java com/ihealth/constants/ConstantsSP.java com/ihealth/network/address/InterfaceAddress.java com/neutral/kit/network/builder/PostFormBuilder.java zendesk/core/Constants.java zendesk/core/ZendeskCoreSettingsStorage.java zendesk/core/ZendeskIdentityStorage.java zendesk/core/ZendeskStorage.java zendesk/support/CreateRequest.java zendesk/support/ZendeskArticleVoteStorage.java zendesk/support/ZendeskRequestStorage.java
4	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/ihealth/analysis/tools/YDMD5Tools.java com/ihealth/communication/base/statistical/litepal/util/cipher/CipherUtil.java com/ihealth/communication/cloud/CommCloudCenter.java com/ihealth/communication/cloud/CommCloudSDK.java com/ihealth/communication/manager/g.java com/ihealth/communication/utils/AppUtils.java com/ihealth/communication/utils/MD5.java com/ihealth/util/EncryptUtils.java com/just/agentweb/AgentWebUtils.java com/neutral/kit/utils/AndonMD5Util.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/ido/ble/common/e.java com/ido/ble/logs/LogTool.java com/ihealth/communication/utils/FileUtils.java com/just/agentweb/AgentWebUtils.java com/neutral/kit/config/Config.java com/neutral/kit/network/AppCenter.java com/neutral/kit/network/Center.java com/neutral/kit/network/ServiceCenter.java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/example/smartlinklib/SmartLinkManipulator.java com/ihealth/communication/base/statistical/model/StatisticalModel.java com/ihealth/communication/cloud/CommCloudCenter.java com/ihealth/communication/cloud/CommCloudSDK.java com/ihealth/communication/cloud/CommCloudSyncTime.java com/ihealth/communication/cloud/data/AM_CommCloud.java com/ihealth/communication/ins/Bpm1InsSet.java com/ihealth/communication/manager/i.java
7	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	com/bumptech/glide/integration/okhttp/BuildConfig.java
8	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/ihealth/communication/cloud/a/c.java
9	This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files.	info	OWASP MASVS: MSTG-CRYPTO-1	org/greenrobot/greendao/database/DatabaseOpenHelper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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/ihealth/communication/base/statistical/litepal/crud/DataSupport.java com/ihealth/communication/base/statistical/litepal/util/DBUtility.java org/greenrobot/greendao/AbstractDao.java org/greenrobot/greendao/DbUtils.java org/greenrobot/greendao/database/StandardDatabase.java
11	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/alibaba/fastjson/util/AntiCollisionHashMap.java com/ihealth/sdk/command/AuthCommand.java com/ihealth/view/bp/BPMeasureView.java org/greenrobot/greendao/test/DbTest.java
12	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/just/agentweb/AgentWebConfig.java
13	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/ihealth/network/eucloud/ssl/TLSSocketFactory.java zendesk/support/SupportSdkModule.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/libiHealth.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
2	arm64-v8a/libVeryFitMulti.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
3	arm64-v8a/libindoor.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
4	arm64-v8a/libECGOffline.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
5	arm64-v8a/libc++_shared.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
6	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
7	arm64-v8a/libECGOnline.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
8	arm64-v8a/libmarsstn.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
9	arm64-v8a/libBodyfat_SDK.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
10	arm64-v8a/liblocSDK7d.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
11	arm64-v8a/libmarsxlog.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
12	x86_64/libiHealth.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	x86_64/libVeryFitMulti.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
14	x86_64/libindoor.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
15	x86_64/libECGOffline.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
16	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.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	x86_64/libECGOnline.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
18	x86_64/libBodyfat_SDK.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	x86_64/liblocSDK7d.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
20	armeabi-v7a/libiHealth.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
21	armeabi-v7a/libVeryFitMulti.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
22	armeabi-v7a/libindoor.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
23	armeabi-v7a/libECGOffline.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
24	armeabi-v7a/libc++_shared.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
25	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.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	armeabi-v7a/libECGOnline.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
27	armeabi-v7a/libmarsstn.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
28	armeabi-v7a/libBodyfat_SDK.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
29	armeabi-v7a/liblocSDK7d.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
30	armeabi-v7a/libmarsxlog.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
31	x86/libiHealth.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
32	x86/libVeryFitMulti.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
33	x86/libindoor.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
34	x86/libECGOffline.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
35	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
36	x86/libECGOnline.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
37	x86/libBodyfat_SDK.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
38	x86/liblocSDK7d.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
39	arm64-v8a/libiHealth.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
40	arm64-v8a/libVeryFitMulti.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
41	arm64-v8a/libindoor.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
42	arm64-v8a/libECGOffline.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
43	arm64-v8a/libc++_shared.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
44	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
45	arm64-v8a/libECGOnline.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
46	arm64-v8a/libmarsstn.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
47	arm64-v8a/libBodyfat_SDK.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
48	arm64-v8a/liblocSDK7d.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
49	arm64-v8a/libmarsxlog.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
50	x86_64/libiHealth.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
51	x86_64/libVeryFitMulti.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
52	x86_64/libindoor.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
53	x86_64/libECGOffline.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
54	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.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
55	x86_64/libECGOnline.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
56	x86_64/libBodyfat_SDK.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
57	x86_64/liblocSDK7d.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
58	armeabi-v7a/libiHealth.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
59	armeabi-v7a/libVeryFitMulti.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
60	armeabi-v7a/libindoor.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
61	armeabi-v7a/libECGOffline.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
62	armeabi-v7a/libc++_shared.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
63	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.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
64	armeabi-v7a/libECGOnline.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
65	armeabi-v7a/libmarsstn.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
66	armeabi-v7a/libBodyfat_SDK.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
67	armeabi-v7a/liblocSDK7d.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
68	armeabi-v7a/libmarsxlog.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
69	x86/libiHealth.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
70	x86/libVeryFitMulti.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
71	x86/libindoor.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
72	x86/libECGOffline.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
73	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
74	x86/libECGOnline.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
75	x86/libBodyfat_SDK.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
76	x86/liblocSDK7d.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
00147	Get the time of current location	collection location	com/ihealth/util/PublicMethod.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/ihealth/util/PublicMethod.java com/just/agentweb/AgentWebUtils.java zendesk/messaging/ui/UtilsAttachment.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/ihealth/util/PublicMethod.java com/just/agentweb/AgentWebUtils.java zendesk/messaging/ui/UtilsAttachment.java
00013	Read file and put it into a stream	file	com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/ihealth/communication/cloud/a/c.java com/ihealth/communication/utils/FileUtils.java com/ihealth/network/eucloud/ssl/TLSSocketFactory.java com/ihealth/util/ImageUtils.java com/jakewharton/disklrucache/DiskLruCache.java com/jakewharton/disklrucache/StrictLineReader.java com/neutral/kit/utils/AndonZipUtils.java jxl/Workbook.java jxl/biff/drawing/PNGReader.java jxl/demo/BiffDump.java jxl/demo/PropertySetsReader.java jxl/demo/WriteAccess.java
00094	Connect to a URL and read data from it	command network	com/ihealth/communication/cloud/a/e.java com/ihealth/communication/cloud/a/g.java
00183	Get current camera parameters and change the setting.	camera	com/ihealth/zxing/camera/CameraConfigurationManager.java com/ihealth/zxing/camera/CameraManager.java
00130	Get the current WIFI information	wifi collection	com/ihealth/communication/base/protocol/WifiCommProtocol.java com/ihealth/communication/utils/WifiAdmin.java com/tencent/mars/BaseEvent.java com/tencent/mars/comm/NetStatusUtil.java com/tencent/mars/comm/NetworkSignalUtil.java com/tencent/mars/comm/PlatformComm.java
00076	Get the current WiFi information and put it into JSON	collection wifi	com/ihealth/communication/base/protocol/WifiCommProtocol.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/ido/ble/common/e.java com/ido/ble/firmware/log/i.java com/ihealth/communication/utils/FileUtils.java com/ihealth/communication/utils/Logger.java com/ihealth/util/ImageUtils.java com/ihealth/util/share/ShareMethodUtils.java com/just/agentweb/AgentWebConfig.java com/just/agentweb/AgentWebUtils.java com/neutral/kit/config/Config.java com/neutral/kit/utils/AndonLogUtils.java y/a.java zendesk/belvedere/Belvedere.java zendesk/belvedere/Storage.java
00024	Write file after Base64 decoding	reflection file	com/ihealth/communication/utils/FileUtils.java
00192	Get messages in the SMS inbox	sms	com/just/agentweb/AgentWebUtils.java
00191	Get messages in the SMS inbox	sms	com/just/agentweb/AgentWebUtils.java
00036	Get resource file from res/raw directory	reflection	com/just/agentweb/AgentWebUtils.java
00096	Connect to a URL and set request method	command network	a/a/a/a/a/e/g.java com/ihealth/communication/cloud/a/e.java com/ihealth/communication/cloud/a/f.java
00089	Connect to a URL and receive input stream from the server	command network	a/a/a/a/a/e/g.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/ihealth/communication/cloud/a/e.java com/ihealth/communication/cloud/a/f.java
00109	Connect to a URL and get the response code	network command	a/a/a/a/a/e/g.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/ihealth/communication/cloud/a/f.java
00014	Read file into a stream and put it into a JSON object	file	com/ihealth/communication/cloud/a/c.java
00125	Check if the given file path exist	file	com/tencent/mars/sample/wrapper/service/MarsServiceStub.java

