

ANDROID STATIC ANALYSIS REPORT



H Band (10.5.08)

File Name: com.veepoo.hband_10508.apk

Package Name: com.veepoo.hband

Scan Date: Sept. 1, 2025, 11:10 a.m.

App Security Score:

44/100 (MEDIUM RISK)

Grade:

B

Trackers Detection:

1/432

♣ FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	ℚ HOTSPOT
6	34	2	1	16



File Name: com.veepoo.hband_10508.apk

Size: 41.14MB

MD5: 48598b911ee4180c3f0b1558c11fe130

SHA1: 5edee6302f690e243d8a7c452da61ad39f94be8b

SHA256: 922a30de3c54d93ec1603c086c26c6e8783ece47224c697a20301bd3fcc47a64

i APP INFORMATION

App Name: H Band

Package Name: com.veepoo.hband

Main Activity: com.veepoo.hband.activity.LaunchActivity

Target SDK: 34 Min SDK: 21 Max SDK:

Android Version Name: 10.5.08 Android Version Code: 10508

APP COMPONENTS

Activities: 240
Services: 18
Receivers: 11
Providers: 8
Exported Activities: 6
Exported Services: 12
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed v1 signature: True v2 signature: True v3 signature: False v4 signature: False X.509 Subject: C=86

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2015-07-15 02:16:14+00:00

Valid To: 2065-07-02 02:16:14+00:00

Issuer: C=86

Serial Number: 0x2b6c2de1

Hash Algorithm: sha256

md5: cdc93a50e26108a342d36bd01fbae1fc

sha1: 808ec43127c1292581affc31c886b58a96714a8b

sha256: 81da19948bfd13139cae459f1bd4e63b8c780e2be846471e74392c0562b53ac5

sha512:961a6d713803bb0b8b030963cbd3452cb104031df29f345e3cd5e0409a5317cffefe58e124055c6c4eee7832edd62e190ff78e693a7e558202a19e6a810790e9

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: ec6dceed93f792b51215a2c1c62092a3306f44b6cec0317f05a0c03e9cdadcc8

Found 1 unique certificates

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE		read external storage contents	Allows an application to read from external storage.
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.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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.DISABLE_KEYGUARD	normal	disable keyguard	Allows applications to disable the keyguard if it is not secure.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.SYSTEM_OVERLAY_WINDOW	unknown	Unknown permission	Unknown permission from android reference
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.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
android.permission.ANSWER_PHONE_CALLS	dangerous	permits an app to answer incoming phone calls.	Allows the app to answer an incoming phone call.
android.permission.CALL_PHONE dange		directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.PROCESS_OUTGOING_CALLS	dangerous	intercept outgoing calls	Allows application to process outgoing calls and change the number to be dialled. Malicious applications may monitor, redirect or prevent outgoing calls.
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.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	normal	access extra location provider commands	Access extra location provider commands. Malicious applications could use this to interfere with the operation of the GPS or other location sources.
android.permission.QUERY_ALL_PACKAGES	normal	enables querying any normal app on the device.	Allows query of any normal app on the device, regardless of manifest declarations.
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.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.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.BLUETOOTH_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.MEDIA_CONTENT_CONTROL	normal	allows control over media content playback.	Allows an application to know what content is playing and control its playback.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE_CONNECTED_DEVICE norma		enables foreground services with connected device use.	Allows a regular application to use Service.startForeground with the type "connectedDevice".
android.permission.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".
android.permission.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.

ক্ল APKID ANALYSIS

FILE	DETAILS	
	FINDINGS	DETAILS
classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.TAGS check
	Compiler	r8
	FINDINGS	DETAILS
classes2.dex	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.BOARD check possible Build.SERIAL check SIM operator check subscriber ID check
	Compiler	r8 without marker (suspicious)

FILE		DETAILS	
		FINDINGS	DETAILS
		Anti-VM Code	Build.MANUFACTURER check
classes3.dex		Obfuscator	unreadable field names unreadable method names
		Compiler	r8 without marker (suspicious)
lib/arm64-v8a/libJni_wgs2gcj.so		FINDINGS	DETAILS
		Obfuscator	Obfuscator-LLVM version 3.6.1
lib/armeabi-v7a/libJni_wgs2gcj.so		FINDINGS	DETAILS
		Obfuscator	Obfuscator-LLVM version 3.6.1
lib/armeabi/libJni_wgs2gcj.so		FINDINGS	DETAILS
instanticus in instan		Obfuscator	Obfuscator-LLVM version 3.6.1
	<u> </u>		
		FINDINGS	DETAILS
lib/x86/libJni_wgs2gcj.so		Obfuscator	Obfuscator-LLVM version 3.6.1

FILE	DETAILS			
lib/x86_64/libJni_wgs2gcj.so		FINDINGS	DETAILS	
110/ X00_04/110J111_vvg32gq.30		Obfuscator	Obfuscator-LLVM vei	rsion 3.6.1
		FINDINGS		DETAILS
assets/skin/theme-20201107.skin!classes.dex		Compiler		r8

■ BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.veepoo.hband.activity.LaunchActivity	Schemes: UMENG_TEST://,
com.mob.tools.MobUIShell	Schemes: tencent100381282://,

△ NETWORK SECURITY

ı	NO	SCOPE	SEVERITY	DESCRIPTION
---	----	-------	----------	-------------

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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

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

Q MANIFEST ANALYSIS

HIGH: 2 | WARNING: 23 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
4	Activity (com.veepoo.hband.activity.TestActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Activity (com.veepoo.hband.activity.MainActivity) 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	Service (com.veepoo.hband.activity.connected.oad.DfuService) 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.
7	Service (com.veepoo.hband.ble.BluetoothService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.FOREGROUND_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.

NO	ISSUE	SEVERITY	DESCRIPTION
8	Service (com.veepoo.hband.ble.NotificationCollectorMonitorService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.FOREGROUND_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	Service (com.veepoo.hband.activity.MusicOpraterService) 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.
10	Service (com.amap.api.location.APSService) 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.
11	Service (com.veepoo.hband.activity.gps.service.LocationService2d) 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.
12	Service (com.veepoo.hband.phone.MessageNotifyCollectService) 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.
13	Broadcast Receiver (com.veepoo.hband.phone.TimeChangedReceiver) 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.
14	Broadcast Receiver (com.veepoo.hband.activity.music.MusicPlayActionReceiver) 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.
15	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.
16	Broadcast Receiver (no.nordicsemi.android.support.v18.scanner.PendingIntentReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
17	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_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.
18	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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.
19	Activity (com.mob.id.MobIDSYActivity) 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.
20	Activity (com.mob.guard.MobTranPullLockActivity) 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.
21	Service (com.mob.MobACService) 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.
22	Activity (com.mob.id.MobIDActivity) 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.
23	Service (com.mob.id.MobIDService) 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.
24	Activity (com.mob.guard.MobTranPullUpActivity) 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.
25	Service (com.mob.guard.MobGuardPullUpService) 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.

</> CODE ANALYSIS

butterknife/ButterKnife.java cat/ereza/customactivityoncrash/CustomActivityOnCra: va cn/smssdk/net/b.java cn/smssdk/lutils/DHelper.java cn/smssdk/tutils/SMSLog.java com/activeandroid/ActiveAndroid.java com/activeandroid/Cache.java com/activeandroid/Configuration.java com/activeandroid/Modellero.java com/activeandroid/Modellinfo.java com/activeandroid/Modellinfo.java com/activeandroid/Tablelinfo.java com/activeandroid/Tablelinfo.java com/activeandroid/tutils/Quits.java com/activeandroid/tutils/Quits.java com/activeandroid/tutils/Quits.java com/activeandroid/tutils/Quitslis.java com/bumptech/gilde/disklrucache/DiskLruCache.java com/bumptech/gilde/disklrucache/DiskLruCache.java com/bumptech/gilde/jifdecoder/Gifheader/Parser.java com/bumptech/gilde/jifdecoder/StandardGifbecoder.java com/bumptech/gilde/jifdecoder/StandardGifbecoder.java
com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbFeti java com/bumptech/glide/load/data/mediastore/ThumbFeti java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/GourceGenerator.java com/bumptech/glide/load/engine/burreGenerator.java com/bumptech/glide/load/engine/bitmap_recycle/LruA Pool.java com/bumptech/glide/load/engine/bitmap_recycle/LruB apPool.java com/bumptech/glide/load/engine/cache/DiskLruCache/ pper.java com/bumptech/glide/load/engine/cache/MemorySizeC lator.java com/bumptech/glide/load/engine/cache/MemorySizeC

NO	ISSUE	SEVERITY	STANDARDS	com/bumptech/glide/load/model/ByteBufferFileLoader.jav
				com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/resource/lmageDecoderResourc eDecoder.java com/bumptech/glide/load/resource/bitmap/BitmapEncode r.java com/bumptech/glide/load/resource/bitmap/BitmapImage DecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultImage HeaderParser.java com/bumptech/glide/load/resource/bitmap/Downsampler. java com/bumptech/glide/load/resource/bitmap/Downsampler. java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/Transformatio nlttils.java com/bumptech/glide/load/resource/bitmap/Transformatio nlttils.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder. java com/bumptech/glide/load/resource/gif/GifDrawableEncod er.java com/bumptech/glide/load/resource/gif/StreamGifDecoder. java com/bumptech/glide/load/resource/gif/StreamGifDecoder. java com/bumptech/glide/manager/DefaultConnectivityMonitor java com/bumptech/glide/manager/RequestManagerFragment.j ava com/bumptech/glide/manager/RequestManagerFragment.j ava com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SupportRequestManagerFr agment.java com/bumptech/glide/manager/SupportRequestManagerFr agment.java com/bumptech/glide/manager/SingleRequest.java com/bumptech/glide/request/singleRequest.java com/bumptech/glide/request/singleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignatur e.java com/bumptech/glide/signature/ApplicationVersionSignatur e.java com/bumptech/glide/tiil/ContentLengthInputStream.java com/bumptech/glide/tiil/ContentLengthInputStream.java com/bumptech/glide/tiil/ContentLengthInputStream.java com/bumptech/glide/tiil/ContentLengthInputStream.java com/bumptech/glide/tiil/ContentLengthInputStream.java

OV	ISSUE	SEVERITY	STANDARDS	com/github/mikephil/charting/charts/Chart.java ፍሬኬዊ§thub/mikephil/charting/charts/CombinedChart.java
				com/github/mikephil/charting/charts/HorizontalBarChart.j
				ava
				com/github/mikephil/charting/charts/PieRadarChartBase.ja
				va
				com/github/mikephil/charting/components/AxisBase.java
				com/github/mikephil/charting/data/ChartData.java
				com/github/mikephil/charting/data/CombinedData.java
				com/github/mikephil/charting/data/LineDataSet.java
				com/github/mikephil/charting/data/PieEntry.java
				com/github/mikephil/charting/listener/BarLineChartTouch
				Listener.java
				com/github/mikephil/charting/renderer/ScatterChartRende
				rer.java
				com/github/mikephil/charting/utils/FileUtils.java
				com/github/mikephil/charting/utils/Utils.java
				com/goodix/ble/libble/v2/impl/BleCharacteristicX.java
				com/goodix/ble/libble/v2/impl/BleGattX.java
				com/goodix/ble/libble/v2/impl/BleRemoteDevice.java
				com/goodix/ble/libble/v2/impl/BleServiceX.java
				com/goodix/ble/libcomx/file/RotateFileOutputStream.java
				com/goodix/ble/libcomx/trx/TrxChain.java
				com/hp/hpl/sparta/DefaultLog.java
				com/hp/hpl/sparta/ParseByteStream.java
				com/hp/hpl/sparta/ParseCharStream.java
				com/hp/hpl/sparta/ParseException.java
				com/huawei/agconnect/AGConnectInstance.java
				com/huawei/agconnect/config/impl/Utils.java
				com/huawei/agconnect/config/impl/c.java
				com/huawei/agconnect/config/impl/e.java
				com/huawei/agconnect/config/impl/h.java
				com/huawei/agconnect/config/impl/k.java
				com/huawei/agconnect/core/a/b.java
				com/huawei/agconnect/core/a/c.java
				com/huawei/agconnect/core/a/d.java
				com/huawei/agconnect/core/provider/AGConnectInitialize
				Provider.java
				com/huawei/hmf/tasks/a/g.java
				com/huawei/hms/common/util/Logger.java
				com/huawei/hms/feature/DynamicModuleInitializer.java
				com/huawei/hms/feature/dynamic/DeferredLifecycleHelpe
				r.java
				com/huawei/hms/feature/dynamic/e/a.java
				com/huawei/hms/feature/dynamic/e/b.java
				com/huawei/hms/feature/dynamic/f/e.java
				com/huawei/hms/framework/common/Logger.java
				com/huawei/hms/hatool/m0.java
				com/huawei/hms/hmsscankit/RemoteView.java
				com/huawei/hms/hmsscankit/ScanKitActivity.java
				com/huawei/hms/hmsscankit/ScanUtil.java
				com/huawei/hms/hmsscankit/c.java

