MOBSF

ANDROID STATIC ANALYSIS REPORT

CloudEdge (5.0.2)

File Name:	com.cloudedge.smarteye_5.0.2-502_minAPI21(arm64-v8a,armeabi-v7a)(nodpi)_apkmirror.com.apk
Package Name:	com.cloudedge.smarteye
Scan Date:	Feb. 10, 2024, 5:13 p.m.

App Security Score: 44/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 6/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
9	46	1	2	18

FILE INFORMATION

File Name: com.cloudedge.smarteye_5.0.2-502_minAPI21(arm64-v8a,armeabi-v7a)(nodpi)_apkmirror.com.apk
Size: 86.95MB
MD5: 63a4201a547c413580fc11829d05f5c0
SHA1: 5410b5ec32c889068c2ff28aa7c587d600c2d3e7
SHA256: 8da3a4a8673dacbf2a28c961687e3288ada4b1b09f0c75b4d92e685181182a87

APP INFORMATION

App Name: CloudEdge
Package Name: com.cloudedge.smarteye
Main Activity: com.ppstrong.weeye.SplashActivity
Target SDK: 31
Min SDK: 21
Max SDK:
Android Version Name: 5.0.2
Android Version Code: 502

APP COMPONENTS

Activities: 379
Services: 26
Receivers: 10
Providers: 5
Exported Activities: 21
Exported Services: 6
Exported Receivers: 5
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=CN, ST=zhejiang, L=hangzhou, O=cloudedge, OU=cloudedge, CN=cloudedge
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-11-10 07:50:31+00:00
Valid To: 2042-11-04 07:50:31+00:00
Issuer: C=CN, ST=zhejiang, L=hangzhou, O=cloudedge, OU=cloudedge, CN=cloudedge
Serial Number: 0x1aaaf557
Hash Algorithm: sha256
md5: 1e33690629f03a8405ac87210074d2c7
sha1: 1fb2c707d1ecd4f1c291c0b1b9bd57ff211c0708

sha256: 68f99e70a395f605dff70233190a3d409aa9d55d4e10c238e7060000d0478153
sha512: fd448441759395d7707b0e4c4a0010095eae8b6c1dc21e226f8f526811fce7a4ba19fa6ea807cbb575166243fe80ded20b89411f56a34d568b7c1ff9a55404a2
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 419c931454356a607ddc5fe998966bc353b466239cee5f789b9ed6b158b0017f
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
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.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.CHANGE_WIFI_MULTICAST_STATE	normal	allow Wi-Fi Multicast reception	Allows an application to receive packets not directly addressed to your device. This can be useful when discovering services offered nearby. It uses more power than the non-multicast mode.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.SYSTEM_OVERLAY_WINDOW	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
com.cloudedge.smarteye.permission.JPUSH_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	unknown	Unknown permission	Unknown permission from android reference
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.ACCESS_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.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.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
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.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
android.permission.DISABLE_KEYGUARD	normal	disable keyguard	Allows applications to disable the keyguard if it is not secure.
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	dangerous	mount and unmount file systems	Allows the application to mount and unmount file systems for removable storage.
android.permission.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
com.cloudedge.smarteye.permission.MIPUSH_RECEIVE	unknown	Unknown permission	Unknown permission from android reference
com.cloudedge.smarteye.permission.PROCESS_PUSH_MSG	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
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.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.READ_PRIVILEGED_PHONE_STATE	unknown	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

PERMISSION	STATUS	INFO	DESCRIPTION
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code DETAILS: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check device ID check subscriber ID check ro.product.device check ro.kernel.qemu check emulator file check FINDINGS: Compiler DETAILS: r8
classes2.dex	FINDINGS: Anti-VM Code DETAILS: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.TAGS check network operator name check possible VM check FINDINGS: Compiler DETAILS: r8 without marker (suspicious)

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
subscriber ID check
emulator file check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
subscriber ID check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes6.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.ppstrong.weeye.view.activity.setting.AlexaActivity	Schemes: https://, Hosts: meari-us.s3.us-west-1.amazonaws.com, Path Prefixes: /8/alexa,
com.ppstrong.weeye.view.activity.setting.cloud_storage.PaypalCheckoutActivity	Schemes: https://, Hosts: meari-us.s3.us-west-1.amazonaws.com, Path Prefixes: /paypal/39,
com.ppstrong.weeye.SplashActivity	Schemes: meari_cloudedge://, vpushscheme://, Hosts: com.cloudedge.smarteye, com.vivo.push.notifysdk, Paths: /hwpush_detail, /detail,
com.braintreepayments.api.BraintreeBrowserSwitchActivity	Schemes: com.cloudedge.smarteye.braintree://,
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.com.cloudedge.smarteye,