RULE ID	BEHAVIOUR	LABEL	FILES
00058	Connect to the specific WIFI network	wifi control	com/ihealth/communication/utils/WifiAdmin.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/ihealth/communication/utils/WifiAdmin.java
00139	Get the current WiFi id	collection wifi	com/ihealth/communication/utils/WifiAdmin.java com/tencent/mars/BaseEvent.java
00134	Get the current WiFi IP address	wifi collection	com/ihealth/communication/utils/WifiAdmin.java
00082	Get the current WiFi MAC address	collection wifi	com/ihealth/communication/utils/WifiAdmin.java
00072	Write HTTP input stream into a file	command network file	com/ihealth/communication/cloud/a/e.java
00108	Read the input stream from given URL	network command	com/ihealth/communication/cloud/a/e.java
00034	Query the current data network type	collection network	com/tencent/mars/comm/PlatformComm.java
00012	Read data and put it into a buffer stream	file	com/neutral/kit/utils/AndonZipUtils.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/ihealth/communication/cloud/a/f.java
00043	Calculate WiFi signal strength	collection wifi	com/tencent/mars/comm/NetworkSignalUtil.java
00189	Get the content of a SMS message	sms	zendesk/belvedere/Storage.java
00188	Get the address of a SMS message	sms	zendesk/belvedere/Storage.java
00200	Query data from the contact list	collection contact	zendesk/belvedere/Storage.java
00201	Query data from the call log	collection calllog	zendesk/belvedere/Storage.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	zendesk/belvedere/Storage.java
00035	Query the list of the installed packages	reflection	com/tencent/mars/comm/NetStatusUtil.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://ihealth-myvitals-pro.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/46426147602/namespaces/firebase:fetch?key=AIzaSyDeQtrrM2pWKUnmE7E2_qAtnTOTGO8akkY is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'bp_average_beta': '{"average_beta":false,"page_type":"","target_page":""}', 'mv_settings_remote_config': '[{ "name": "Ask & Support AI", "icon": "https://zhuchuankai.s3.us-west-2.amazonaws.com/mv_icon_ai_chat_bot.png", "smallIcon": "https://zhuchuankai.s3.us-west-2.amazonaws.com/mv_icon_beta.png", "url": "https://customer-service-bot.ihealthlabs.com/business/index.html#/CustimerServicePage", "subTitle": "24/7 service, Reply within 1 minute", "isSmall": true, "supportEU": false, "settingType": 1000 }]'}, 'state': 'UPDATE', 'experimentDescriptions': [{'experimentId': '_exp_rollout_5', 'variantId': '1', 'experimentStartTime': '2025-04-15T06:25:05.429279Z', 'triggerTimeoutMillis': '15552000000', 'timeToLiveMillis': '15552000000'}], 'templateVersion': '12', 'rolloutMetadata': [{'rolloutId': 'rollout_5', 'variantId': '1', 'affectedParameterKeys': ['mv_settings_remote_config']}]}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	15/25	android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.INTERNET, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.CAMERA, android.permission.VIBRATE, android.permission.RECORD_AUDIO, android.permission.READ_PHONE_STATE, android.permission.RECEIVE_SMS, android.permission.READ_CALL_LOG, android.permission.READ_CONTACTS, android.permission.WAKE_LOCK, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE
Other Common Permissions	11/44	android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.CHANGE_NETWORK_STATE, android.permission.CHANGE_WIFI_STATE, android.permission.ACTIVITY_RECOGNITION, android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, android.permission.FLASHLIGHT, com.google.android.c2dm.permission.RECEIVE, 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
www.qq.com	IP: 43.159.109.55 Country: China Region: Beijing City: Beijing