NO	ISSUE	SEVERITY	STANDARDS	com/huawei/hms/hmsscankit/f.java
				com/huawei/hms/ml/common/utils/ActivityMgr.java
				com/huawei/hms/ml/common/utils/CountryCodeBean.jav
				a
				com/huawei/hms/ml/common/utils/SmartLog.java
				com/huawei/hms/ml/common/utils/StreamUtils.java
				com/huawei/hms/ml/scan/HmsScan.java
				com/huawei/hms/mlsdk/common/AgConnectInfo.java
				com/huawei/hms/mlsdk/common/MLApplication.java
				com/huawei/hms/mlsdk/common/provider/MLInitializerPr
				ovider.java
				com/huawei/hms/scankit/ViewfinderView.java
				com/huawei/hms/scankit/b.java
				com/huawei/hms/scankit/c.java
				com/huawei/hms/scankit/drawable/ScanDrawable.java
				com/huawei/hms/scankit/e.java
				com/huawei/hms/scankit/h.java
				com/huawei/hms/scankit/i.java
				com/huawei/hms/scankit/p/a4.java
				com/huawei/hms/scankit/p/f0.java
				com/huawei/hms/scankit/p/h0.java
				com/huawei/hms/scankit/p/i0.java
				com/huawei/hms/scankit/p/j0.java
				com/huawei/hms/scankit/p/l0.java
				com/huawei/hms/scankit/p/m1.java
				com/huawei/hms/scankit/p/n0.java
				com/huawei/hms/scankit/p/n1.java
				com/huawei/hms/scankit/p/o4.java
				com/huawei/hms/scankit/p/u3.java
				com/huawei/hms/scankit/p/w7.java
				com/huawei/hms/scankit/p/y3.java
				com/huawei/secure/android/common/anonymization/Ano
				nymizer.java
				com/huawei/secure/android/common/encrypt/keystore/rs
				a/RSASignKS.java
				com/huawei/secure/android/common/encrypt/utils/b.java
				com/huawei/secure/android/common/ssl/util/BksUtil.java
				com/huawei/secure/android/common/ssl/util/e.java
				com/huawei/secure/android/common/util/EncodeUtil.java
				com/huawei/secure/android/common/util/HexUtil.java
				com/huawei/secure/android/common/util/IOUtil.java
				com/huawei/secure/android/common/util/LogsUtil.java
				com/huawei/secure/android/common/util/PermissionUtil.j
				ava
				com/huawei/secure/android/common/util/SafeBase64.jav
				a
				com/huawei/secure/android/common/util/SafePrintExcept
				ion.java
				com/huawei/secure/android/common/util/SafeString.java
				com/huawei/secure/android/common/util/SafeStringBuffe
				r.java

NO	ISSUE	SEVERITY	STANDARDS	com/huawei/secure/android/common/util/SafeStringBuild
				com/huawei/secure/android/common/util/ZipUtil.java
				com/huawei/secure/android/common/util/a.java
				com/huawei/secure/android/common/webview/SafeGetUr
				l.java
				com/huawei/secure/android/common/webview/SafeWebV
				iew.java
				com/huawei/secure/android/common/webview/UriUtil.jav
				com/jieli/bmp_convert/BmpConvert.java
				com/jieli/jl_bt_ota/impl/BluetoothBase.java
				com/jieli/jl_bt_ota/impl/BluetoothBreProfiles.java
				com/jieli/jl_bt_ota/impl/BluetoothDiscovery.java
				com/jieli/jl_bt_ota/impl/BluetoothOTAManager.java
				com/jieli/jl_bt_ota/impl/RcspAuth.java
				com/jieli/jl_bt_ota/model/cmdHandler/RcspCmdHandler.ja
				va
				com/jieli/jl_bt_ota/thread/ReadFileThread.java
				com/jieli/jl_bt_ota/tool/DataHandler.java
				com/jieli/jl_bt_ota/tool/DataHandlerModify.java
				com/jieli/jl_bt_ota/tool/DeviceReConnectManager.java
				com/jieli/jl_bt_ota/tool/ParseHelper.java
				com/jieli/jl_bt_ota/tool/RcspParser.java
				com/jieli/jl_bt_ota/util/BluetoothUtil.java
				com/jieli/jl_bt_ota/util/FileUtil.java
				com/jieli/jl_bt_ota/util/JL_Log.java com/jieli/jl_bt_ota/util/ParseDataUtil.java
				com/jieli/jl_fatfs/FatFileSystem.java
				com/jieli/jl_fatfs/tool/PackResFormat.java
				com/jieli/ji_fatfs/tool/ReadFileThread.java
				com/jieli/jl_fatfs/utils/ZipUtil.java
				com/jieli/jl_filebrowse/FileBrowseManager.java
				com/jieli/jl_filebrowse/FileBrowseUtil.java
				com/jieli/jl_filebrowse/util/DeviceChoseUtil.java
				com/jieli/jl_rcsp/impl/DataTransferOpImpl.java
				com/jieli/jl_rcsp/impl/NfcOpImpl.java
				com/jieli/jl_rcsp/impl/OnFileBrowseCallbackImpl.java
				com/jieli/jl_rcsp/impl/RTCOplmpl.java
				com/jieli/jl_rcsp/impl/RcspAuth.java
				com/jieli/jl_rcsp/impl/RcspOpImpl.java
				com/jieli/jl_rcsp/impl/RecordOpImpl.java
				com/jieli/jl_rcsp/impl/WatchOpImpl.java
				com/jieli/jl_rcsp/model/cmdHandler/DeviceExtendParamC
				mdHandler.java com/jieli/jl_rcsp/model/cmdHandler/HealthSettingCmdHan
				dler.java
				com/jieli/jl_rcsp/model/cmdHandler/NFCOperationCmdHa
				ndler.java
				com/jieli/jl_rcsp/model/cmdHandler/RcspCmdHandler.java
				com/jieli/jl_rcsp/model/cmdHandler/SmallFileTransferCmd
1				Handler.java
1	The App logs information. Sensitive information	info	CWE: CWE-532: Insertion of Sensitive Information into Log File	

ا م	should never be logged.	CEL (EDIT)	OWASP MASVS: MSTG-STORAGE-3	com/jieli/jl_rcsp/model/cmdHandler/SportsInfoStatusCmd
0	ISSUE	SEVERITY	STANDARDS	Filio⊞Se r.java
-				com/jieli/jl_rcsp/model/command/file_op/LargeFileTransfe
				rGetNameCmd.java
				com/jieli/jl_rcsp/model/device/NfcMsg.java
				com/jieli/jl_rcsp/model/device/health/AirPressure.java
				com/jieli/jl_rcsp/model/device/health/Altitude.java
				com/jieli/jl_rcsp/model/device/health/ExerciseRecoveryTi
				me.java
				com/jieli/jl_rcsp/model/device/health/HeartRate.java
				com/jieli/jl_rcsp/model/device/health/MaxOxygenUptake.j
				ava
				com/jieli/jl_rcsp/model/device/health/OxygenSaturation.ja va
				com/jieli/jl_rcsp/model/device/health/PressureDetection.ja
				va
				com/jieli/jl_rcsp/model/device/health/SportsSteps.java
				com/jieli/jl_rcsp/model/device/health/TrainingLoad.java
				com/jieli/jl_rcsp/model/parameter/ModifyNfcMsgParam.ja
				va
				com/jieli/jl_rcsp/task/GetFileTask.java
				com/jieli/jl_rcsp/task/TaskBase.java
				com/jieli/jl_rcsp/task/TransferTask.java
				com/jieli/jl_rcsp/task/contacts/ReadContactsBySmallFileTas
				k.java
				com/jieli/jl_rcsp/task/contacts/ReadContactsTask.java
				com/jieli/jl_rcsp/task/contacts/UpdateContactsBySmallFile
				Task.java
				com/jieli/jl_rcsp/task/contacts/UpdateContactsTask.java
				com/jieli/jl_rcsp/task/format/FormatCmdTask.java
				com/jieli/jl_rcsp/task/format/FormatTask.java
				com/jieli/jl_rcsp/task/logcat/ReadLogcatTask.java
				com/jieli/jl_rcsp/task/nfc/NfcSyncTask.java
				com/jieli/jl_rcsp/task/smallfile/AddFileTask.java
				com/jieli/jl_rcsp/task/smallfile/DeleteFileTask.java
				com/jieli/jl_rcsp/task/smallfile/QueryFileTask.java
				com/jieli/jl_rcsp/task/smallfile/ReadFileTask.java
				com/jieli/jl_rcsp/tool/CustomRcspActionCallback.java
				com/jieli/jl_rcsp/tool/HealthDataParseHelper.java
				com/jieli/jl_rcsp/tool/RcspDataHandler.java
				com/jieli/jl_rcsp/tool/SyncMessageTask.java
				com/jieli/jl_rcsp/tool/UpdateResourceTask.java
				com/jieli/jl_rcsp/tool/UpdateResourceThread.java
				com/jieli/jl_rcsp/tool/WatchCallbackManager.java
				com/jieli/jl_rcsp/tool/datahandles/BasePacketParse.java
				com/jieli/jl_rcsp/tool/datahandles/DataHandlerModify.java
				com/jieli/jl_rcsp/tool/datahandles/DataHandlerOld.java
				com/jieli/jl_rcsp/tool/datahandles/ParseHelper.java
				com/jieli/jl_rcsp/tool/filebrowse/FileBrowseOperatorImpl.j
				ava com/jieli/jl_rcsp/tool/filebrowse/LrcReadOperatorImpl.java
				com/jieli/ji_rcsp/toti/iilebrowse/ErcReadOperatorimpi.java com/jieli/ji_rcsp/util/CrashHandler.java
				com/jieii/ji_rcsp/utii/crasmantiier.java

O	ISSUE	SEVERITY	STANDARDS	com/jieli/jl_rcsp/util/JL_Log.java
				com/jieli/jl_rcsp/util/WatchFileUtil.java
				com/jieli/jl_rcsp/watch/WatchBase.java
				com/jieli/jl_rcsp/watch/WatchProgressHandler.java
				com/jieli/jl_rcsp/watch/fatfs/FatFsBluetoothImp.java
				com/jieli/jl_rcsp/watch/fatfs/FatFsWatch.java
				com/jieli/jl_rcsp/watch/rcsp/RcspWatch.java
				com/luck/picture/lib/loader/LocalMediaPageLoader.java
				com/luck/picture/lib/thread/PictureThreadUtils.java
				com/luck/picture/lib/utils/PSEglUtils.java
				com/luck/picture/lib/utils/PictureFileUtils.java
				com/mob/MobSDK.java
				com/mob/commons/x.java
				com/mob/tools/log/NLog.java
				com/mob/tools/utils/SharePrefrenceHelper.java
				com/nanchen/compresshelper/FileUtil.java
				com/orhanobut/logger/AndroidLogAdapter.java
				com/veepoo/hband/HBandApplication.java
				com/veepoo/hband/ProcessObserver.java
				com/veepoo/hband/activity/MainActivity.java
				com/veepoo/hband/activity/MusicUtils.java
				com/veepoo/hband/activity/ThreadTest.java
				com/veepoo/hband/activity/connected/backdoor/JLOTATe
				stActivity.java
				com/veepoo/hband/activity/connected/backdoor/ShowBac
				kActivity.java
				com/veepoo/hband/activity/connected/backdoor/ShowLog
				Activity.java
				com/veepoo/hband/activity/connected/camera/CameraSur
				faceView.java
				com/veepoo/hband/activity/connected/camera/DisplayUtil
				.java
				com/veepoo/hband/activity/connected/detect/EcgMultiLea
				dDetectActivity.java
				com/veepoo/hband/activity/connected/oad/BluetrumOTA
				Activity.java
				com/veepoo/hband/activity/connected/oad/JLOTAActivity.j
				ava
				com/veepoo/hband/activity/connected/oad/OadNoricActiv
				ity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_172320_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_200320_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_228460_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_240240_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_240280_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				com, veepoornbandractivity/connected/setting/Editivation

NO	ISSUE	SEVERITY	STANDARDS	iJL_240284_Activity.java FULESeepoo/hband/activity/connected/setting/EditWatchU
				iJL_240286_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_240292_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_240296_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_240Round_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_320380_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_320386_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_320Round_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_360360_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_360Round_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_368448_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_390Round_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_410502_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_412Round_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_416Round_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_466Round_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_480Round_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				i_135240Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				i_167240Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				i_172320Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				i_200320Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				i_240240Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				i_240280Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				i_240284Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				i_240286Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				i_240295Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU

NO	ISSUE	SEVERITY	STANDARDS	i_240RoundActivity.java
				i_320380Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU i_360RoundActivity.java com/veepoo/hband/activity/connected/setting/EditWatchU i_80160Activity.java com/veepoo/hband/activity/connected/setting/WeatherSet tingActivity.java com/veepoo/hband/activity/desingguide/GuideScanListActi vity.java com/veepoo/hband/activity/desingguide/NotifySettingActiv
				ity.java com/veepoo/hband/activity/desingguide/PermissionActivit y.java com/veepoo/hband/activity/desingguide/ScanPermissionA ctivity.java com/veepoo/hband/activity/fragment/HomeFragment.java com/veepoo/hband/activity/gps/GoogleMapActivity.java com/veepoo/hband/activity/gps/util/UploadUtil.java com/veepoo/hband/activity/history/EcgGloassaryActivity.ja
				va com/veepoo/hband/activity/history/HRVHistoryNewActivit y.java com/veepoo/hband/activity/history/SleepV1HistroyActivity .java com/veepoo/hband/activity/music/MusicActivityDemo.java com/veepoo/hband/activity/setting/MessageSettingHelpAc tivity.java
				com/veepoo/hband/activity/setting/WhiteListHelpActivity.j ava com/veepoo/hband/adapter/BleScanViewAdapter.java com/veepoo/hband/adapter/CustomLogAdapter.java com/veepoo/hband/adapter/HistoryHRVBaseAdapter.java com/veepoo/hband/adapter/HistorySpo2hBaseAdapter.jav a
				com/veepoo/hband/adapter/PermissionCheckAdapter.java com/veepoo/hband/adapter/RecleViewBaseAdapter.java com/veepoo/hband/adapter/RecleViewBaseAdapterPWSett ing.java com/veepoo/hband/adapter/RecleViewBaseAdapterSetting. java com/veepoo/hband/adapter/WomanSettingAdapter.java
				com/veepoo/hband/ble/BleScanActivity.java com/veepoo/hband/ble/BluetoothService.java com/veepoo/hband/ble/bluetrum/dial/ZKImageConvertHel per.java com/veepoo/hband/ble/readmanager/multi_lead/ECGMult iLeadDetectHandler.java com/veepoo/hband/ble/send/BleDataSendManager.java com/veepoo/hband/httputil/GoogleFitSyncSessionTest.java

NO	ISSUE	SEVERITY	STANDARDS	com/veepoo/hband/j_l/dial/AbstractTestTask.java Fillt
				com/veepoo/hband/j_l/dial/fattask/FatFileTestTask.java com/veepoo/hband/j_l/ota/BLEScanner.java com/veepoo/hband/j_l/send/SendBleDataThread.java com/veepoo/hband/j_l/send/SendBleDataThread.java com/veepoo/hband/phone/CrashHandler.java com/veepoo/hband/sql/SqlHelperUtil.java com/veepoo/hband/util/ConnectTestManager.java com/veepoo/hband/util/FonnectTestManager.java com/veepoo/hband/util/FonnectTestManager.java com/veepoo/hband/util/FonnectTestManager.java com/veepoo/hband/util/FoSConverterUtils.java com/veepoo/hband/util/MDS.java com/veepoo/hband/util/MDS.java com/veepoo/hband/util/PictureSelectorManager.java com/veepoo/hband/util/PictureSelectorManager.java com/veepoo/hband/util/RepoCutUtil.java com/veepoo/hband/util/RepoCutUtil.java com/veepoo/hband/util/RepoCutUtil.go1.java com/veepoo/hband/viil/RepoCutUtil.go1.java com/veepoo/hband/viil/RepoCutUtilSDK.java com/veepoo/hband/view/EcgDeatectView.java com/veepoo/hband/view/EcgBeatctView.java com/veepoo/hband/view/EcgRepoCutView.java com/veepoo/hband/view/EcgRepoCutView.java com/veepoo/hband/view/EcgRepoCutView.java com/veepoo/hband/view/PrecisionSleepView.java com/veepoo/hband/view/ScgRepoView.java com/veepoo/hband/view/ScgNepOustomView.java com/veepoo/hband/view/ScgNepOustomView.java com/veepoo/hband/view/ScleepCustomView.java com/veepoo/hband/view/ScleepCustomView.java com/veepoo/hband/view/FrecisionSleepView.java com/veepoo/hba
				રશિર્મ/દુવામ(ત્રિક)મોદિરામાં/પ્રમીક/ર્સિક)ન્દ્રેમ્યુનેs/Chart.java રજમ્પુનુમાના પ્રત્યાદેક માર્ગાસ્થાના માના કર્યો કર્

OV	ISSUE	SEVERITY	STANDARDS	com/jieli/jl_bt_ota/util/FileUtil.java
				com/jieli/jl_rcsp/util/jl_l.og.java
				com/luck/picture/lib/manager/PictureCacheManager.java
				com/luck/picture/lib/utils/DownloadFileUtils.java
				com/luck/picture/lib/utils/FileDirMap.java
				com/luck/picture/lib/utils/MediaStoreUtils.java
				com/luck/picture/lib/utils/PictureFileUtils.java
				com/mob/tools/b/b.java
				com/nostra13/universalimageloader/utils/StorageUtils.java
				com/veepoo/hband/activity/connected/backdoor/ShowBac
				kActivity.java
				com/veepoo/hband/activity/connected/camera/ShowPictu
				reActivity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_172320_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_200320_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_228460_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_240240_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_240280_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_240284_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_240286_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_240292_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_240296_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_240Round_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_320380_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_320386_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_320Round_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				,
				iJL_360360_Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_360Round_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_368448_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_390450_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_390Round_Activity.java
				com/veepoo/hband/activity/connected/setting/EditWatchU
				iJL_410502_Activity.java

NO	ISSUE	SEVERITY	STANDARDS	com/veepoo/hband/activity/connected/setting/EditWatchU Fil_45SRound_Activity.java
2	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/veepoo/hband/activity/connected/setting/EditWatchU iJL_466Round_Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU iJL_46Round_Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU iJL_480Round_Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU iZK_172320_Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU iZK_200320_Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU iZK_240280_Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU iZK_240284_Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU iZK_240286_Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU iZK_320386_Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU iZK_360RoundActivity.java com/veepoo/hband/activity/connected/setting/EditWatchU iZK_360RoundActivity.java com/veepoo/hband/activity/connected/setting/EditWatchU iZK_368448_Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU iZK_410502_Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU i_15240Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU i_167240Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU i_167240Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU i_167240Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU i_1200320Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU i_240240Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU i_240280Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU i_240280Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU i_240280Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU i_240280Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU i_240280Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU i_240280Activity.java com/veepoo/hband/activity/connected/setting/EditWatchU i_240280Activity.jav

NO	ISSUE	SEVERITY	STANDARDS	com/veepoo/hband/activity/connected/setting/EditWatchU FB0E&0Activity.java com/veepoo/hband/activity/connected/setting/OrcodeBin
				dingActivity.java com/veepoo/hband/activity/setting/ProfileActivity.java com/veepoo/hband/activity/setting/WechatSportActivity.ja va com/veepoo/hband/activity/setting/WechatSportServiceAct ivity.java com/veepoo/hband/j_l/dial/AppUtil.java com/veepoo/hband/j_l/ota/JLOTAManager.java com/veepoo/hband/j_l/ota/JLOTAManager.java com/veepoo/hband/phone/CrashHandler.java com/veepoo/hband/util/FileUtilQ.java com/veepoo/hband/util/FileUtilQ.java com/veepoo/hband/util/HBFileSystem.java com/veepoo/hband/util/PickPhotoUtil.java com/veepoo/hband/util/PictureSelectorManager.java com/veepoo/hband/util/PictureSelectorManager.java com/veepoo/hband/util/PictureSelectorManager.java com/veepoo/hband/util/RealPathUtil.java com/veepoo/hband/util/Iog/HBLogger.java com/yalantis/ucrop/util/FileUtils.java solid/ren/skinlibrary/utils/SkinFileUtils.java
				top/zibin/luban/LubanUtils.java com/huawei/agconnect/core/BuildConfig.java com/huawei/hms/feature/dynamic/a.java com/huawei/hms/framework/common/BuildConfig.java com/huawei/hms/framework/common/PackageManagerC ompat.java com/huawei/hms/framework/common/hianalytics/Hianaly ticsHelper.java com/huawei/hms/framework/network/frameworkcompat/BuildConfig.java com/huawei/hms/framework/network/grs/BuildConfig.java com/huawei/hms/framework/network/grs/BuildConfig.java a com/huawei/hms/framework/network/grs/g/j/a.java com/huawei/hms/framework/network/grs/h/a.java com/huawei/hms/hatool/m0.java com/huawei/hms/hatool/u0.java com/huawei/hms/hatool/y0.java com/huawei/hms/hmsscankit/g.java com/huawei/hms/mlkit/agc/BuildConfig.java com/huawei/hms/mlkit/agc/BuildConfig.java com/huawei/hms/scankit/c.java com/huawei/hms/scankit/p/m1.java com/huawei/hms/scankit/p/u3.java com/huawei/hms/scankit/p/u3.java com/huawei/hms/scankit/p/u3.java com/huawei/hms/scankit/p/u3.java com/huawei/secure/android/common/encrypt/a.java com/huawei/secure/android/common/encrypt/a.java com/huawei/secure/android/common/ssl/a.java
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/huawei/secure/android/common/ssl/util/BksUtil.java com/huawei/secure/android/common/util/e.java com/mob/commons/i.java com/mob/tools/b/i.java