NETWORK SECURITY

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

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

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 33 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched 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	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Activity (com.ppstrong.weeye.view.activity.setting.AlexaActivity) 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.
4	Activity (com.ppstrong.weeye.view.activity.setting.cloud_storage.PaypalCheckoutActivity) 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.cloudedge.smarteye.wxapi.WXEntryActivity) 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	Activity (com.braintreepayments.api.BraintreeBrowserSwitchActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Service (com.ppstrong.weeye.service.FrontService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Service (com.ppstrong.weeye.service.FloatingService) 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.
9	Service (com.ppstrong.weeye.service.CheckUpgradeService) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
10	Broadcast Receiver (com.ppstrong.weeye.receiver.BootReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.RECEIVE_BOOT_COMPLETED [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.
11	Service (com.vivo.push.sdk.service.CommandClientService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.push.permission.UPSTAGESERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
12	Broadcast Receiver (com.meari.base.push.PushMessageReceiverImpl) 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.
13	Service (com.xiaomi.mipush.sdk.PushMessageHandler) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
14	Broadcast Receiver (com.xiaomi.push.service.receivers.NetworkStatusReceiver) 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	Broadcast Receiver (com.ppstrong.weeye.receiver.MiPushReceiver) 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.
16	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
17	Activity (com.meari.device.nvr.NvrRenameActivity) 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.
18	Activity (com.meari.device.nvr.NvrTimingActivity) 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.
19	Activity (com.meari.device.nvr.NvrUpdateActivity) 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.meari.device.nvr.NvrMotionActivity) 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	Activity (com.meari.device.nvr.NvrImageSettingActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
22	Activity (com.meari.device.nvr.NvrInformationActivity) 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	Activity (com.meari.device.nvr.NvrChannelSettingActivity) 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.
24	Activity (com.meari.device.nvr.NvrMainActivity) 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	Activity (com.meari.device.nvr.NvrDiskInfoActivity) 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.
26	Activity (com.meari.device.nvr.NvrDiskManagerActivity) 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.
27	Activity (com.meari.device.nvr.NvrQrcodeActivity) 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.
28	Activity (com.meari.device.nvr.NvrMainSettingActivity) 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.
29	Activity (com.darsh.multipleimageselect.activities.AlbumSelectActivity) 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.
30	Activity (com.darsh.multipleimageselect.activities.ImageSelectActivity) 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.
31	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
32	Service (com.firebase.jobdispatcher.GooglePlayReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_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.
33	Activity (com.alipay.sdk.app.PayResultActivity) 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.
34	Activity (com.alipay.sdk.app.AlipayResultActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