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.ihealthlabs.eu	ok	**IP:** 87.98.144.147 **Country:** France **Region:** Hauts-de-France **City:** Roubaix **Latitude:** 50.694210 **Longitude:** 3.174560 **View:** Google Map
test-proapi.ihealthlabs.com	ok	**IP:** 54.215.130.168 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.ihealthlabs.com	ok	**IP:** 50.18.151.109 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
www.zendesk.com	ok	**IP:** 104.18.34.51 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.qq.com	ok	**IP:** 43.159.109.55 **Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map
ihealth-myvitals-pro.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
test-proapi-am6.ihealthlabs.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.112.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
myvitals.ihealthlabs.com	ok	**IP:** 13.56.190.139 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
proapi-notification.ihealthlabs.com	ok	**IP:** 54.183.61.74 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
proapi.ihealthlabs.com	ok	**IP:** 52.53.54.50 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
www.google.com	ok	**IP:** 172.217.20.164 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.apple.com	ok	**IP:** 23.32.229.38 **Country:** United States of America **Region:** Georgia **City:** Atlanta **Latitude:** 33.749001 **Longitude:** -84.387978 **View:** Google Map
requestcert.ihealthlabs.eu	ok	**IP:** 185.49.208.9 **Country:** France **Region:** Bourgogne-Franche-Comte **City:** Montceau-les-Mines **Latitude:** 46.666672 **Longitude:** 4.366670 **View:** Google Map
ihealthlabs.eu	ok	**IP:** 87.98.144.147 **Country:** France **Region:** Hauts-de-France **City:** Roubaix **Latitude:** 50.694210 **Longitude:** 3.174560 **View:** Google Map
test.ihealthlabs.com	ok	**IP:** 13.57.143.79 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
test-notifications.ihealthlabs.com	ok	**IP:** 54.215.130.168 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cert.idshost.fr	ok	**IP:** 185.49.208.111 **Country:** France **Region:** Bourgogne-Franche-Comte **City:** Montceau-les-Mines **Latitude:** 46.666672 **Longitude:** 4.366670 **View:** Google Map
proapi.ihealthlabs.eu	ok	**IP:** 185.49.208.3 **Country:** France **Region:** Bourgogne-Franche-Comte **City:** Montceau-les-Mines **Latitude:** 46.666672 **Longitude:** 4.366670 **View:** Google Map
cloud.ihealthlabs.com	ok	**IP:** 54.67.125.148 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
test-api.ihealthlabs.com	ok	**IP:** 52.53.185.209 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
www.cnil.fr	ok	**IP:** 172.66.152.244 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
proapi-am6.ihealthlabs.com	ok	**IP:** 54.241.106.38 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
dashboard.ihealthlabs.com	ok	**IP:** 18.155.173.93 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
cdn.ihealthlabs.com	ok	**IP:** 18.155.173.113 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api.ihealthlabs.eu	ok	**IP:** 185.49.208.9 **Country:** France **Region:** Bourgogne-Franche-Comte **City:** Montceau-les-Mines **Latitude:** 46.666672 **Longitude:** 4.366670 **View:** Google Map
www.ihealthlabs.com	ok	**IP:** 23.227.38.74 **Country:** Canada **Region:** Ontario **City:** Ottawa **Latitude:** 45.418877 **Longitude:** -75.696510 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
tools.android.com	ok	**IP:** 142.250.179.115 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
esante.gouv.fr	ok	**IP:** 37.59.26.43 **Country:** France **Region:** Hauts-de-France **City:** Roubaix **Latitude:** 50.694210 **Longitude:** 3.174560 **View:** Google Map
apipublic.ihealthlabs.eu	ok	**IP:** 185.49.208.8 **Country:** France **Region:** Bourgogne-Franche-Comte **City:** Montceau-les-Mines **Latitude:** 46.666672 **Longitude:** 4.366670 **View:** Google Map
ihealthlabs.com	ok	**IP:** 23.227.38.65 **Country:** Canada **Region:** Ontario **City:** Ottawa **Latitude:** 45.418877 **Longitude:** -75.696510 **View:** Google Map