NO	ISSUE	SEVERITY	STANDARDS	com/mob/tools/b/j.java Filh
				.java com/veepoo/hband/activity/connected/Biet Onnectsuccess .java com/veepoo/hband/activity/connected/backdoor/SportMo deTestUtil.java com/veepoo/hband/activity/connected/oad/BluetrumOTA Activity.java com/veepoo/hband/activity/connected/oad/JLOTAActivity.j ava com/veepoo/hband/activity/connected/oad/OadNoricActiv ity.java com/veepoo/hband/activity/connected/setting/ServerDialN ewActivity.java com/veepoo/hband/activity/connected/setting/ServerJLDia lNewActivity.java com/veepoo/hband/activity/connected/setting/UpdateJLW atchUiActivity.java com/veepoo/hband/activity/connected/setting/UpdateWat chUiActivity.java com/veepoo/hband/activity/connected/setting/UpdateWat chUiActivity.java com/veepoo/hband/ble/BluetoothService.java com/veepoo/hband/ble/BluetoothService.java com/veepoo/hband/ble/readmanager/BatterManagerHand ler.java com/veepoo/hband/util/AfterGetDeviceNumber.java
4	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/jieli/jl_bt_ota/tool/SnGenerator.java com/jieli/jl_rcsp/tool/SnGenerator.java com/mob/tools/utils/MobPersistence.java com/veepoo/hband/activity/fragment/HomeFragment.java com/veepoo/hband/activity/history/BloodCompositionHist oryActivity.java com/veepoo/hband/activity/history/RateHistoryActivity.jav a com/veepoo/hband/ble/bluetrum/dial/VPRGBQuadCluster. java com/veepoo/hband/j_l/dial/fattask/FatFileTestTask.java com/veepoo/hband/sql/SqlHelperUtil.java com/veepoo/hband/view/LorenzChartView.java com/veepoo/hband/view/LorenzChartView.java com/veepoo/hband/view/MarqueeText.java com/veepoo/hband/view/MarqueeText.java
5	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	cat/ereza/customactivityoncrash/activity/DefaultErrorActivi ty.java
6	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/nostra13/universalimageloader/BuildConfig.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/manager/RequestManagerRetriever.j ava com/chauthai/swipereveallayout/ViewBinderHelper.java com/chauthai/swipereveallayout/ViewBinderHelper.java com/huawei/hms/framework/common/hianalytics/Hianaly ticsBaseData.java com/huawei/hms/mlsdk/common/AgConnectInfo.java com/jieli/jl_bt_ota/model/response/TargetInfoResponse.java a com/jieli/jl_rcsp/model/response/TargetInfoResponse.java com/jieli/jl_rcsp/model/response/TargetInfoResponse.java com/jieli/jl_rcsp/tool/SyncMessageTask.java com/luck/picture/lib/config/PictureConfig.java com/veepoo/hband/activity/MainActivity.java com/veepoo/hband/activity/connected/setting/AGPSSettin gActivity.java com/veepoo/hband/activity/connected/setting/ScreenStyle JLActivity.java com/veepoo/hband/activity/history/HRVHistoryActivity.java a com/veepoo/hband/activity/history/HRVHistoryNewActivit y.java com/veepoo/hband/activity/history/HRVHistoryNewActivit y.java com/veepoo/hband/activity/history/HRVHistoryNewActivit y.java com/veepoo/hband/httputil/HttpUtil.java com/veepoo/hband/httputil/HttpUtil.java com/veepoo/hband/httputil/HttpUtil.java com/veepoo/hband/httputil/HttpUtil.java com/veepoo/hband/modle/UserBean.java com/veepoo/hband/modle/UserBean.java no/nordicsemi/android/log/LogContract.java rx/internal/schedulers/NewThreadWorker.java
8	Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	com/huawei/secure/android/common/webview/SafeWebV iew.java
9	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/huawei/secure/android/common/ssl/SecureX509Trus tManager.java com/mob/tools/network/NetworkHelper.java com/veepoo/hband/adapter/AuthImageDownloader.java com/veepoo/hband/httputil/CHttpUtilCommon.java com/veepoo/hband/httputil/HttpGoogleUtil.java com/veepoo/hband/httputil/HttpUtil.java com/veepoo/hband/httputil/HttpUtill.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/nanchen/compresshelper/FileUtil.java
11	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/huawei/agconnect/config/impl/i.java
12	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/huawei/agconnect/config/impl/i.java com/huawei/secure/android/common/encrypt/utils/Encry ptUtil.java com/huawei/secure/android/common/util/EncryptUtil.java
13	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	solid/ren/skinlibrary/utils/SkinPreferencesUtils.java
14	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	cn/smssdk/net/login/e.java com/bluetrum/fota/manager/OtaDataProvider.java com/luck/picture/lib/loader/SandboxFileLoader.java com/qweather/sdk/c/e.java com/veepoo/hband/util/MD5.java
15	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/activeandroid/ActiveAndroid.java com/activeandroid/DatabaseHelper.java com/huawei/hms/framework/common/NetworkKitSQLite OpenHelper.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/libjl_pack_format.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: ['_vsnprintf_chk', '_strlen_chk', '_memmove_chk']	True info Symbols are stripped.
2	arm64-v8a/libjl_ota_auth.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 readonly.	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: ['_strlen_chk', '_memcpy_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	arm64-v8a/libjl_bmp_convert.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 readonly.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
8	arm64-v8a/libabpartool.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: ['_memmove_chk', '_strlen_chk', '_vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	arm64-v8a/libjl_fatfs.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: ['vsnprintf_chk', 'strlen_chk', 'memmove_chk', 'vsprintf_chk']	True info Symbols are stripped.
10	arm64-v8a/libJni_wgs2gcj.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/libscannative.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: ['_memmove_chk', '_memset_chk', '_fgets_chk']	True info Symbols are stripped.
12	arm64-v8a/libjl_auth.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
13	arm64-v8a/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
14	x86_64/libjl_pack_format.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: ['vsnprintf_chk', 'strlen_chk', 'memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	x86_64/libjl_ota_auth.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: ['_strlen_chk', '_memcpy_chk']	True info Symbols are stripped.
16	x86_64/libnative-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as readonly.	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', '_memmove_chk', '_strlen_chk', '_memcpy_chk', '_memmove_chk', '_memmove_chk', '_strlen_chk', '_strlen_chk', '_vsnprintf_chk']	False warning Symbols are available.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	x86_64/libJni_wgs2gcj.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 readonly.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
24	x86_64/libjl_auth.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 readonly.	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
25	x86_64/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
26	armeabi-v7a/libjl_pack_format.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/libjl_ota_auth.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: ['strlen_chk']	True info Symbols are stripped.
28	armeabi-v7a/libnative-lib.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	armeabi-v7a/libapssdk.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.
30	armeabi-v7a/libluoentz.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 readonly.	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	armeabi-v7a/libjl_crc.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.
32	armeabi-v7a/libjl_bmp_convert.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	armeabi-v7a/libjl_fatfs.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: ['strlen_chk', 'vsprintf_chk']	True info Symbols are stripped.
34	armeabi-v7a/libJni_wgs2gcj.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	armeabi-v7a/libscannative.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: ['fgets_chk', 'memset_chk']	True info Symbols are stripped.
36	armeabi-v7a/libjl_auth.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 readonly.	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	armeabi-v7a/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
38	armeabi/libapssdk.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	armeabi/libJni_wgs2gcj.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.
40	armeabi/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
41	x86/libjl_pack_format.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.
42	x86/libjl_ota_auth.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: ['strlen_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
49	x86/libJni_wgs2gcj.so	True info The binary has NX bit set. This marks a memory page nonexecutable making attacker injected shellcode nonexecutable.	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.
50	x86/libjl_auth.so	True info The binary has NX bit set. This marks a memory page nonexecutable making attacker injected shellcode nonexecutable.	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/libpl_droidsonroids_gif.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 readonly.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
52	mips/libpl_droidsonroids_gif.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 readonly.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
53	mips64/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
54	arm64-v8a/libjl_pack_format.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: ['vsnprintf_chk', 'strlen_chk', 'memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
55	arm64-v8a/libjl_ota_auth.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: ['strlen_chk', 'memcpy_chk']	True info Symbols are stripped.
56	arm64-v8a/libnative-lib.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as readonly.	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: ['_vsnprintf_chk', '_strlen_chk', '_memcpy_chk', '_memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
57	arm64-v8a/libapssdk.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.
58	arm64-v8a/libluoentz.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	arm64-v8a/libjl_crc.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.
60	arm64-v8a/libjl_bmp_convert.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	arm64-v8a/libabpartool.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: ['_memmove_chk', '_strlen_chk', '_vsnprintf_chk']	True info Symbols are stripped.
62	arm64-v8a/libjl_fatfs.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 readonly.	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: ['_vsnprintf_chk', '_strlen_chk', '_memmove_chk', '_vsprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
63	arm64-v8a/lib]ni_wgs2gcj.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.
64	arm64-v8a/libscannative.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: ['_memmove_chk', '_memset_chk', '_fgets_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
65	arm64-v8a/libjl_auth.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.
66	arm64-v8a/libpl_droidsonroids_gif.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 readonly.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
67	x86_64/libjl_pack_format.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: ['_vsnprintf_chk', '_strlen_chk', '_memmove_chk']	True info Symbols are stripped.
68	x86_64/libjl_ota_auth.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 readonly.	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: ['_strlen_chk', '_memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
69	x86_64/libnative-lib.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['memcpy_chk', 'strlen_chk', 'vsnprintf_chk', 'memcpy_chk', 'memmove_chk', '_strlen_chk', 'strlen_chk', 'strlen_chk', 'strlen_chk',	False warning Symbols are available.
70	x86_64/libapssdk.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 readonly.	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_64/libluoentz.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.
72	x86_64/libjl_crc.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_64/libjl_bmp_convert.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.
74	x86_64/libabpartool.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 readonly.	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: ['_memmove_chk', '_strlen_chk', '_vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
75	x86_64/libjl_fatfs.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: ['strlen_chk', 'vsprintf_chk', 'memmove_chk', 'vsnprintf_chk']	True info Symbols are stripped.
76	x86_64/libJni_wgs2gcj.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 readonly.	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
77	x86_64/libjl_auth.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.
78	x86_64/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
79	armeabi-v7a/libjl_pack_format.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 readonly.	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.
80	armeabi-v7a/libjl_ota_auth.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: ['strlen_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
87	armeabi-v7a/libJni_wgs2gcj.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.
88	armeabi-v7a/libscannative.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: ['fgets_chk', 'memset_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
91	armeabi/libapssdk.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.
92	armeabi/libJni_wgs2gcj.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
93	armeabi/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
94	x86/libjl_pack_format.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
95	x86/libjl_ota_auth.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: ['strlen_chk']	True info Symbols are stripped.
96	x86/libnative-lib.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
97	x86/libapssdk.so	True info The binary has NX bit set. This marks a memory page nonexecutable making attacker injected shellcode nonexecutable.	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 readonly.	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.
98	x86/libluoentz.so	True info The binary has NX bit set. This marks a memory page nonexecutable making attacker injected shellcode nonexecutable.	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 readonly.	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
99	x86/libjl_crc.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 readonly.	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.
100	x86/libjl_bmp_convert.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 readonly.	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
101	x86/libjl_fatfs.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 readonly.	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: ['strlen_chk', 'vsprintf_chk']	True info Symbols are stripped.
102	x86/libJni_wgs2gcj.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 readonly.	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
103	x86/libjl_auth.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.
104	x86/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
105	mips/libpl_droidsonroids_gif.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 readonly.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.
106	mips64/libpl_droidsonroids_gif.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read- only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

■ NIAP ANALYSIS v1.3

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
			com/goodix/ble/gr/libdfu/task/DeviceFirmwareUpdate.java com/goodix/ble/gr/libdfu/task/DeviceFirmwareUpdate.java com/goodix/ble/gr/libdfu/task/DeviceRirmwareUpdate.java com/goodix/ble/libcomx/file/Fileditj.java com/goodix/ble/libcomx/file/Fileditj.java com/goodix/ble/libcomx/file/Fileditj.java com/goodix/ble/libcomx/file/Fileditj.java com/goodix/ble/libcomx/file/Fileditj.java com/lock/bje/libcomx/file/Fileditj.java com/lock/bje/titure/lib/astic/PictureCommonFragment.java com/luck/picture/lib/astic/PictureCommonFragment.java com/luck/picture/lib/anagger/PictureCacheManager.java com/luck/picture/lib/anagger/PictureCacheManager.java com/luck/picture/lib/astic/Media/StoreUtils.java com/luck/picture/lib/utils/Media/StoreUtils.java com/luck/picture/lib/utils/Media/StoreUtils.java com/luck/picture/lib/utils/Media/Utils.java com/luck/picture/lib/utils/Media/Utils.java com/luck/picture/lib/utils/Media/Utils.java com/mob/commons/a/c.java com/mob/commons/a/c.java com/mob/commons/a/c.java com/mob/commons/c.java com/mob/commons/c.java com/mob/commons/c.java com/mob/commons/p.java com/mob/commons/p.java com/mob/commons/p.java com/mob/commons/p.java com/mob/tools/b/d.java com/mob/tools/b/d.ja
			com/veepoo/hband/activity/connected/setting/EditWatchUiJL_240296_Activity.java com/veepoo/hband/activity/connected/setting/EditWatchUiJL_240Round_Activity.java

			com/veepoo/hband/activity/connected/setting/EditWatchUiJL_320380_Activity.java
RULE ID	BEHAVIOUR	LABEL	File Seepoo/hband/activity/connected/setting/EditWatchUiJL_320386_Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUilL_320Round_Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUiJL_360360_Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUiJL_360Round_Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUiJL_368448_Activity.java
00022	Open a file from given absolute path of the file	file	com/veepoo/hband/activity/connected/setting/EditWatchUiJL_390450_Activity.java
00022	open a me nom given absolute path of the me	THE STATE OF THE S	com/veepoo/hband/activity/connected/setting/EditWatchUiJL_390Round_Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUiJL_410502_Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUiJL_412Round_Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUiJL_416Round_Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUiJL_466Round_Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUiJL_480Round_Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUiZK_172320_Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUiZK_200320_Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUiZK_240280_Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUiZK_240284_Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUiZK_240296_Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUiZK_240296_Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUiZK_320386_Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUiZK_360R6UnidActivity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUiZK_300446_Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUiZK_41030Z_Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUi_135240Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUi_167240Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUi_172320Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUi_200320Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUi_240240Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUi_240280Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUi_240284Activity.java com/veepoo/hband/activity/connected/setting/EditWatchUi_240286Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUi_240295Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUi_240RoundActivity.java com/veepoo/hband/activity/connected/setting/EditWatchUi_320380Activity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUi_320380Activity.java com/veepoo/hband/activity/connected/setting/EditWatchUi_360RoundActivity.java
			com/veepoo/hband/activity/connected/setting/EditWatchUi_80160Activity.java com/veepoo/hband/activity/connected/setting/QrcodeBindingActivity.java
			com/veepoo/hband/activity/connected/setting/QrcodebindingActivity.java com/veepoo/hband/activity/connected/setting/ServerJLDialNewActivity.java
			com/veepoo/hband/activity/connected/setting/serverJLHistoryDialActivity.java
			com/veepoo/hband/activity/connected/setting/serverjEnistoryDialActivity.java
			com/veepoo/hband/activity/setting/ProfileActivity.java
			com/veepoo/hband/activity/setting/FronteActivity.java com/veepoo/hband/activity/setting/WechatSportActivity.java
			com/veepoo/hband/activity/setting/WechatSportServiceActivity.java com/veepoo/hband/ble/JLWatchFaceManager.java
			com/veepoo/hband/util/CropPhotoUtils.java
			' '
			com/veepoo/hband/util/FileUtilQ.java
			com/veepoo/hband/util/HBFileSystem.java
			com/veepoo/hband/util/ImageUtil.java
			com/veepoo/hband/util/PdfUtils.java
			com/veepoo/hband/util/PictureSelectorManager.java
			com/veepoo/hband/util/PngToBmpUtil.java
			com/veepoo/nband/util/RepoCutUtil.java
			com/veepoo/hband/util/RepoCutUtil.java

RULE ID	BEHAVIOUR	LABEL	com/veepoo/hband/util/RepoCutUtilG01.java Ghtseepoo/hband/util/ShareUtil.java com/veepoo/hband/util/log/HBLogger.java
			com/yalantis/ucrop/UCropMultipleActivity.java pl/droidsonroids/gif/ReLinker.java solid/ren/skinlibrary/utils/SkinFileUtils.java top/zibin/luban/Luban.java

RULE ID	BEHAVIOUR	LABEL	FILES
00054	Install other APKs from file	reflection	com/veepoo/hband/activity/connected/setting/EditWatchUijL_172320_Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_200320_Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_24024_Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_240280_Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_240286_Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_240286_Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_240286_Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_240286_Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_240286_Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_240286_Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_240286_Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_32080_Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_32080_Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_30800_Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_3080Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_3080Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_3080Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_3080Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_3080Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_4080Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_4080Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_4080Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_4080Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_4080Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_4080Activity_java com/veepoo/hband/activity/connected/setting/EditWatchUijL_4080Activity_java com/veepoo/hband/activity/connec