35	High Intent Priority (1000) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: **6** | WARNING: **10** | INFO: **1** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/braintreepayments/api/internal/TLSSocketFactory.java com/meari/sdk/http/https/HttpsUtils.java com/meari/sdk/mqtt/PPMqttService.java com/meari/sdk/utils/SdkUtils.java lib/android/paypal/com/magnessdk/network/base/f.java org/conscrypt/DefaultSSLContextImpl.java org/conscrypt/SSLParametersImpl.java org/eclipse/paho/android/service/MqttAndroidClient.java org/eclipse/paho/client/mqttv3/internal/security/SSLSocketFactoryFactory.java
2	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/alipay/sdk/app/b.java
				butterknife/ButterKnife.java cn/jzvd/JZTextureView.java cn/jzvd/JZUtils.java cn/jzvd/Jzvd.java cn/jzvd/JzvdStd.java com/alibaba/android/arouter/launcher/_ARouter.java com/alibaba/android/arouter/utils/ClassUtils.java com/alibaba/android/arouter/utils/DefaultLogger.java com/alibaba/sdk/android/oss/common/OSSLog.java com/alibaba/sdk/android/oss/common/OSSLogToFileUtils.java com/alibaba/sdk/android/oss/common/auth/OSSFederationToken.java com/alibaba/sdk/android/oss/common/utils/HttpdnsMini.java com/alibaba/sdk/android/oss/network/OSSRequestTask.java com/alipay/android/phone/mrpc/core/b.java com/amazonaws/cognito/clientcontext/data/UserContextDataProvider.java com/amazonaws/cognito/clientcontext/datacollection/ApplicationDataCollector.java com/amazonaws/cognito/clientcontext/util/SignatureGenerator.java com/amazonaws/logging/AndroidLog.java com/amazonaws/logging/LogFactory.java com/amazonaws/mobile/auth/core/DefaultSignInResultHandler.java com/amazonaws/mobile/auth/core/IdentityManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/amazonaws/mobile/auth/core/signin/SignInManager.java com/amazonaws/mobile/client/AWSMobileClient.java com/amazonaws/mobile/client/internal/InternalCallback.java com/amazonaws/mobile/client/internal/oauth2/OAuth2Client.java com/amazonaws/mobileconnectors/cognitoidentityprovider/CognitoUserSession.java com/bigkoo/pickerview/lib/WheelView.java com/bigkoo/pickerview/utils/LunarCalendar.java com/braintreepayments/browserswitch/BrowserSwitchPersistentStore.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/Glide.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/ImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerFragment.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/clj/fastble/BleManager.java com/clj/fastble/bluetooth/BleBluetooth.java com/clj/fastble/bluetooth/SplitWriter.java com/clj/fastble/scan/BleScanPresenter.java com/clj/fastble/scan/BleScanner.java com/clj/fastble/utils/BleLog.java com/davemorrissey/labs/subscaleview/SubsamplingScaleImageView.java com/davemorrissey/labs/subscaleview/decoder/SkiaPooledImageRegion Decoder.java com/dctrain/module_add_device/adapter/AddDeviceKindTwoAdapter.jav a com/dctrain/module_add_device/view/BleDeviceAndWifiScanActivity.java com/dctrain/module_add_device/view/BleSearchDeviceActivity.java com/firebase/jobdispatcher/DefaultJobValidator.java com/firebase/jobdispatcher/ExecutionDelegator.java com/firebase/jobdispatcher/GooglePlayCallbackExtractor.java com/firebase/jobdispatcher/GooglePlayMessageHandler.java com/firebase/jobdispatcher/GooglePlayReceiver.java com/firebase/jobdispatcher/JobCoder.java com/firebase/jobdispatcher/JobService.java com/firebase/jobdispatcher/JobServiceConnection.java com/github/mikephil/charting/charts/BarChart.java com/github/mikephil/charting/charts/BarLineChartBase.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/charts/CombinedChart.java com/github/mikephil/charting/charts/HorizontalBarChart.java com/github/mikephil/charting/charts/PieRadarChartBase.java 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/BarLineChartTouchListener.java com/github/mikephil/charting/renderer/CombinedChartRenderer.java com/github/mikephil/charting/renderer/ScatterChartRenderer.java com/github/mikephil/charting/utils/FileUtils.java com/github/mikephil/charting/utils/Utils.java com/heytap/mcssdk/utils/d.java com/hp/hpl/sparta/ParseByteStream.java com/hp/hpl/sparta/ParseCharStream.java com/hp/hpl/sparta/ParseException.java com/huantansheng/easyphotos/models/album/entity/Photo.java com/huantansheng/easyphotos/models/puzzle/DegreeSeekBar.java com/huantansheng/easyphotos/models/puzzle/PuzzleView.java com/huantansheng/easyphotos/models/puzzle/straight/StraightLine.