✉ EMAILS

EMAIL	FILE
support@ihealthlabs.com □□ihealth□□□□support@ihealthlabs.eu □□□□□□□□support@ihealthlabs.com□□□1 support@ihealthlabs.eu □□□□□□□□support@ihealthlabs.com□□□1 □□ihealth□□□□support@ihealthlabs.eu	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyDeQtrrM2pWKUnmE7E2_qAtnTOTGO8akkY"
"setting_user_name" : "□□"
"googlefit_authorize_btn" : "Autoriser"
"device_hs2s_reset_user" : "□□□□"
"setting_user_name" : "Name"
"app_selectUser" : "□□□□"

POSSIBLE SECRETS
"setting_user_name" : "Nome"
"googlefit_authorize_btn" : "Autorisieren"
"app_user_password" : "□□"
"deviceDetails_hs6_passWord" : "□□:"
"app_user_password" : "Kennwort"
"deviceDetails_hs6_passWord" : "Password"
"guide_hs6_wifi_pwd_limit" : "Wi-Fi□□□□□□32□"
"firebase_database_url" : "https://ihealth-myvitals-pro.firebaseio.com"
"deviceDetails_hs6_passWord" : "Clave"
"setting_authorize_des_epic" : "Epic"
"googlefit_authorize_btn" : "Autorizza"
"userRegister_enter_email_and_password" : "□□□□□□□"
"setting_authorize_des_fitbit" : "Fitbit"
"app_user_password" : "Palavra-passe"
"userRegister_enter_email_and_password" : "□□□□□□□"
"deviceDetails_hs6_passWord" : "Palavra-passe"
"app_checkPassword" : "□□□□□□6-128□□□□□□"
"com.google.firebase.crashlytics.mapping_file_id" : "6c8427b56cc249dfb4b017c207588fc8"

POSSIBLE SECRETS
"setting_user_name" : "Nom"
"guide_bpm1_setUser" : "□□□□"
"setting_user_name" : "□□"
"google_api_key" : "AIzaSyDeQtrrM2pWKUnmE7E2_qAtnTOTGO8akkY"
"deviceDetails_hs6_passWord" : "Kennwort"
"setting_user_name" : "Nombre"
"app_user_password" : "□□"
"app_user_password" : "Password"
"guide_hs6_wifi_pwd_limit" : "Wifi□□□□□□32□"
"app_user_password" : "Clave"
"guide_bpm1_setUser" : "□□□□"
"deviceDetails_hs6_passWord" : "□□:"
"device_hs2s_reset_user" : "□□□□"
"rl_settings_author_fitbit" : "Fitbit"
"app_selectUser" : "□□□□"
"deviceDetails_hs6_passWord" : "Password:"
"googlefit_authorize_btn" : "Authorize"
"googlefit_authorize_btn" : "Autorizar"