JLE ID BEHAVIOUR	LABEL	For Rarumi/dexter/listener/SettingsClickListener.java
Implicit intent(view a web page, make a phone call, etc.)	control	com/huawel/hms/scankit/p/w7, java Eth-Khrumi/dexter/listener/SettingsClickListener.java com/mob/commons/b/i,java com/mob/commons/b/i,java com/weepoo/hband/activity/connected/cabckdoor/ShowBackActivity.java com/weepoo/hband/activity/connected/cameral/cameralnterface.java com/weepoo/hband/activity/connected/cameral/cameralnterface.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_172320_Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_172320_Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_2200320_Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_2200320_Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_240284_Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_240284_Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_240284_Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_240284_Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_240284_Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_240284_Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_240284_Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_230380_Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_320380_Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_320380_Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_320380_Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_36080_Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_36080_Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_36080_Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_36080_Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_412800.Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_42080_Activity.java com/weepoo/hband/activity/connected/setting/EditWatchUjl_440800.Activity.ja

RULE ID	BEHAVIOUR	LABEL	com/veepoo/hband/activity/connected/setting/EditWatchUi_320380Activity.java Ghtseepoo/hband/activity/connected/setting/EditWatchUi_360RoundActivity.java com/veepoo/hband/activity/connected/setting/EditWatchUi_80160Activity.java
			com/veepoo/hband/activity/desingguide/NotifySettingActivity.java com/veepoo/hband/activity/desingguide/PermissionActivity.java com/veepoo/hband/activity/fragment/SettingFragment.java com/veepoo/hband/activity/setting/PermissionCheckActivity.java com/veepoo/hband/activity/setting/ProfileActivity.java com/veepoo/hband/ble/BluetoothService.java com/veepoo/hband/util/AutoStartSettingUtil.java com/veepoo/hband/util/BadgeUtil.java com/veepoo/hband/util/FileUtilQ.java com/veepoo/hband/util/PictureSelectorManager.java com/veepoo/hband/util/SmsUtil.java com/veepoo/hband/util/SmsUtil.java com/veepoo/hband/util/SmsUtil.java com/veepoo/hband/util/SmsUtil.java com/veepoo/hband/util/SmsUtil.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_172320_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_172320_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_240240_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_240240_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_240240_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_240240_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_240240_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_240286_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_24029_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_240280_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_320380_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_320380_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_32080und_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_32080und_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_36080_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_36080_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_36080_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_36080_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_30080_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_30080_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_30080_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_30080_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_30080_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_30080_Activity.java com/veepoo/hband/activity/connected/setting/Edit/WatchUijL_30080_Activity.java com/veepoo/hband/activity/connected/setting/Edit/Watch

RULE ID	BEHAVIOUR	LABEL	com/veepoo/hband/util/AutoStartSettingUtil.java FILES
NOLL ID	DEI I/ WIGGIN	D (DLL	
00191	Get messages in the SMS inbox	sms	com/huawei/hms/scankit/p/w7.java com/luck/picture/lib/utils/MediaUtils.java com/mob/commons/b/i.java com/mob/commons/b/p.java com/mob/tools/utils/ResHelper.java com/veepoo/hband/util/SmsUtil.java
			com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/goodix/ble/gr/libdfu/task/DeviceFirmwareUpdate.java com/goodix/ble/gr/libdfu/task/DeviceResourceUpdate.java com/goodix/ble/gr/libdfu/task/DeviceResourceUpdate.java com/goodix/ble/gr/libdfu/task/DeviceResourceUpdate.java com/huawei/ble/libcomx/file/FileUtil.java com/huawei/hms/framework/common/CreateFileUtil.java com/huawei/secure/android/common/encrypt/hash/FileSHA256.java com/huawei/secure/android/common/ssl/util/BksUtil.java com/huawei/secure/android/common/ssl/util/BksUtil.java com/huawei/secure/android/common/util/ZipUtil.java com/jieli/jl_bt_ota/util/FileUtil.java com/jieli/jl_bt_ota/util/FileUtil.java com/jieli/jl_fatfs/tool/ReadFileThread.java com/jieli/jl_fatfs/tool/ReadFileThread.java com/jieli/jl_rtsfx/task/contacts/ReadContactsTask.java com/jieli/jl_rcsp/task/contacts/ReadContactsTask.java com/jieli/jl_rcsp/task/contacts/ReadContactsTask.java com/jieli/jl_rcsp/task/contacts/ReadContactsTask.java com/luck/picture/lib/utils/DownloadFileUtils.java com/luck/picture/lib/utils/MediaUtils.java com/luck/picture/lib/utils/MediaUtils.java com/luck/picture/lib/utils/SandboxTransformUtils.java com/luck/picture/lib/utils/SandboxTransformUtils.java com/mob/commons/ccjava com/mob/commons/cc/x.java com/mob/commons/cc/x.java com/mob/commons/eventrecoder/EventRecorder.java com/mob/commons/eventrecoder/EventRecorder.java com/mob/cols/b/b.java
00013	Read file and put it into a stream	file	com/mob/tools/b/j.java com/mob/tools/network/FilePart.java com/mob/tools/network/NetworkHelper.java com/mob/tools/utils/BitmapHelper.java com/mob/tools/utils/Data.java com/mob/tools/utils/FileUtils.java com/mob/tools/utils/FileUtils.java com/mob/tools/utils/ResHelper.java com/mob/tools/utils/SharePrefrenceHelper.java com/nanchen/compresshelper/BitmapUtil.java com/nostra13/universalimageloader/core/download/BaseImageDownloader.java com/veepoo/hband/activity/connected/backdoor/ShowBackActivity.java com/veepoo/hband/activity/connected/oad/BluetrumOTAActivity.java com/veepoo/hband/activity/connected/oad/OadNoricActivity.java com/veepoo/hband/activity/connected/oad/OadNoricActivity.java

RULE ID	BEHAVIOUR	LABEL	com/veepoo/hband/ble/readmanager/AGPSManager.java 日比亞全poo/hband/ble/readmanager/HuitopUIUpdateHandler.java
			com/veepoo/hband/ble/readmanager/UIUpdateHandler.java com/veepoo/hband/phone/CrashHandler.java com/veepoo/hband/util/FileUtilQ.java com/veepoo/hband/util/ImageUtils.java com/veepoo/hband/util/MD5.java com/veepoo/hband/util/PngToBmpUtil.java com/veepoo/hband/util/SystemInfoUtils.java com/veepoo/hband/util/SystemInfoUtils.java com/veepoo/hband/util/Jog/HBLogger.java com/veepoo/hband/util/FileUtils.java javax/mail/Session.java net/sourceforge/pinyin4j/multipinyin/Trie.java no/nordicsemi/android/dfu/DfuBaseService.java okio/Okio.java top/zibin/luban/io/ArrayPoolProvide.java
00012	Read data and put it into a buffer stream	file	com/huawei/secure/android/common/util/ZipUtil.java com/luck/picture/lib/utils/PictureFileUtils.java com/mob/commons/cc/x.java com/mob/commons/cc/y.java com/mob/tools/utils/FileUtils.java com/nostra13/universalimageloader/core/download/BaseImageDownloader.java com/veepoo/hband/util/log/HBLogger.java com/yalantis/ucrop/util/FileUtils.java javax/mail/Session.java
00189	Get the content of a SMS message	sms	com/veepoo/hband/j_l/music/MusicLoader.java com/veepoo/hband/util/CropPhotoUtils.java com/veepoo/hband/util/SmsUtil.java
00188	Get the address of a SMS message	sms	com/veepoo/hband/j_l/music/MusicLoader.java com/veepoo/hband/util/CropPhotoUtils.java com/veepoo/hband/util/SmsUtil.java
00200	Query data from the contact list	collection contact	com/veepoo/hband/j_l/music/MusicLoader.java com/veepoo/hband/util/CropPhotoUtils.java com/veepoo/hband/util/SmsUtil.java
00187	Query a URI and check the result	collection sms calllog calendar	com/veepoo/hband/j_l/music/MusicLoader.java com/veepoo/hband/util/SmsUtil.java
00201	Query data from the call log	collection calllog	com/veepoo/hband/j_l/music/MusicLoader.java com/veepoo/hband/util/CropPhotoUtils.java com/veepoo/hband/util/SmsUtil.java

RULE ID	BEHAVIOUR	LABEL	FILES
00192	Get messages in the SMS inbox	sms	com/luck/picture/lib/loader/LocalMediaPageLoader.java com/luck/picture/lib/utils/PictureFileUtils.java com/veepoo/hband/util/PickPhotoUtil.java com/veepoo/hband/util/RealPathUtil.java com/yalantis/ucrop/util/FileUtils.java top/zibin/luban/LubanUtils.java
00092	Send broadcast	command	com/veepoo/hband/activity/MainActivity.java com/veepoo/hband/activity/binderbluetooth3/BindBluetooth3.java com/veepoo/hband/activity/connected/setting/PersonWatchSettingActivity.java com/veepoo/hband/activity/desingguide/NotifySettingActivity.java com/veepoo/hband/activity/fragment/FitSportFragment.java com/veepoo/hband/activity/fragment/HomeFragment.java com/veepoo/hband/activity/setting/LowSpo2hRemindActivity.java com/veepoo/hband/ble/BleScanActivity.java com/veepoo/hband/ble/BleScanActivity.java
00193	Send a SMS message	sms	com/veepoo/hband/activity/connected/backdoor/SendSMSActivity.java com/veepoo/hband/activity/connected/backdoor/ShowBackActivity.java
00036	Get resource file from res/raw directory	reflection	com/huawei/hms/scankit/p/w7.java com/karumi/dexter/listener/SettingsClickListener.java com/luck/picture/lib/utils/PictureFileUtils.java com/mob/commons/b/i.java com/mob/tools/utils/ResHelper.java com/veepoo/hband/activity/binderbluetooth3/BindBluetooth3.java com/veepoo/hband/activity/connected/backdoor/ShowBackActivity.java com/veepoo/hband/activity/desingguide/NotifySettingActivity.java com/veepoo/hband/activity/desingguide/PermissionActivity.java com/veepoo/hband/activity/setting/PermissionCheckActivity.java com/veepoo/hband/ble/BluetoothService.java com/veepoo/hband/ble/BluetoothService.java
00183	Get current camera parameters and change the setting.	camera	com/huawei/hms/scankit/p/f0.java com/huawei/hms/scankit/p/h0.java com/huawei/hms/scankit/p/i0.java com/huawei/hms/scankit/p/j0.java com/huawei/hms/scankit/p/j0.java com/huawei/hms/scankit/p/l0.java com/huawei/hms/scankit/p/n0.java com/huawei/hms/scankit/p/n0.java com/veepoo/hband/activity/connected/camera/CameraInterface.java
00130	Get the current WIFI information	wifi collection	com/qweather/sdk/c/a.java com/veepoo/hband/util/NetworkUtil.java
00033	Query the IMEI number	collection	com/qweather/sdk/c/a.java com/veepoo/hband/util/SystemUtil.java

RULE ID	BEHAVIOUR	LABEL	FILES
00065	Get the country code of the SIM card provider	collection	com/huawei/hms/framework/network/grs/local/model/CountryCodeBean.java com/huawei/hms/ml/common/utils/CountryCodeBean.java com/huawei/hms/scankit/p/u3.java com/qweather/sdk/c/a.java
00066	Query the ICCID number	collection	com/qweather/sdk/c/a.java
00067	Query the IMSI number	collection	com/qweather/sdk/c/a.java
00015	Put buffer stream (data) to JSON object	file	com/mob/commons/cc/y.java
00014	Read file into a stream and put it into a JSON object	file	com/mob/commons/ac.java com/mob/commons/cc/y.java
00004	Get filename and put it to JSON object	file collection	com/mob/commons/cc/y.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/huawei/hms/hatool/w.java com/mob/tools/network/NetworkHelper.java com/nostra13/universalimageloader/core/download/BaseImageDownloader.java com/veepoo/hband/activity/gps/util/UploadUtil.java com/veepoo/hband/adapter/AuthImageDownloader.java
00112	Get the date of the calendar event	collection calendar	com/mob/tools/utils/ResHelper.java com/veepoo/hband/util/TimeUtils.java
00132	Query The ISO country code	telephony collection	com/huawei/hms/framework/network/grs/local/model/CountryCodeBean.java com/huawei/hms/ml/common/utils/CountryCodeBean.java com/huawei/hms/scankit/p/u3.java
00177	Check if permission is granted and request it	permission	com/huawei/hms/hmsscankit/RemoteView.java com/huawei/hms/scankit/b.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/mob/tools/utils/BitmapHelper.java
00072	Write HTTP input stream into a file	command network file	com/huawei/hms/hatool/k1.java com/mob/tools/network/NetworkHelper.java
00108	Read the input stream from given URL	network command	com/huawei/hms/hatool/k1.java com/mob/tools/network/NetworkHelper.java com/veepoo/hband/activity/gps/util/UploadUtil.java