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/huantansheng/easyphotos/models/puzzle/template/slant/NumberSlantLayout.java com/huantansheng/easyphotos/models/puzzle/template/straight/NumberStraightLayout.java com/huantansheng/easyphotos/models/puzzle/template/straight/TwoStraightLayout.java com/huantansheng/easyphotos/ui/EasyPhotosActivity.java com/huantansheng/easyphotos/utils/file/FileUtils.java com/huantansheng/easyphotos/utils/uri/UriUtils.java com/jph/takephoto/app/TakePhotoFragment.java com/jph/takephoto/app/TakePhotoImpl.java com/jph/takephoto/uitl/ImageRotateUtil.java com/jph/takephoto/uitl/IntentUtils.java com/jph/takephoto/uitl/TImageFiles.java com/jph/takephoto/uitl/TUriParse.java com/jph/takephoto/uitl/TUtils.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/meari/base/app/MeariApplication.java com/meari/base/common/NotificationUtil.java com/meari/base/util/AesBtye16Helper.java com/meari/base/util/AppConfigManager.java com/meari/base/util/FileUtil.java com/meari/base/util/GooglePayManager.java com/meari/base/util/GsonUtil.java com/meari/base/util/LanguageUtil.java com/meari/base/util/NotificationUtils.java com/meari/base/util/PermissionUtil.java com/meari/base/util/RomUtil.java com/meari/base/util/WifiConnectHelper.java com/meari/base/util/WifiUtil.java com/meari/base/util/db/AlertMsgDb.java com/meari/base/util/db/RecentContactsDao.java com/meari/base/util/fresco/MyFresco.java com/meari/base/util/statistic/LogcatHelper.java com/meari/base/util/statistic/ReportedData.java com/meari/base/util/utils/WifiUtil.java com/meari/base/view/CalendarView.java com/meari/base/view/ChrysanthemumView.java com/meari/base/view/CircleCameraPreview.java com/meari/base/view/CircleProgressView.java com/meari/base/view/FlowLayout.java com/meari/base/view/InputEditext.java com/meari/base/view/RoundProgressBar.java com/meari/base/view/SwipeLayout.java com/meari/base/view/VerifyEditText.java com/meari/base/view/pickerview/utils/LunarCalendar.java com/meari/base/view/pop/ScaleRulePop.java com/meari/base/view/pullToRefresh/OverscrollHelper.java com/meari/base/view/pullToRefresh/PullToRefreshBase.java com/meari/base/view/pullToRefresh/Utils.java com/meari/base/view/recyclerview/divider/DividerMiddleItemDecoration.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/meari/base/view/ruler/RulerView.java com/meari/base/view/ruler/utils/DateUtils.java com/meari/base/view/wheelview/view/WheelView.java com/meari/base/view/widget/CircleProgressView.java com/meari/base/view/widget/DragPolygonView.java com/meari/base/view/widget/LightHsvView.java com/meari/base/view/widget/playcontrolview/IntercomView.java com/meari/cloudconfig/ConfigUtils.java com/meari/cloudconfig/GsonUtil.java com/meari/device/common/view/Chronometer.java com/meari/device/jingle/db/JingleMsgDao.java com/meari/device/jingle/db/JingleMsgDbUtils.java com/meari/device/jingle/ui/JingleMsgViewModel.java com/meari/device/receptacle/ReceptacleMainViewModel.java com/meari/family/activity/AddRoomActivity.java com/meari/ffplayer/ffplayer.java com/meari/scene/view/activity/SceneDeviceStatusActivity$showEnumView$adapter$1.java com/meari/scene/view/activity/SceneDeviceStatusActivity.java com/meari/scene/view/activity/SceneDpTaskActivity$showPopWindow$2.java com/meari/scene/view/activity/SceneDpTaskActivity$showPopWindow$3.java com/meari/scene/view/activity/SceneDpTaskActivity.java com/meari/scene/view/activity/SceneEditActivity.java com/meari/scene/view/activity/SceneLogActivity.java com/meari/scene/view/activity/SceneManageActivity.java com/meari/scene/view/activity/SceneTimeDelayActivity.java com/meari/scene/view/activity/SceneValidTimeActivity$showEffectivePeriodCustomPopWindow$1.java com/meari/scene/view/fragment/SceneFragment.java com/meari/scene/view/widget/SceneActionDialog.java com/meari/sdk/MeariIotController.java com/meari/sdk/MeariUser.java com/meari/sdk/PrtpDeviceController.java com/meari/sdk/UserRequestManager.java com/meari/sdk/http/ResponseData.java com/meari/sdk/http/cookie/store/PersistentCookieStore.java com/meari/sdk/mqtt/AWSMqttService.java com/meari/sdk/mqtt/PPMqttService.java com/meari/sdk/scene/util/JsonUtil.java com/meari/sdk/utils/CloudPlaybackUtil.java com/meari/sdk/utils/GsonUtil.java com/meari/sdk/utils/OkLogger.java com/meari/sdk/utils/SdkUtils.java com/meari/sdk/zxing/CodeUtils.java com/meari/sdk/zxing/camera/AutoFocusCallback.java com/meari/sdk/zxing/camera/CameraConfigurationManager.java com/meari/sdk/zxing/camera/FlashlightManager.java com/meari/sdk/zxing/camera/PreviewCallback.java com/next/easynavigation/view/EasyNavigationBar.java com/paypal/android/sdk/data/collector/PayPalDataCollector.java com/paypal/android/sdk/onetouch/core/Result.java com/ppstrong/ppsplayer/PPSGLSurfaceView.java com/ppstrong/ppsplayer/PPSMediaCodec.