POSSIBLE SECRETS
"app_checkPassword" : "□□□□□□6-128□□□□□□"
2fb61340b51445daa7670d781b0a7cc5
7265632e-6a69-7561-6e2e-424755343200
636f6d2e-6a69-7561-6e2e-425753563032
7365642e-6a69-7561-6e2e-425041563130
636f6d2e-6a69-7561-6e2e-424755343200
7265632e-6a69-7561-6e2e-414d56313100
f62995e6922547e294d11f7218a91383
636f6d2e-6a69-7561-6e2e-485332533032
f845fc6716664a2aaf52e58b9aaf4881
399027b443004d4b93b6570567318a8e
9745d67abfac436a9ca101d11ebd2ea1
b497716bec0b4850a0cc1d2026412d9a
7365646a-6975-616e-2e42-475634323000
1000cb16425d4dbc844718322cc1de9e
0e04a426ab964f068cfb46a4f964e700
7265632e-6a69-7561-6e2e-424756343000
636f6d2e-6a69-7561-6e2e-424756343500

POSSIBLE SECRETS
716cb07e07e34da181ce7c66af8d3b6e
f655fca476104655b4b7a89cfde03661
98a5cba3e3a7420cabc66343fea0c964
202570447f88469ba83051ea3a16d81e
f845fc6716646a2aaf52e58b9aaf4881
8cb5d0d8417f4254b6960b74bde20623
bb20763bdcd544ebba960fe8233252dd
7f3894e6ab614c778d47c61bd1f605e6
ace761655f754e11843fcd408517db5d
7265632e-6a69-7561-6e2e-424756343300
7365642e-6a69-7561-6e2e-425041563231
46d171ad45fa41d88ee4af3257d67066
9f80b0dafe394009a28756d17d077472
8ef723f6792f40778aec4f1dc1229cb0
636f6d2e-6a69-7561-6e2e-454347563130
800700ec199843e1988677893a838a87
7365642e-6a69-7561-6e2e-425056323400
636f6d2e-6a69-7561-6e2e-414d56313000

POSSIBLE SECRETS
06184b97223f4b20bc5aa56c1637a37e
0136024004378801593602O505
4c60fce10c154ff2a3ebd4fbe040e782
636f6d2e-6a69-7561-6e2e-425056333000
7365642e-6a69-7561-6e2e-424756343300
dd603c07bff9428280e0c7452b48a79e
d7552cab65714e28a080b9a8caa42a65
bc38642855144e4a8bb47e29a71e8c39
636f6d2e-6a69-7561-6e2e-425041563130
63220b76c65441c09151b753450e39ec
cec7c99b534049de90b211ac7f4e90c5
6695adca89834f1794cc02ac1ff7c7fc
12c878d58c4b48f6abd282fd74c990ee
7365642e-6a69-7561-6e2e-414d56313000
7265632e-6a69-7561-6e2e-454347563130
7265632e-6a69-7561-6e2e-414d56313200
e6004ee3520a4e4f91fd621489c3fdeb
1176afb15bf946a396cedd785f316372

POSSIBLE SECRETS
7265632e-6a69-7561-6e2e-425042563130
49e8e57939694526bbfa0da8c7a80622
636f6d2e-6a69-7561-6e2e-425753563031
a72ea89a88444112a931f71234bd61f4
7365642e-6a69-7561-6e2e-424756343200
ca15f57b71444381a5a75272a8c32e9d
27df995faeb34ca7ae5ab72a9dc2face
636f6d2e-6a69-7561-6e2e-505433534254
6a97e0de8bcf4ae2a042b1b924cfae4b
6089f6b908684656a84fd5ce449042bf
6f6d2e6a-6975-616e-2e42-475634323000
7365642e-6a69-7561-6e2e-414d56313200
7265632e-6a69-7561-6e2e-424c45303100
7265632e-6a69-7561-6e2e-504f31000000
636f6d2e-6a69-7561-6e2e-414d56313100
33e26882afaa4e51a75e6847c1be087b
7365642e-6a69-7561-6e2e-504f31000000
163fc4265de64d518e287d7696d3b71f

POSSIBLE SECRETS
7265632e-6a69-7561-6e2e-425041563130
399027b443041d4b93b6570576318a8e
636f6d2e-6a69-7561-6e2e-425056323500
3ae4618f19f64aa89446719af52db000
636f6d2e-6a69-7561-6e2e-425042563130
7365642e-6a69-7561-6e2e-424c45303100
6a697561-6e2e-636f-6d2e-424756343200
192c31f3f8b111eaa89902a205162323
d33f5ba526e44b58ab84c6f29d00b716
9a1932f91aba409baafa9c091728ec8d
636f6d6a-6975-616e-2e42-475634323000
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
636f6d2e-6a69-7561-6e2e-424756343400
7365642e-6a69-7561-6e2e-425042563130
e3c149d65d2b4b97a0fcb520a83f923a
4e4d39ad421e47dea254a86d91e673e3
c1da25bfc46b4a638839f454bb96b725
16ddf342816b4401a2eab2e57a2afcd2