RULE ID	BEHAVIOUR	LABEL	FILES
00121	Create a directory file command		com/huawei/hms/feature/dynamic/ModuleCopy.java com/yalantis/ucrop/UCropMultipleActivity.java top/zibin/luban/Luban.java
00125	Check if the given file path exist	file	com/huawei/hms/feature/dynamic/DynamicModule.java com/huawei/hms/feature/dynamic/ModuleCopy.java com/veepoo/hband/activity/connected/oad/OadNoricActivity.java com/veepoo/hband/activity/fragment/SettingFragment.java com/yalantis/ucrop/UCropMultipleActivity.java top/zibin/luban/Luban.java
00104	Check if the given path is directory	file	com/huawei/hms/feature/dynamic/ModuleCopy.java top/zibin/luban/Luban.java
00056	Modify voice volume	control	com/veepoo/hband/activity/music/MusicActivityDemo.java com/veepoo/hband/util/VolumeController.java
00034	Query the current data network type	collection network	com/huawei/hms/scankit/p/b4.java
00055	Query the SMS content and the source of the phone number	sms collection	com/veepoo/hband/phone/PhoneStatReceiver.java
00091	Retrieve data from broadcast	collection	com/veepoo/hband/phone/PhoneStatReceiver.java com/yalantis/ucrop/UCropMultipleActivity.java
00048	Query the SMS contents	sms collection	com/veepoo/hband/phone/PhoneStatReceiver.java
00064	Monitor incoming call status	control	com/veepoo/hband/phone/PhoneStatReceiver.java
00049	Query the phone number from SMS sender	sms collection	com/veepoo/hband/phone/PhoneStatReceiver.java
00088	Create a secure socket connection to the given host address	command network	com/huawei/secure/android/common/SecureSSLSocketFactory.java com/huawei/secure/android/common/ssl/SSFCompatiableSystemCA.java com/huawei/secure/android/common/ssl/SecureSSLSocketFactory.java com/huawei/secure/android/common/ssl/SecureSSLSocketFactoryNew.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java com/huawei/hms/hatool/w.java com/mob/tools/network/NetworkHelper.java com/nostra13/universalimageloader/core/download/BaseImageDownloader.java com/veepoo/hband/activity/gps/util/UploadUtil.java

RULE ID	BEHAVIOUR	LABEL	FILES
00024	Write file after Base64 decoding reflection file		com/mob/tools/a/b.java com/mob/tools/utils/ResHelper.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/veepoo/hband/util/CropPhotoUtils.java com/veepoo/hband/util/SmsUtil.java
00096	Connect to a URL and set request method	command network	com/huawei/hms/hatool/w.java com/mob/tools/network/NetworkHelper.java com/veepoo/hband/activity/gps/util/UploadUtil.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/mob/tools/network/NetworkHelper.java
00153	Send binary data over HTTP	http	com/mob/tools/network/NetworkHelper.java com/veepoo/hband/activity/gps/util/UploadUtil.java
00094	Connect to a URL and read data from it	command network	com/mob/tools/network/NetworkHelper.java com/veepoo/hband/activity/gps/util/UploadUtil.java
00071	Write the ISO country code of the current network operator into a file	collection command network file	com/veepoo/hband/activity/connected/setting/AGPSSettingActivity.java
00031	Check the list of currently running applications	reflection collection	com/veepoo/hband/HBandApplication.java
00005	Get absolute path of file and put it to JSON object	file	com/luck/picture/lib/basic/PictureCommonFragment.java com/yalantis/ucrop/UCropMultipleActivity.java
00043	Calculate WiFi signal strength	collection wifi	com/huawei/hms/framework/common/NetworkUtil.java
00002	Open the camera and take picture	camera	com/veepoo/hband/activity/connected/camera/CameraInterface.java
00053	Monitor data identified by a given content URI changes(SMS, MMS, etc.)	sms	com/veepoo/hband/util/SmsUtil.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/veepoo/hband/util/SmsUtil.java
00163	Create new Socket and connecting to it	socket	com/mob/mcl/c/f.java

******* ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	16/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.VIBRATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_WIFI_STATE, android.permission.CAMERA, android.permission.WAKE_LOCK, android.permission.GET_ACCOUNTS, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.SYSTEM_ALERT_WINDOW, android.permission.READ_CONTACTS, android.permission.READ_PHONE_STATE, android.permission.READ_CALL_LOG, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION
Other Common Permissions	13/44	android.permission.MODIFY_AUDIO_SETTINGS, android.permission.FOREGROUND_SERVICE, android.permission.ACCESS_NOTIFICATION_POLICY, android.permission.CHANGE_WIFI_STATE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.WRITE_CONTACTS, android.permission.CALL_PHONE, android.permission.PROCESS_OUTGOING_CALLS, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.ACCESS_LOCATION_EXTRA_COMMANDS, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.BROADCAST_STICKY

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.vphband.com	IP: 120.79.208.77 Country: China Region: Zhejiang City: Hangzhou
120.79.208.77	IP: 120.79.208.77 Country: China Region: Zhejiang City: Hangzhou
www.umeng.com	IP: 59.82.60.43 Country: China Region: Zhejiang City: Hangzhou
www.mob.com	IP: 180.188.26.28 Country: China Region: Zhejiang City: Taizhou

DOMAIN	COUNTRY/REGION
domain-publish-devapi.qweather.net	IP: 123.56.216.251 Country: China Region: Zhejiang City: Hangzhou
devapi-413-aa3b3.qweather.net	IP: 123.56.216.251 Country: China Region: Zhejiang City: Hangzhou
auth-413-aa3b3.qweather.net	IP: 47.95.178.71 Country: China Region: Zhejiang City: Hangzhou
u.wechat.com	IP: 43.159.94.110 Country: China Region: Beijing City: Beijing
i.qianbao.qq.com	IP: 122.188.45.140 Country: China Region: Hubei City: Jingmen
identify.verify.mob.com	IP: 47.243.26.137 Country: Hong Kong Region: Hong Kong City: Hong Kong
qr.alipay.com	IP: 110.76.30.76 Country: China Region: Zhejiang City: Hangzhou
datasetapi-413-aa3b3.qweather.net	IP: 39.105.162.191 Country: China Region: Zhejiang City: Hangzhou
qm.qq.com	IP: 43.129.2.81 Country: China Region: Beijing City: Beijing

DOMAIN	COUNTRY/REGION
init.sms.mob.com	IP: 47.243.26.137 Country: Hong Kong Region: Hong Kong City: Hong Kong
starcourse.rx-networks.cn	IP: 118.193.97.144 Country: China Region: Beijing City: Beijing

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
maps.googleapis.com	ok	IP: 142.250.74.138 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.vphband.com	ok	IP: 120.79.208.77 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 View: Google Map
120.79.208.77	ok	IP: 120.79.208.77 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 View: Google Map

DOMAIN	STATUS	GEOLOCATION
192.168.1.128	ok	IP: 192.168.1.128 Country: - Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
xml.org	ok	IP: 104.239.142.8 Country: United States of America Region: Texas City: Windcrest Latitude: 29.499678 Longitude: -98.399246 View: Google Map
geoapi-413-aa3b3.qweather.net	ok	IP: 45.79.230.148 Country: United States of America Region: California City: Fremont Latitude: 37.548271 Longitude: -121.988571 View: Google Map
www.umeng.com	ok	IP: 59.82.60.43 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 View: Google Map
www.mob.com	ok	IP: 180.188.26.28 Country: China Region: Zhejiang City: Taizhou Latitude: 28.666668 Longitude: 121.349998 View: Google Map

DOMAIN	STATUS	GEOLOCATION
domain-publish-devapi.qweather.net	ok	IP: 123.56.216.251 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 View: Google Map
github.com	ok	IP: 140.82.114.4 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
devapi-413-aa3b3.qweather.net	ok	IP: 123.56.216.251 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 View: Google Map
auth-413-aa3b3.qweather.net	ok	IP: 47.95.178.71 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 View: Google Map
u.wechat.com	ok	IP: 43.159.94.110 Country: China Region: Beijing City: Beijing Latitude: 39.907501 Longitude: 116.397232 View: Google Map

DOMAIN	STATUS	GEOLOCATION
i.qianbao.qq.com	ok	IP: 122.188.45.140 Country: China Region: Hubei City: Jingmen Latitude: 31.033609 Longitude: 112.204720 View: Google Map
identify.verify.mob.com	ok	IP: 47.243.26.137 Country: Hong Kong Region: Hong Kong City: Hong Kong Latitude: 22.285521 Longitude: 114.157692 View: Google Map
starcourse.location.io	ok	IP: 18.238.109.54 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
www.instagram.com	ok	IP: 31.13.70.174 Country: United States of America Region: California City: Los Angeles Latitude: 34.052231 Longitude: -118.243683 View: Google Map
domain-publish-api.qweather.net	ok	IP: 45.79.230.148 Country: United States of America Region: California City: Fremont Latitude: 37.548271 Longitude: -121.988571 View: Google Map

DOMAIN	STATUS	GEOLOCATION
qr.alipay.com	ok	IP: 110.76.30.76 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 View: Google Map
datasetapi-413-aa3b3.qweather.net	ok	IP: 39.105.162.191 Country: China Region: Zhejiang City: Hangzhou Latitude: 30.293650 Longitude: 120.161423 View: Google Map
qm.qq.com	ok	IP: 43.129.2.81 Country: China Region: Beijing City: Beijing Latitude: 39.907501 Longitude: 116.397232 View: Google Map
xml.apache.org	ok	IP: 151.101.2.132 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
api-413-aa3b3.qweather.net	ok	IP: 45.79.230.148 Country: United States of America Region: California City: Fremont Latitude: 37.548271 Longitude: -121.988571 View: Google Map

DOMAIN	STATUS	GEOLOCATION
init.sms.mob.com	ok	IP: 47.243.26.137 Country: Hong Kong Region: Hong Kong City: Hong Kong Latitude: 22.285521 Longitude: 114.157692 View: Google Map
schemas.android.com	ok	No Geolocation information available.
xmlpull.org	ok	IP: 185.199.111.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map
weather.visualcrossing.com	ok	IP: 52.22.202.101 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
starcourse.rx-networks.cn	ok	IP: 118.193.97.144 Country: China Region: Beijing City: Beijing Latitude: 39.907501 Longitude: 116.397232 View: Google Map

EMAILS

EMAIL	FILE
036de@dcdjdkdidcdlsefi.dlpc	com/mob/tools/utils/NtFetcher.java

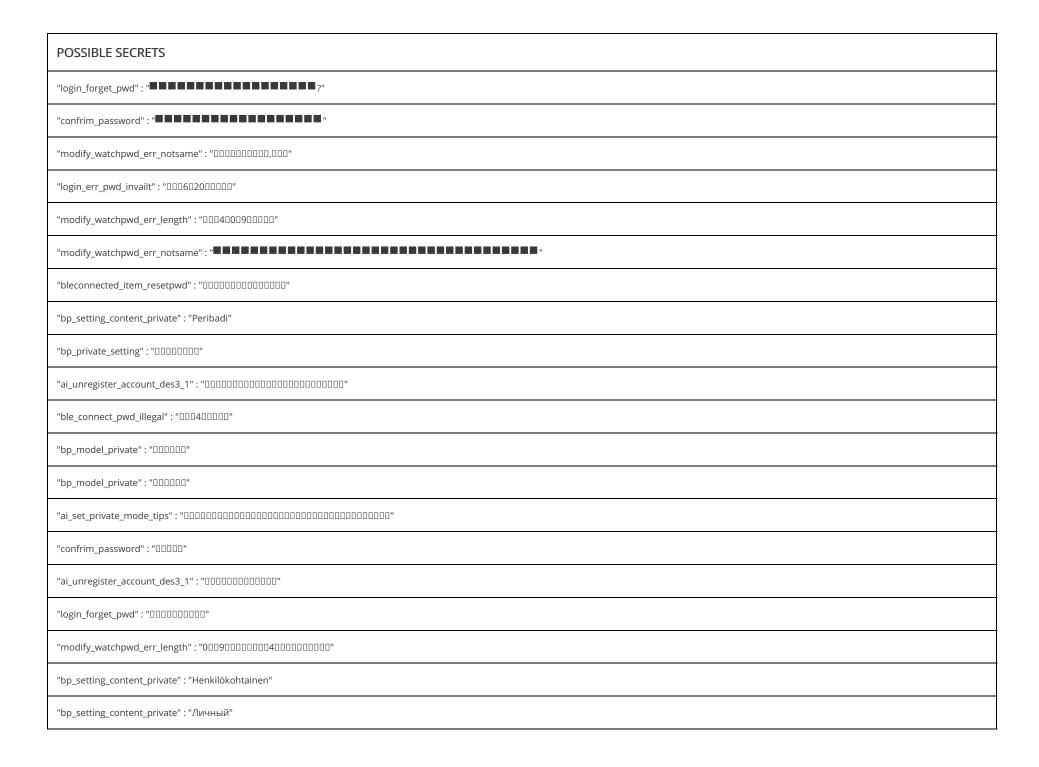
EMAIL	FILE	
005@hgdi.eg5di	com/mob/tools/utils/g.java	
032de9dcdjdkdidcdl@godkucdi0didk.eidlfedk	com/mob/tools/b/h.java	
support@bingo-fit.com wy_ljl@163.com	com/veepoo/hband/activity/fragment/SettingFragment.java	