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/ppstrong/ppsplayer/PPSProgram.java com/ppstrong/ppsplayer/PPSStreamDecoderCore.java com/ppstrong/ppsplayer/PrtpCameraPlayer.java com/ppstrong/ppsplayer/UtilRecord.java com/ppstrong/ppsplayer/meariLog.java com/ppstrong/weeye/firebase/FirebaseEventRecorder.java com/ppstrong/weeye/play/PlayVideoControl.java com/ppstrong/weeye/play/PlayVideoControlMode.java com/ppstrong/weeye/presenter/SplashPresenter.java com/ppstrong/weeye/presenter/device/MessageDevicePresenter.java com/ppstrong/weeye/presenter/setting/ContactSearchResultPresenter.java com/ppstrong/weeye/presenter/setting/FaceAddPresenter.java com/ppstrong/weeye/presenter/setting/FaceManagePresenter.java com/ppstrong/weeye/presenter/setting/LeaveMessagePresenter.java com/ppstrong/weeye/presenter/setting/RegularlyPatrolPresenter.java com/ppstrong/weeye/presenter/setting/setup/SetupHintPresenter.java com/ppstrong/weeye/presenter/user/CustomerServicePresenterImpl.java com/ppstrong/weeye/push/MyFirebaseMessagingService.java com/ppstrong/weeye/service/BellCallService.java com/ppstrong/weeye/service/MyJobService.java com/ppstrong/weeye/test/TestCaseManager.java com/ppstrong/weeye/utils/FragmentFitsSystemWindowInViewPagerFix.java com/ppstrong/weeye/utils/NetObserver.java com/ppstrong/weeye/utils/glide/AlarmLocalImageModule.java com/ppstrong/weeye/utils/glide/AlarmNetImageModule.java com/ppstrong/weeye/utils/glide/AliOSSNetImageModule.java com/ppstrong/weeye/utils/glide/EncryptedNetImageModule.java com/ppstrong/weeye/view/CommonWebViewActivity.java com/ppstrong/weeye/view/activity/MainActivity.java com/ppstrong/weeye/view/activity/TestActivity.java com/ppstrong/weeye/view/activity/customer/PicAdapter.java com/ppstrong/weeye/view/activity/customer/ProblemFeedbackActivity.java com/ppstrong/weeye/view/activity/device/BellCallActivity.java com/ppstrong/weeye/view/activity/device/MultiVideoActivity.java com/ppstrong/weeye/view/activity/message/CustomerMessageActivity.java com/ppstrong/weeye/view/activity/message/MessageNotifySettingActivity.java com/ppstrong/weeye/view/activity/setting/CloudPayNewActivity.java com/ppstrong/weeye/view/activity/setting/FaceAddChooseActivity.java com/ppstrong/weeye/view/activity/setting/PolygonRoiActivity.java com/ppstrong/weeye/view/activity/setting/RegularlyPatrolActivity.java com/ppstrong/weeye/view/activity/setting/TimeSetPopActivity.java com/ppstrong/weeye/view/activity/setting/cloud_storage/PaypalCheckoutActivity.java com/ppstrong/weeye/view/activity/user/BaseCustomerPhotoActivity.java com/ppstrong/weeye/view/activity/user/BaseUpIconActivity.java com/ppstrong/weeye/view/activity/user/FeedbackActivity.java com/ppstrong/weeye/view/activity/user/SettingActivity.java com/ppstrong/weeye/view/activity/user/TakePhotoActivity.java com/ppstrong/weeye/view/adapter/MultiVideoAdapter.java com/ppstrong/weeye/view/adapter/PlaybackCloudAlarmMsgAdapter.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/ppstrong/weeye/view/adapter/ProblemPhotoAdapter.java com/ppstrong/weeye/view/fragment/AccountFragment.java com/ppstrong/weeye/view/fragment/AlarmMsgLoader.java com/ppstrong/weeye/view/fragment/CustomerServiceMsgFragment.java com/ppstrong/weeye/view/fragment/HomeFragment.java com/ppstrong/weeye/view/fragment/HuntingLiveFragment.java com/ppstrong/weeye/view/fragment/LiveFragment.java com/ppstrong/weeye/view/fragment/MainMsgAlarmFragment.java com/ppstrong/weeye/view/fragment/MainMsgAlarmFragment_1.java com/ppstrong/weeye/view/fragment/PlaybackCloudFragmentNew.java com/ppstrong/weeye/view/fragment/SinglePreviewFragment.java