POSSIBLE SECRETS
7265632c-6a69-7561-6e2e-424756343200
08f8480f0d2f4bd4bb63a23ceebeb45a
7274782e-6a69-7561-6e2e-425753563031
7265632e-6a69-7561-6e2e-424756343200
569f5746b8a840a490a4f7287ba822fa
636f6d2c-6a69-7561-6e2e-424756343200
7365642e-6a69-7561-6e2e-424756343400
f0d8b10f2b8f48ec9939cf4efbfe366e
7365642e-6a69-7561-6e2e-424756343000
7365642e-6a69-7561-6e2e-414d56313100
8f75928e6bc9490bafea38be9d3e678c
759ab656ca4d439ca7a290a9d00ac36a
b6e5a20ce407455b87d539f97da63f9f
038e0b1af7794472a7e663d27aa59573
d00bb36fc4d549b4a3c32973cd578ada
636f6d2e-6a69-7561-6e2e-504f31000000
7265632e-6a69-7561-6e2e-414d56313000
7274782e-6a69-7561-6e2e-425753563032

POSSIBLE SECRETS
636f6d2e-6a69-7561-6e2e-424756323000
828811c6b7494c7b8c34b101a95f7877
636f6d2e-6a69-7561-6e2e-425041563231
636f6d2e-6a69-7561-6e2e-424c45303100
7365642e-6a69-7561-6e2e-454347563130
9e4a5f26773e4d8a87ce2b83fa2641b3
11e89cb2030745b0839adb744f410cd4
636f6d2e-6a69-7561-6e2e-424756343000
d63856e6867d45a2b5d4a598e49cc161
7274782e-6a69-7561-6e2e-504f56313100
8ef723f6792f77058aec4fcd11229cb0
b3118e4fa5204f6dba1e2f1723270747
572d1e2710ae5fbca54c76a382fdd44050b3a675cb2bf39feebe85ef63d947aff0fa4943f1112e8b6af34bebebbaefa1a0aae055d9259b89a1858f7cc9af9df1
7265632e-6a69-7561-6e2e-424756323000
7365642e-6a69-7561-6e2e-425056333000
269b771d557543c98f107fd6df2ca96a
3574ce171f834a109a572d0a3431025b
636f6d2e-6a69-7561-6e2e-424756343300

POSSIBLE SECRETS
444f63ec37a843e497566855a0d45fec
7365642e-6a69-7561-6e2e-424755343200
636f6d2e-6a69-7561-6e2e-414d56313200
8168e412dfef47bb865ac097b91e95cc
4afa5254bd374475afc5fcf0155f06d7
87a5c5fde8a1413bb34f1059e6a9a377
636f6d2e-6a69-7561-6e2e-425056323400
7365642e-6a69-7561-6e2e-424756323000
00001530-1212-efde-1523-785feabcd123
9252cb16425d4dbc844718223cc1de9e
636f6d2e-6a69-7561-6e2e-504f56313100
c629584d4e8141a6b18b2fab90d28b1e
7365642e-6a69-7561-6e2e-485332533032
7265636a-6975-616e-2e42-475634323000
388072b443041d4b93b6570576318a8e
662e062c4b264c1abc107f6e626f5012
7365642c-6a69-7561-6e2e-424756343200
6c6944aa58b14f119b338eb24e9a07f4

POSSIBLE SECRETS
636f6d2e-6a69-7561-6e2e-424756343200
7c789858c0ec4ebf8189ebb14b6730a5
7265632e-6a69-7561-6e2e-485332533032
7265632e-6a69-7561-6e2e-424756343400
8c14e817f97811eaa89902a205162323
af7593f2e0744df2ab05f053d08f4dbf
789495e955fe4d59b007c365cfd61412

PLAYSTORE INFORMATION

Title: iHealth MyVitals

Score: 4.7668223 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.ihealthlabs.MyVitalsPro

Developer Details: iHealth Labs, Inc., iHealth+Labs,+Inc., None, http://ihealthlabs.com, support@ihealthlabs.com,

Release Date: Oct 16, 2020 **Privacy Policy:** Privacy link

Description:

The Myvitals App allows users to easily manage and view their health data. By creating an iHealth account and connecting our devices, you'll be able to store data securely in the cloud. [Device Support] This app will support iHealth blood pressure monitors, pulse oximeters, touchless forehead thermometers, weighing scales, and smartwatch (enable the user to connect a mobile device to a connected smartwatch send/receive texts and phone calls) [Graphs and charts] Using easy-to-read graphs and charts, you'll be able to view changes and trends over time. You can view all types of graphic trends on the same screen and use the share function to keep your care team up to date with your condition status. [Measurement Results] After taking a measurement, you'll be able to see the results in real-time. By connecting the device to your iHealth account, you'll be able to sync the data and access it at any time. [Contact Us] If you have any questions about how to use our products, or if you would like to provide feedback, please let us know in the app. You may message the care team directly or fill out the feedback form in the settings section.