TRACKERS

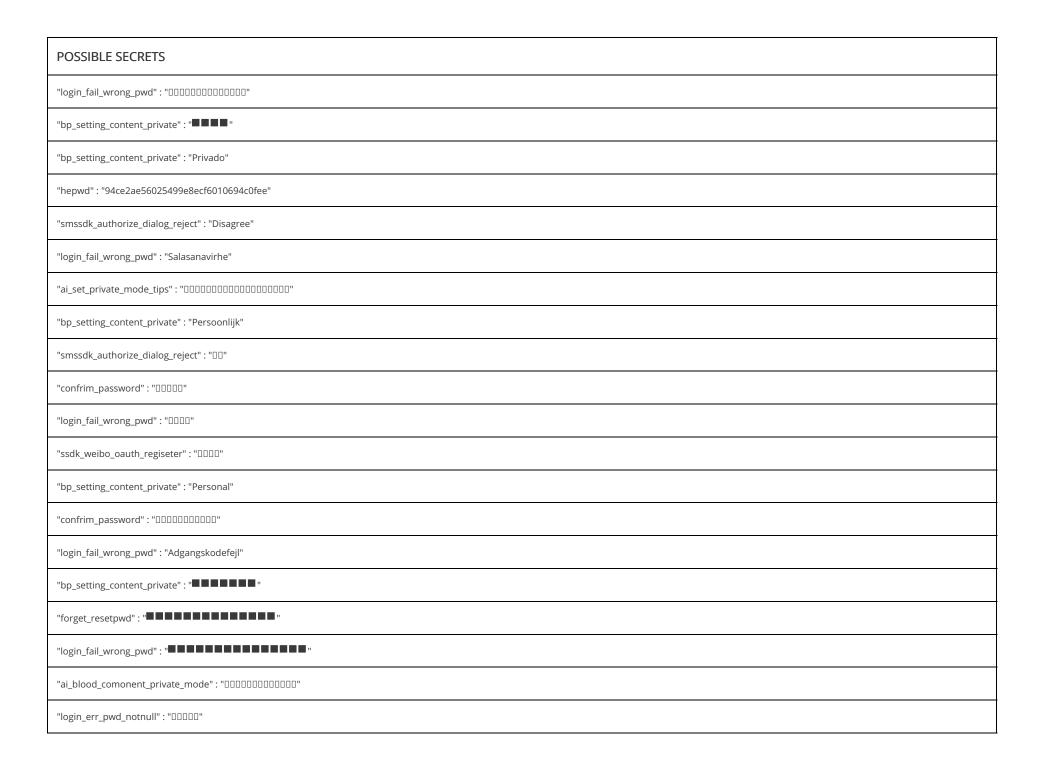
TRACKER	CATEGORIES	URL
Huawei Mobile Services (HMS) Core	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/333

₽ HARDCODED SECRETS

POSSIBLE SECRETS
"ssdk_cmcc_login_one_key" : "DDDDDDDD"
"ssdk_weibo_oauth_regiseter" : "Authorization"
"login_err_pwd_notnull" : "DDDDDDDDDDDD"
"bp_setting_content_private" : "Προσωπικός"
"main_token_unuse" : "DDDDDDDDDDDDD"
"modifypwd_initpwd" : "
"umeng_app_key": "5f602bf9b4739632429f20b7"
"login_err_pwd_invailt": "DDD6D20DDDD"
"ssdk_instapaper_pwd" : "DD"



POSSIBLE SECRETS
"ai_unregister_account_des3_1" : "DDDDDDDDDDDD"
"login_fail_wrong_pwd" : "DDDD"
"bp_setting_content_private" : "Osobno"
"bp_setting_content_private" : "Osobný"
"forget_resetpwd": "DDDD"
"bleconnected_item_resetpwd": "" " " " " " " " " " " " " " " " " "
"bp_setting_content_private" : "□□"
"smssdk_authorize_dialog_accept" : "DD"
"bp_private_setting" : "000000000000"
"login_forget_pwd" : "DDDD?"
"bp_setting_content_private" : "אישי"
"bp_setting_content_private" : "Persönlich"
"modifypwd_initpwd": "DDDDDD0000"
"modify_watchpwd_err_notsame" : "DDDDDDDDDDDDDDD"
"bp_setting_content_private" : "Osobisty"
"ai_unregister_account_des3_1" : "
"bp_setting_content_private" : "Osobní"
"login_err_pwd_notnull" : "DDDDD"
"ssdk_cmcc_auth": "00000000000"
"bp_setting_content_private" : "DDDD"



POSSIBLE SECRETS
"login_forget_pwd": "DDDDD"
"ble_connect_pwd_illegal" : "DDD4DDDD"
"ssdk_instapaper_pwd" : "Password"
"modifypwd_initpwd": "DDDDD0000"
"bleconnected_item_resetpwd":"DDDDDD"
"bp_setting_content_private" : "Pessoal"
"forget_resetpwd": "DDDD"
"bp_setting_content_private" : "Pribadi"
"login_fail_wrong_pwd" : "Lösenordsfel"
"ai_blood_comonent_private_mode" : "
"ble_connect_pwd_illegal" : "000400000000000000"
"forget_resetpwd" : "DDDDDDDD"
"bp_model_private": "0000000000"
"main_token_unuse": "0000,00000"
"ai_blood_comonent_private_mode" : "DDDDDDDD"
"main_token_unuse" : "D000,00000"
"bp_setting_content_private" : "شخصی"
"ai_set_private_mode_tips" : "
"modify_watchpwd_err_notsame" : "0000000000000000000000000000000000
"bp_private_setting" : "DDDDDDDD"

POSSIBLE SECRETS
"ai_set_private_mode_tips" : "0000000000000000000000000000000000
"modify_watchpwd_err_length" : "0004000900000"
"login_err_pwd_notnull" : "
"bp_setting_content_private" : "personalizzata"
"smssdk_authorize_dialog_accept" : "Agree"
"bp_setting_content_private" : "Personlig"
"bp_setting_content_private" : "DDDD"
"modifypwd_initpwd": "DDDDD0000"
"bleconnected_item_resetpwd": "DDDDDD"
"hekey" : "HE2304140935071667"
"login_err_pwd_invailt" : "DDDDDDDDDDDDDDDDDDDDD"
"bp_setting_content_private" : "شخصي"
"smssdk_authorize_dialog_title" : "DDDD"
"bp_setting_content_private" : "Privé"
27749621e6ca022469645faed16e8261acf6af822467382d55c24bb9bc02356ab16e76ddc799dc8ba6b4f110411996eeb63505c9dcf969d3fc085d712f0f1a9713b67aa1128d7cc41bda363afb0ec7ade60e542a4e228693953 31cc0096de412034551e98bb2629ae1b7168b8bc82006d064ab335d8567283e70beb6a49e9423
a6ed0702-d344-460a-8075-b9e8ec90d71b
3517262215D8D3008CBF888750B6418EDC4D562AC33ED6874E0D73ABA667BC3C
fa3acdf1b118fc26668bf72a70d60aa024a2667254c5f0bb8f082bc384b38a4e6d3d1b672467a19793c8f770c63f48b409e87f5787371789af40b95eae9867b9
E49D5C2C0E11B3B1B96CA56C6DE2A14EC7DAB5CCC3B5F300D03E5B4DBA44F539
1234515BA676E63852BD3BF0FB8FFAC9

POSSIBLE SECRETS ceeef5035212dfe7c6a0acdc0ef35ce5b118aab916477037d7381f85c6b6176fcf57b1d1c3296af0bb1c483fe5e1eb0ce9eb2953b44e494ca60777a1b033cc07 b368b110e3b565fe97c91f786e11bc48754cc8e4e6f21d8a94a68ac6ad67aaaf 258EAFA5-E914-47DA-95CA-C5AB0DC85B11 4bdecdf772491e35c4e8b48f88aee22bae1311984f2e1da4dfad0b78ee7f5163 f53c224aefb38daa0825c1b8ea691b16d2e16db10880548afddd780c6670a091a11dafa954ea4a9483797fda1045d2693a08daa48cf9cedce1e8733b857304cb a6ed0701-d344-460a-8075-b9e8ec90d71b 009cbd92ccef123be840deec0c6ed0547194c1e471d11b6f375e56038458fb18833e5bab2e1206b261495d7e2d1d9e5aa859e6d4b67 0123456789ABCDEFabcdef 5fed96c85bd58c58aadbd465c172a4c9a794d8eb2f86cbc7bcee6caf4c7a2c5f 3081a0adab3018d57165e6dd24074bdbac640f6dbe21a9e24d3474a87ebf38b8 13bda4b87eb42ab9e64e6b4f3d17cf8005a4ae94af37bc9fd76ebd91a828f017c81bd63cbe2924e361e20003b9e5f47cdac1f5fba5fca05730a32c5c65869590287207e79a604a2aac429e55f0d35c211367bd226dd5e57df781 0f036071854aa1061a0f34b418b9178895a531107c652a428cfa6ecfa65333580ae7e0edf0e1 d80f18e8081b624cc64985f87f70118f1702985d2e10dbc985ee7be334fd3c7d 49f946663a8deb7054212b8adda248c6 db48223fd9e143f7e133c57f5d08a4e38549ce3ebd921fe3b4003c26e5e35bed ab0a0a6473d1891d388773574764b239d4ad80cb2fd3a83d81d03901c1548c13fee7c9692c326e6682b239d4c5d0021d1b607642c47ec29f10b0602908c3e6c9 8EC90002-F315-4F60-9FB8-838830DAEA50 5c5b6626-aa06-4591-932d-338abd0a988f a6ed0404-d344-460a-8075-b9e8ec90d71b 1dfd1d615cb891ce9a76f42d036af7fce5f8b8efaa11b2f42590ecc4ea4cff28f5f6b0726aeb76254ab5b02a58c1d5b486c39d9da1a58fa6ba2f22196493b3a4cbc283dcf749bf63679ee24d185de70c8dfe05605886c9b53e9f569 082eabdf98c4fb0dcf07eb9bb3e647903489ff0b5d933bd004af5be4a1022fdda41f347f1

POSSIBLE SECRETS

 $f6040d0e807aaec325ecf44823765544e92905158169f694b282bf17388632cf95a83bae7d2d235c1f039b0df1dcca5fda619b6f7f459f2ff8d70ddb7b601592fe29fcae58c028f319b3b12495e67aa5390942a997a8cb572c8030\\b2df5c2b622608bea02b0c3e5d4dff3f72c9e3204049a45c0760cd3604af8d57f0e0c693cc$

e9702f1e92e97fce49cdf81a5fa730a4e913554d09b3fe41e1d8a7fba00a8459

9e87e8d4b8f52f2916d0fb4342aa6b54a81a05666d0bdb23cc5ebf3a07440bc3976adff1ce11c64ddcdbfc017920648217196d51e3165e780e58b5460c525ee9

92974c6802419e4d18b5ec536cbfa167b8e8eff09ec4c8510a5b95750b1e0c82

23c3c8cb41c47dd288cc7f4c218fbc7c839a34e0a0d1b2130e87b7914936b120a2d6570ee7ac66282328d50f2acfd82f2259957c89baea32547758db05de9cd7c6822304c8e45742f24bbbe41c1e12f09e18c6fab4d078065f2e5aaed94c900c66e8bbf8a120eefa7bd1fb52114d529250084f5f6f369ed4ce9645978dd30c51

8EC90001-F315-4F60-9FB8-838830DAEA50

173cf86fe9894a0f70dadd09d4fd88c380836099d4939f8c3754361bdc16a32b

191737288d17e660c4b61440d5d14228a0bf9854499f9d68d8274db55d6d954489371ecf314f26bec236e58fac7fffa9b27bcf923e1229c4080d49f7758739e5bd6014383ed2a75ce1be9b0ab22f283c5c5e11216c5658ba4442 12b6270d629f2d615b8dfdec8545fb7d4f935b0cc10b6948ab4fc1cb1dd496a8f94b51e888dd

B92825C2BD5D6D6D1E7F39EECD17843B7D9016F611136B75441BC6F4D3F00F05

a6ed0401-d344-460a-8075-b9e8ec90d71b

1ef570e1013109c50df8f8c2015faed71e4cf7c53ca9195a99c574ca046aeefdf70bc5fd69f04b0eadf63398698f776cf1ef0db5134efddc3aa4825b69aee94b55356a15d2a50a325ef7bd2d9efe15f3ac5d2303e0bdf5147b3d0fb5fa4fd1d5ea07fe1b45912ff9d7fe472136ff49cb1176f039219bc737ec7ccad132a5ce57

a6ed0402-d344-460a-8075-b9e8ec90d71b

f8d927750a0952ffb5bd87dfb83d781ae65f7bed043a7886d1d3cdcfc94bb77a

4c5f81a0-4728-476f-a57f-b46fa44f07d3

f6af99e2-2b64-4eb6-aba6-4d44fb935939

4230baa077b401374d0fc012375047e79ea0790d58d095ef18d97d95470c738d

00001530-1212-EFDE-1523-785FEABCD123

07ff9b7aeeff969173c45b285fe0fecdbaae244576ff7a2796a36f1c0c11adb4

POSSIBLE SECRETS
c103703e120ae8cc73c9248622f3cd1e
a6ed0703-d344-460a-8075-b9e8ec90d71b
575b6626-fa06-4591-832d-338abd0a988f
24fbae40bcd50b759b26e3ba0f46aa25e932fa7da05f226d75ec507bcf53bce5
e2f856b9f9a4fd4cb2795aeaf83268e4bff189aaec05d691ffde76e075b82648
a6ed0403-d344-460a-8075-b9e8ec90d71b
db53fcdc9ab71e9bdd4eab257fe1aba7989ad2b24fbe3a85dfef72ea1dd6bae2
A6ED0401-D344-460A-8075-B9E8EC90D71B
403f14ad2f0e5eb3c4f3a0bcd5c1592cc4492662ad53191c92905255d4990656