com/ppstrong/weeye/view/pop/ScaleRulePop.java com/ppstrong/weeye/widget/media/IjkVideoView.java com/ppstrong/weeye/widget/media/MeariGlView.java com/ppstrong/weeye/widget/media/MeariMediaPlayer.java com/ppstrong/weeye/widget/media/SurfaceRenderView.java com/ppstrong/weeye/widget/media/TextureRenderView.java com/snail/collie/battery/BatteryStatsTracker.java com/snail/collie/core/LooperMonitor.java com/snail/collie/startup/$$Lambda$LauncherTracker$activityLifecycleCallbacks1Su_VtrQL_8X29T05LpYI1KU2Lj0.java com/soundcloud/android/crop/CropImageActivity.java com/soundcloud/android/crop/CropUtil.java com/soundcloud/android/crop/Log.java com/tbruyelle/rxpermissions2/RxPermissionsFragment.java com/tencent/bugly/crashreport/BuglyLog.java com/tencent/bugly/crashreport/CrashReport.java com/tencent/bugly/proguard/al.java com/tencent/bugly/proguard/p.java com/tencent/mm/opensdk/channel/MMessageActV2.java com/tencent/mm/opensdk/channel/a/a.java com/tencent/mm/opensdk/diffdev/DiffDevOAuthFactory.java com/tencent/mm/opensdk/diffdev/a/a.java com/tencent/mm/opensdk/diffdev/a/b.java com/tencent/mm/opensdk/diffdev/a/d.java com/tencent/mm/opensdk/diffdev/a/e.java com/tencent/mm/opensdk/diffdev/a/f.java com/tencent/mm/opensdk/modelbiz/AddCardToWXCardPackage.java com/tencent/mm/opensdk/modelbiz/ChooseCardFromWXCardPackage.java com/tencent/mm/opensdk/modelbiz/SubscribeMessage.java com/tencent/mm/opensdk/modelbiz/SubscribeMiniProgramMsg.java com/tencent/mm/opensdk/modelbiz/WXInvoiceAuthInsert.java com/tencent/mm/opensdk/modelbiz/WXLaunchMiniProgram.java com/tencent/mm/opensdk/modelbiz/WXLaunchMiniProgramWithToken.java com/tencent/mm/opensdk/modelbiz/WXNontaxPay.java com/tencent/mm/opensdk/modelbiz/WXOpenBusinessView.java com/tencent/mm/opensdk/modelbiz/WXPayInsurance.java com/tencent/mm/opensdk/modelbiz/WXPreloadMiniProgram.java com/tencent/mm/opensdk/modelmsg/GetMessageFromWX.java com/tencent/mm/opensdk/modelmsg/LaunchFromWX.java com/tencent/mm/opensdk/modelmsg/SendAuth.java com/tencent/mm/opensdk/modelmsg/SendMessageToWX.java com/tencent/mm/opensdk/modelmsg/WXAppExtendObject.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/tencent/mm/opensdk/modelmsg/WXDesignerSharedObject.java com/tencent/mm/opensdk/modelmsg/WXDynamicVideoMiniProgramObject.java com/tencent/mm/opensdk/modelmsg/WXEmojiObject.java com/tencent/mm/opensdk/modelmsg/WXEmojiPageSharedObject.java com/tencent/mm/opensdk/modelmsg/WXEmojiSharedObject.java com/tencent/mm/opensdk/modelmsg/WXEnterpriseCardObject.java com/tencent/mm/opensdk/modelmsg/WXFileObject.java com/tencent/mm/opensdk/modelmsg/WXGameVideoFileObject.java com/tencent/mm/opensdk/modelmsg/WXImageObject.java com/tencent/mm/opensdk/modelmsg/WXMediaMessage.java com/tencent/mm/opensdk/modelmsg/WXMiniProgramObject.java com/tencent/mm/opensdk/modelmsg/WXMusicObject.java com/tencent/mm/opensdk/modelmsg/WXTextObject.java com/tencent/mm/opensdk/modelmsg/WXVideoFileObject.java com/tencent/mm/opensdk/modelmsg/WXVideoObject.java com/tencent/mm/opensdk/modelmsg/WXWebpageObject.java com/tencent/mm/opensdk/modelpay/PayReq.java com/tencent/mm/opensdk/openapi/BaseWXApiImplV10.java com/tencent/mm/opensdk/openapi/MMSharedPreferences.java com/tencent/mm/opensdk/openapi/WXAPIFactory.java com/tencent/mm/opensdk/openapi/WXApiImplComm.java com/tencent/mm/opensdk/utils/Log.java com/tencent/mm/opensdk/utils/a.java com/tencent/mm/opensdk/utils/c.java com/tencent/mm/opensdk/utils/d.java com/tencent/mmkv/MMKV.java com/tencent/mmkv/MMKVContentProvider.java com/uuzuche/lib_zxing/activity/CaptureActivity.java com/uuzuche/lib_zxing/camera/AutoFocusCallback.java com/uuzuche/lib_zxing/camera/CameraConfigurationManager.java com/uuzuche/lib_zxing/camera/FlashlightManager.java com/uuzuche/lib_zxing/camera/PreviewCallback.java com/uuzuche/lib_zxing/decoding/CaptureActivityHandler.java com/uuzuche/lib_zxing/decoding/DecodeHandler.java com/vivo/push/util/g.java com/vivo/push/util/n.java com/xiaomi/channel/commonutils/logger/a.java com/xiaomi/mipush/sdk/y.java com/xiaomi/push/Cdo.java com/xiaomi/push/az.java com/xiaomi/push/ba.java com/xiaomi/push/cq.java com/xiaomi/push/dp.java com/zhy/view/flowlayout/TagAdapter.java com/zhy/view/flowlayout/TagFlowLayout.java dagger/android/AndroidInjection.java io/github/inflationx/viewpump/internal/ReflectionUtils.java lib/android/paypal/com/magnessdk/b/a.java lib/android/paypal/com/magnessdk/network/b.java me/shaohui/advancedluban/Luban.java net/danlew/android/joda/ResUtils.java net/danlew/android/joda/TimeZoneChangedReceiver.java org/conscrypt/Platform.java org/conscrypt/ct/CTVerifier.