SCAN LOGS

Timestamp	Event	Error

2025-09-01 00:01:38	Generating Hashes	OK
2025-09-01 00:01:38	Extracting APK	OK
2025-09-01 00:01:38	Unzipping	OK
2025-09-01 00:01:39	Parsing APK with androguard	OK
2025-09-01 00:01:40	Extracting APK features using aapt/aapt2	OK
2025-09-01 00:01:41	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 00:01:41	Parsing AndroidManifest.xml	OK
2025-09-01 00:01:41	Extracting Manifest Data	OK
2025-09-01 00:01:41	Manifest Analysis Started	OK
2025-09-01 00:01:41	Reading Network Security config from network_security_config.xml	OK
2025-09-01 00:01:41	Parsing Network Security config	OK
2025-09-01 00:01:41	Performing Static Analysis on: iHealth (com.ihealthlabs.MyVitalsPro)	OK

2025-09-01 00:01:42	Fetching Details from Play Store: com.ihealthlabs.MyVitalsPro	OK
2025-09-01 00:01:44	Checking for Malware Permissions	OK
2025-09-01 00:01:44	Fetching icon path	OK
2025-09-01 00:01:44	Library Binary Analysis Started	OK
2025-09-01 00:01:44	Analyzing lib/arm64-v8a/libiHealth.so	OK
2025-09-01 00:01:44	Analyzing lib/arm64-v8a/libVeryFitMulti.so	OK
2025-09-01 00:01:44	Analyzing lib/arm64-v8a/libindoor.so	OK
2025-09-01 00:01:44	Analyzing lib/arm64-v8a/libECGOffline.so	OK
2025-09-01 00:01:44	Analyzing lib/arm64-v8a/libc++_shared.so	OK
2025-09-01 00:01:44	Analyzing lib/arm64-v8a/libimage_processing_util_jni.so	OK
2025-09-01 00:01:44	Analyzing lib/arm64-v8a/libECGOnline.so	OK
2025-09-01 00:01:44	Analyzing lib/arm64-v8a/libmarsstn.so	OK

2025-09-01 00:01:44	Analyzing lib/arm64-v8a/libBodyfat_SDK.so	OK
2025-09-01 00:01:44	Analyzing lib/arm64-v8a/liblocSDK7d.so	OK
2025-09-01 00:01:44	Analyzing lib/arm64-v8a/libmarsxlog.so	OK
2025-09-01 00:01:44	Analyzing lib/x86_64/libiHealth.so	OK
2025-09-01 00:01:44	Analyzing lib/x86_64/libVeryFitMulti.so	OK
2025-09-01 00:01:44	Analyzing lib/x86_64/libindoor.so	OK
2025-09-01 00:01:44	Analyzing lib/x86_64/libECGOffline.so	OK
2025-09-01 00:01:44	Analyzing lib/x86_64/libimage_processing_util_jni.so	OK
2025-09-01 00:01:44	Analyzing lib/x86_64/libECGOnline.so	OK
2025-09-01 00:01:44	Analyzing lib/x86_64/libBodyfat_SDK.so	OK
2025-09-01 00:01:44	Analyzing lib/x86_64/liblocSDK7d.so	OK
2025-09-01 00:01:44	Analyzing lib/armeabi-v7a/libiHealth.so	OK

2025-09-01 00:01:44	Analyzing lib/armeabi-v7a/libVeryFitMulti.so	OK
2025-09-01 00:01:44	Analyzing lib/armeabi-v7a/libindoor.so	OK
2025-09-01 00:01:44	Analyzing lib/armeabi-v7a/libECGOffline.so	OK
2025-09-01 00:01:44	Analyzing lib/armeabi-v7a/libc++_shared.so	OK
2025-09-01 00:01:44	Analyzing lib/armeabi-v7a/libimage_processing_util_jni.so	OK
2025-09-01 00:01:44	Analyzing lib/armeabi-v7a/libECGOnline.so	OK
2025-09-01 00:01:44	Analyzing lib/armeabi-v7a/libmarsstn.so	OK
2025-09-01 00:01:44	Analyzing lib/armeabi-v7a/libBodyfat_SDK.so	OK
2025-09-01 00:01:44	Analyzing lib/armeabi-v7a/liblocSDK7d.so	OK
2025-09-01 00:01:44	Analyzing lib/armeabi-v7a/libmarsxlog.so	OK
2025-09-01 00:01:44	Analyzing lib/x86/libiHealth.so	OK
2025-09-01 00:01:44	Analyzing lib/x86/libVeryFitMulti.so	OK