► PLAYSTORE INFORMATION

Title: H Band

Score: 3.6527777 Installs: 5,000,000+ Price: 0 Android Version Support: Category: Health & Fitness Play Store URL: com.veepoo.hband

 $\textbf{Developer Details:} Shenzhen \ Veepoo\ Technology\ Co.,\ Ltd.,\ Shenzhen + Veepoo+Technology+Co., + Ltd.,\ None,\ None,\ veepoo\ and\ roid\ @gmail.com,\ None,\ None,\$

Release Date: Sep 9, 2016 Privacy Policy: Privacy link

Description:

H Band is an application designed to connect with smartwatches. The core features of this application are as follows: Smartwatch management: Users can connect their smartwatches to enjoy a more convenient lifestyle, including features like call handling, sedentary reminders, message synchronization, and app notifications. Data synchronization between phone and device: With the support of smartwatches, users can analyze their sleep patterns, heart health, exercise, and step count. Step counting: Set daily step goals and easily track the number of steps taken by syncing with the smartwatch. Running, walking, cycling: Track routes, analyze data, and monitor your exercise progress for each session. Professional health knowledge about weight, heart rate, and sleep. With the support of smartwatches, accurately monitor different stages of sleep (awake, light, deep, REM) and provide scientific suggestions to help improve sleep quality. We welcome your feedback and suggestions for improvement. Please feel free to let us know your thoughts on the application. Thank you. Supported smartwatches: FireBoltt 084 VEE

∷ SCAN LOGS

Timestamp Event Error

2025-09-01 11:10:33	Generating Hashes	ОК
2025-09-01 11:10:34	Extracting APK	ОК
2025-09-01 11:10:34	Unzipping	OK
2025-09-01 11:10:34	Parsing APK with androguard	ОК
2025-09-01 11:10:36	Extracting APK features using aapt/aapt2	ОК
2025-09-01 11:10:37	Getting Hardcoded Certificates/Keystores	ОК
2025-09-01 11:10:41	Parsing AndroidManifest.xml	ОК
2025-09-01 11:10:41	Extracting Manifest Data	ОК
2025-09-01 11:10:41	Manifest Analysis Started	ОК
2025-09-01 11:10:41	Performing Static Analysis on: H Band (com.veepoo.hband)	ОК
2025-09-01 11:10:43	Fetching Details from Play Store: com.veepoo.hband	ОК
2025-09-01 11:10:44	Checking for Malware Permissions	ОК
2025-09-01 11:10:44	Fetching icon path	ОК
2025-09-01 11:10:44	Library Binary Analysis Started	ОК

2025-09-01 11:10:44	Analyzing lib/arm64-v8a/libjl_pack_format.so	ОК
2025-09-01 11:10:44	Analyzing lib/arm64-v8a/libjl_ota_auth.so	ОК
2025-09-01 11:10:44	Analyzing lib/arm64-v8a/libnative-lib.so	OK
2025-09-01 11:10:44	Analyzing lib/arm64-v8a/libapssdk.so	ОК
2025-09-01 11:10:44	Analyzing lib/arm64-v8a/libluoentz.so	ОК
2025-09-01 11:10:44	Analyzing lib/arm64-v8a/libjl_crc.so	ОК
2025-09-01 11:10:44	Analyzing lib/arm64-v8a/libjl_bmp_convert.so	ОК
2025-09-01 11:10:44	Analyzing lib/arm64-v8a/libabpartool.so	ОК
2025-09-01 11:10:44	Analyzing lib/arm64-v8a/libjl_fatfs.so	ОК
2025-09-01 11:10:44	Analyzing lib/arm64-v8a/libJni_wgs2gcj.so	ОК
2025-09-01 11:10:44	Analyzing lib/arm64-v8a/libscannative.so	ОК
2025-09-01 11:10:44	Analyzing lib/arm64-v8a/libjl_auth.so	ОК
2025-09-01 11:10:44	Analyzing lib/arm64-v8a/libpl_droidsonroids_gif.so	ОК
2025-09-01 11:10:44	Analyzing lib/x86_64/libjl_pack_format.so	ОК

2025-09-01 11:10:44	Analyzing lib/x86_64/libjl_ota_auth.so	ОК
2025-09-01 11:10:44	Analyzing lib/x86_64/libnative-lib.so	ОК
2025-09-01 11:10:44	Analyzing lib/x86_64/libapssdk.so	OK
2025-09-01 11:10:44	Analyzing lib/x86_64/libluoentz.so	ОК
2025-09-01 11:10:44	Analyzing lib/x86_64/libjl_crc.so	ОК
2025-09-01 11:10:44	Analyzing lib/x86_64/libjl_bmp_convert.so	ОК
2025-09-01 11:10:44	Analyzing lib/x86_64/libabpartool.so	ОК
2025-09-01 11:10:44	Analyzing lib/x86_64/libjl_fatfs.so	ОК
2025-09-01 11:10:44	Analyzing lib/x86_64/libJni_wgs2gcj.so	ОК
2025-09-01 11:10:44	Analyzing lib/x86_64/libjl_auth.so	ОК
2025-09-01 11:10:44	Analyzing lib/x86_64/libpl_droidsonroids_gif.so	ОК
2025-09-01 11:10:44	Analyzing lib/armeabi-v7a/libjl_pack_format.so	ОК
2025-09-01 11:10:44	Analyzing lib/armeabi-v7a/libjl_ota_auth.so	ОК
2025-09-01 11:10:44	Analyzing lib/armeabi-v7a/libnative-lib.so	ОК

2025-09-01 11:10:44	Analyzing lib/armeabi-v7a/libapssdk.so	ОК
2025-09-01 11:10:44	Analyzing lib/armeabi-v7a/libluoentz.so	ОК
2025-09-01 11:10:44	Analyzing lib/armeabi-v7a/libjl_crc.so	ОК
2025-09-01 11:10:44	Analyzing lib/armeabi-v7a/libjl_bmp_convert.so	ОК
2025-09-01 11:10:44	Analyzing lib/armeabi-v7a/libjl_fatfs.so	ОК
2025-09-01 11:10:44	Analyzing lib/armeabi-v7a/libJni_wgs2gcj.so	ОК
2025-09-01 11:10:44	Analyzing lib/armeabi-v7a/libscannative.so	ОК
2025-09-01 11:10:44	Analyzing lib/armeabi-v7a/libjl_auth.so	ОК
2025-09-01 11:10:45	Analyzing lib/armeabi-v7a/libpl_droidsonroids_gif.so	ОК
2025-09-01 11:10:45	Analyzing lib/armeabi/libapssdk.so	ОК
2025-09-01 11:10:45	Analyzing lib/armeabi/libJni_wgs2gcj.so	ОК
2025-09-01 11:10:45	Analyzing lib/armeabi/libpl_droidsonroids_gif.so	ОК
2025-09-01 11:10:45	Analyzing lib/x86/libjl_pack_format.so	ОК
2025-09-01 11:10:45	Analyzing lib/x86/libjl_ota_auth.so	ОК

2025-09-01 11:10:45	Analyzing lib/x86/libnative-lib.so	ОК
2025-09-01 11:10:45	Analyzing lib/x86/libapssdk.so	ОК
2025-09-01 11:10:45	Analyzing lib/x86/libluoentz.so	OK
2025-09-01 11:10:45	Analyzing lib/x86/libjl_crc.so	ОК
2025-09-01 11:10:45	Analyzing lib/x86/libjl_bmp_convert.so	ОК
2025-09-01 11:10:45	Analyzing lib/x86/libjl_fatfs.so	ОК
2025-09-01 11:10:45	Analyzing lib/x86/libJni_wgs2gcj.so	ОК
2025-09-01 11:10:45	Analyzing lib/x86/libjl_auth.so	ОК
2025-09-01 11:10:45	Analyzing lib/x86/libpl_droidsonroids_gif.so	ОК
2025-09-01 11:10:45	Analyzing lib/mips/libpl_droidsonroids_gif.so	ОК
2025-09-01 11:10:45	Analyzing lib/mips64/libpl_droidsonroids_gif.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/arm64-v8a/libjl_pack_format.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/arm64-v8a/libjl_ota_auth.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/arm64-v8a/libnative-lib.so	ОК

2025-09-01 11:10:45	Analyzing apktool_out/lib/arm64-v8a/libapssdk.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/arm64-v8a/libluoentz.so	OK
2025-09-01 11:10:45	Analyzing apktool_out/lib/arm64-v8a/libjl_crc.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/arm64-v8a/libjl_bmp_convert.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/arm64-v8a/libabpartool.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/arm64-v8a/libjl_fatfs.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/arm64-v8a/libJni_wgs2gcj.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/arm64-v8a/libscannative.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/arm64-v8a/libjl_auth.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/arm64-v8a/libpl_droidsonroids_gif.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86_64/libjl_pack_format.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86_64/libjl_ota_auth.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86_64/libnative-lib.so	OK
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86_64/libapssdk.so	ОК

2025-09-01 11:10:45	Analyzing apktool_out/lib/x86_64/libluoentz.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86_64/libjl_crc.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86_64/libjl_bmp_convert.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86_64/libabpartool.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86_64/libjl_fatfs.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86_64/libJni_wgs2gcj.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86_64/libjl_auth.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86_64/libpl_droidsonroids_gif.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/armeabi-v7a/libjl_pack_format.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/armeabi-v7a/libjl_ota_auth.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/armeabi-v7a/libnative-lib.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/armeabi-v7a/libapssdk.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/armeabi-v7a/libluoentz.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/armeabi-v7a/libjl_crc.so	ОК

2025-09-01 11:10:45	Analyzing apktool_out/lib/armeabi-v7a/libjl_bmp_convert.so	OK
2025-09-01 11:10:45	Analyzing apktool_out/lib/armeabi-v7a/libjl_fatfs.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/armeabi-v7a/libJni_wgs2gcj.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/armeabi-v7a/libscannative.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/armeabi-v7a/libjl_auth.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/armeabi-v7a/libpl_droidsonroids_gif.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/armeabi/libapssdk.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/armeabi/libJni_wgs2gcj.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/armeabi/libpl_droidsonroids_gif.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86/libjl_pack_format.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86/libjl_ota_auth.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86/libnative-lib.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86/libapssdk.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86/libluoentz.so	ОК

2025-09-01 11:10:45	Analyzing apktool_out/lib/x86/libjl_crc.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86/libjl_bmp_convert.so	OK
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86/libjl_fatfs.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86/libJni_wgs2gcj.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86/libjl_auth.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/x86/libpl_droidsonroids_gif.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/mips/libpl_droidsonroids_gif.so	ОК
2025-09-01 11:10:45	Analyzing apktool_out/lib/mips64/libpl_droidsonroids_gif.so	ОК
2025-09-01 11:10:45	Reading Code Signing Certificate	ОК
2025-09-01 11:10:46	Running APKiD 2.1.5	ОК
2025-09-01 11:10:52	Detecting Trackers	ОК
2025-09-01 11:10:55	Decompiling APK to Java with JADX	ОК
2025-09-01 11:11:14	Converting DEX to Smali	ОК
2025-09-01 11:11:14	Code Analysis Started on - java_source	ОК

2025-09-01 11:11:17	Android SBOM Analysis Completed	ОК
2025-09-01 11:11:22	Android SAST Completed	ОК
2025-09-01 11:11:22	Android API Analysis Started	ОК
2025-09-01 11:11:28	Android API Analysis Completed	ОК
2025-09-01 11:11:28	Android Permission Mapping Started	ОК
2025-09-01 11:11:42	Android Permission Mapping Completed	ОК
2025-09-01 11:11:42	Android Behaviour Analysis Started	ОК
2025-09-01 11:11:50	Android Behaviour Analysis Completed	ОК
2025-09-01 11:11:50	Extracting Emails and URLs from Source Code	ОК
2025-09-01 11:11:55	Email and URL Extraction Completed	ОК
2025-09-01 11:11:55	Extracting String data from APK	ОК
2025-09-01 11:11:57	Extracting String data from SO	ОК
2025-09-01 11:11:57	Extracting String data from Code	ОК
2025-09-01 11:11:57	Extracting String values and entropies from Code	ОК
		·

2025-09-01 11:12:00	Performing Malware check on extracted domains	ОК
2025-09-01 11:12:19	Saving to Database	ОК

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.

© 2025 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.