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/eclipse/paho/android/service/AlarmPingSender.java org/eclipse/paho/android/service/MqttConnection.java org/joda/time/tz/DateTimeZoneBuilder.java org/slf4j/helpers/Util.java org/slf4j/impl/AndroidLoggerAdapter.java rx/internal/util/IndexedRingBuffer.java top/zibin/luban/Checker.java top/zibin/luban/Luban.java top/zibin/luban/LubanUtils.java top/zibin/luban/io/LuEmptyArrayPool.java
4	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/alibaba/sdk/android/oss/common/OSSLogToFileUtils.java com/alibaba/sdk/android/oss/internal/ExtensionRequestOperation.java com/alipay/apmobilesecuritysdk/a/a.java com/alipay/apmobilesecuritysdk/a/b.java com/alipay/security/mobile/module/b/b.java com/alipay/security/mobile/module/c/c.java com/danikula/videocache/StorageUtils.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/utils/FileUtils.java com/huantansheng/easyphotos/ui/EasyPhotosActivity.java com/huantansheng/easyphotos/ui/PuzzleSelectorActivity.java com/huantansheng/easyphotos/utils/bitmap/BitmapUtils.java com/huantansheng/easyphotos/utils/file/FileUtils.java com/huantansheng/easyphotos/utils/uri/UriUtils.java com/jph/takephoto/uitl/TImageFiles.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/meari/base/common/Constant.java com/meari/base/util/CommonUtils.java com/meari/base/util/FileUtil.java com/meari/base/util/LocalLog.java com/meari/base/util/PhotoUtils.java com/meari/base/util/statistic/CrashHandler.java com/meari/base/util/statistic/LogcatHelper.java com/meari/cloudconfig/ConfigUtils.java com/meari/device/hunting/view/HuntPlayBackActivity.java com/meari/sdk/http/convert/FileConvert.java com/meari/sdk/mqtt/AWSMqttService.java com/meari/sdk/utils/LoggerUtil.java com/meari/sdk/utils/SdkUtils.java com/ppstrong/ppsplayer/meariLog.java com/ta/utdid2/b/a/c.java com/tencent/bugly/proguard/ab.java com/tencent/bugly/proguard/as.java com/xiaomi/clientreport/processor/a.java com/xiaomi/clientreport/processor/b.java com/xiaomi/mipush/sdk/u.java com/xiaomi/push/Cdo.java com/xiaomi/push/aa.java com/xiaomi/push/ag.java com/xiaomi/push/bl.java com/xiaomi/push/dj.java com/xiaomi/push/dk.java com/xiaomi/push/dl.java com/xiaomi/push/ef.java com/xiaomi/push/ek.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/xiaomi/push/i.java lib/android/paypal/com/magnessdk/a/a.java lib/android/paypal/com/magnessdk/b.java lib/android/paypal/com/magnessdk/i.java org/eclipse/paho/android/service/MqttConnection.java top/zibin/luban/LubanUtils.java
				com/alibaba/android/arouter/utils/Consts.java com/alibaba/fastjson/JSON.java com/alibaba/fastjson/support/geo/Geometry.java com/amazonaws/auth/CognitoCachingCredentialsProvider.java com/amazonaws/auth/policy/conditions/ConditionFactory.java com/amazonaws/auth/policy/conditions/S3ConditionFactory.java com/amazonaws/cognito/clientcontext/data/UserContextDataProvider.java com/amazonaws/cognito/clientcontext/datacollection/DeviceDataCollector.java com/amazonaws/internal/keyvaluestore/AWSKeyValueStore.java com/amazonaws/internal/keyvaluestore/KeyProvider18.java com/amazonaws/mobile/auth/core/IdentityManager.java com/amazonaws/mobile/client/AWSMobileClient.java com/amazonaws/mobile/client/internal/oauth2/OAuth2Client.java com/amazonaws/mobileconnectors/cognitoidentityprovider/util/CognitoDeviceHelper.java com/amazonaws/mobileconnectors/cognitoidentityprovider/util/CognitoPinpointSharedContext.java com/amazonaws/mobileconnectors/cognitoidentityprovider/util/CognitoServiceConstants.java com/amazonaws/mobileconnectors/iot/AWSIotKeystoreHelper.java com/amazonaws/mobileconnectors/s3/transferutility/TransferObserver.java com/amazonaws/mobileconnectors/s3/transferutility/TransferTable.java com/amazonaws/services/s3/Headers.java com/amazonaws/services/s3/model/S3ObjectSummary.java