2025-09-01 00:01:45	Analyzing lib/x86/libindoor.so	OK
2025-09-01 00:01:45	Analyzing lib/x86/libECGOffline.so	OK
2025-09-01 00:01:45	Analyzing lib/x86/libimage_processing_util_jni.so	OK
2025-09-01 00:01:45	Analyzing lib/x86/libECGOnline.so	OK
2025-09-01 00:01:45	Analyzing lib/x86/libBodyfat_SDK.so	OK
2025-09-01 00:01:45	Analyzing lib/x86/liblocSDK7d.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/arm64-v8a/libiHealth.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/arm64-v8a/libVeryFitMulti.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/arm64-v8a/libindoor.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/arm64-v8a/libECGOffline.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/arm64-v8a/libc++_shared.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/arm64-v8a/libimage_processing_util_jni.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/arm64-v8a/libECGOnline.so	OK

2025-09-01 00:01:45	Analyzing apktool_out/lib/arm64-v8a/libmarsstn.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/arm64-v8a/libBodyfat_SDK.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/arm64-v8a/liblocSDK7d.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/arm64-v8a/libmarsxlog.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/x86_64/libiHealth.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/x86_64/libVeryFitMulti.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/x86_64/libindoor.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/x86_64/libECGOffline.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/x86_64/libimage_processing_util_jni.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/x86_64/libECGOnline.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/x86_64/libBodyfat_SDK.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/x86_64/liblocSDK7d.so	OK

2025-09-01 00:01:45	Analyzing apktool_out/lib/armeabi-v7a/libiHealth.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/armeabi-v7a/libVeryFitMulti.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/armeabi-v7a/libindoor.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/armeabi-v7a/libECGOffline.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/armeabi-v7a/libc++_shared.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/armeabi-v7a/libimage_processing_util_jni.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/armeabi-v7a/libECGOnline.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/armeabi-v7a/libmarsstn.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/armeabi-v7a/libBodyfat_SDK.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/armeabi-v7a/liblocSDK7d.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/armeabi-v7a/libmarsxlog.so	OK
2025-09-01 00:01:45	Analyzing apktool_out/lib/x86/libiHealth.so	OK

2025-09-01 00:01:45	Analyzing apktool_out/lib/x86/libVeryFitMulti.so	OK
2025-09-01 00:01:46	Analyzing apktool_out/lib/x86/libindoor.so	OK
2025-09-01 00:01:46	Analyzing apktool_out/lib/x86/libECGOffline.so	OK
2025-09-01 00:01:46	Analyzing apktool_out/lib/x86/libimage_processing_util_jni.so	OK
2025-09-01 00:01:46	Analyzing apktool_out/lib/x86/libECGOnline.so	OK
2025-09-01 00:01:46	Analyzing apktool_out/lib/x86/libBodyfat_SDK.so	OK
2025-09-01 00:01:46	Analyzing apktool_out/lib/x86/liblocSDK7d.so	OK
2025-09-01 00:01:46	Reading Code Signing Certificate	OK
2025-09-01 00:01:46	Running APKiD 2.1.5	OK
2025-09-01 00:01:53	Updating Trackers Database....	OK
2025-09-01 00:01:53	Detecting Trackers	OK
2025-09-01 00:01:59	Decompiling APK to Java with JADX	OK

2025-09-01 00:31:56	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/e235e29bcc9de21aaec336958a7bce51/java_source', '-q', '-r', '--show-bad-code', '/home/mobsf/.MobSF/uploads/e235e29bcc9de21aaec336958a7bce51/e235e29bcc9de21aaec336958a7bce51.apk'], 999.9999721646309)
2025-09-01 00:31:56	Converting DEX to Smali	OK
2025-09-01 00:31:56	Code Analysis Started on - java_source	OK
2025-09-01 00:32:06	Android SBOM Analysis Completed	OK
2025-09-01 00:32:12	Android SAST Completed	OK
2025-09-01 00:32:12	Android API Analysis Started	OK
2025-09-01 00:32:17	Android API Analysis Completed	OK
2025-09-01 00:32:18	Android Permission Mapping Started	OK
2025-09-01 00:32:26	Android Permission Mapping Completed	OK
2025-09-01 00:32:27	Android Behaviour Analysis Started	OK
2025-09-01 00:32:33	Android Behaviour Analysis Completed	OK
2025-09-01 00:32:33	Extracting Emails and URLs from Source Code	OK

2025-09-01 00:32:36	Email and URL Extraction Completed	OK
2025-09-01 00:32:36	Extracting String data from APK	OK
2025-09-01 00:32:37	Extracting String data from SO	OK
2025-09-01 00:32:37	Extracting String data from Code	OK
2025-09-01 00:32:37	Extracting String values and entropies from Code	OK
2025-09-01 00:32:42	Performing Malware check on extracted domains	OK
2025-09-01 00:32:57	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.