com/braintreepayments/api/DataCollector.java com/braintreepayments/api/PayPal.java com/braintreepayments/api/PayPalTwoFactorAuthSharedPreferences.java com/braintreepayments/api/UnionPay.java com/braintreepayments/api/Venmo.java com/braintreepayments/api/exceptions/BraintreeError.java com/braintreepayments/api/exceptions/ErrorWithResponse.java com/braintreepayments/api/internal/AnalyticsEvent.java com/braintreepayments/api/internal/AnalyticsSender.java com/braintreepayments/api/internal/BraintreeHttpClient.java com/braintreepayments/api/internal/UUIDHelper.java com/braintreepayments/api/models/AmericanExpressRewardsBalance.java com/braintreepayments/api/models/AnalyticsConfiguration.java com/braintreepayments/api/models/AuthenticationInsight.java com/braintreepayments/api/models/BaseCardBuilder.java com/braintreepayments/api/models/BinData.java com/braintreepayments/api/models/BraintreeApiConfiguration.java com/braintreepayments/api/models/CardBuilder.java com/braintreepayments/api/models/CardConfiguration.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/braintreepayments/api/models/CardNonce.java com/braintreepayments/api/models/ClientToken.java com/braintreepayments/api/models/Configuration.java
5	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/braintreepayments/api/models/GooglePaymentCardNonce.java com/braintreepayments/api/models/GooglePaymentConfiguration.java com/braintreepayments/api/models/KountConfiguration.java com/braintreepayments/api/models/LocalPaymentRequest.java com/braintreepayments/api/models/LocalPaymentResult.java com/braintreepayments/api/models/MetadataBuilder.java com/braintreepayments/api/models/PayPalAccountBuilder.java com/braintreepayments/api/models/PayPalAccountNonce.java com/braintreepayments/api/models/PayPalConfiguration.java com/braintreepayments/api/models/PayPalCreditFinancing.java com/braintreepayments/api/models/PayPalCreditFinancingAmount.java com/braintreepayments/api/models/PayPalPaymentResource.java com/braintreepayments/api/models/PayPalTwoFactorAuthResponse.java com/braintreepayments/api/models/PaymentMethodBuilder.java com/braintreepayments/api/models/PaymentMethodNonce.java com/braintreepayments/api/models/PostalAddressParser.java com/braintreepayments/api/models/SamsungPayConfiguration.java com/braintreepayments/api/models/ThreeDSecureAuthenticationResponse.java com/braintreepayments/api/models/ThreeDSecureInfo.java com/braintreepayments/api/models/ThreeDSecureLookup.java com/braintreepayments/api/models/ThreeDSecurePostalAddress.java com/braintreepayments/api/models/UnionPayCapabilities.java com/braintreepayments/api/models/UnionPayCardBuilder.java com/braintreepayments/api/models/VenmoAccountBuilder.java com/braintreepayments/api/models/VenmoAccountNonce.java com/braintreepayments/api/models/VenmoConfiguration.java com/braintreepayments/api/models/VisaCheckoutNonce.java com/braintreepayments/browserswitch/BrowserSwitchPersistentStore.java com/braintreepayments/browserswitch/PersistentStore.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/manager/RequestManagerRetriever.java com/cloudedge/smarteye/wxapi/WXEntryActivity.java com/dctrain/module_add_device/presenter/AddSeriesTypePresenter.java com/dctrain/module_add_device/presenter/RouterWiFiPresenter.java com/heytap/msp/push/encrypt/AESEncrypt.java com/luck/picture/lib/config/PictureConfig.java com/meari/base/common/CommonFunction.java com/meari/base/common/Config.java com/meari/base/common/StringConstants.java com/meari/base/util/ExampleUtil.java com/meari/base/util/WifiAutoConnectManager.java com/meari/base/util/WifiConnectHelper.java com/meari/base/util/utils/WifiUtil.java com/meari/sdk/common/ArentiServerUrl.java com/meari/sdk/common/IotConstants.java com/meari/sdk/common/ProtocalConstants.java com/meari/sdk/common/ServerUrl.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/meari/sdk/http/cache/CacheEntity.java com/meari/sdk/http/cache/CacheHelper.java com/meari/sdk/mqtt/AWSMqttService.java com/meari/sdk/mqtt/PPMqttService.java com/meari/sdk/utils/MMKVUtil.java com/meari/sdk/utils/SdkUtils.java com/meari/sdk/zxing/decoding/Intents.java com/paypal/android/sdk/onetouch/core/CheckoutRequest.java com/paypal/android/sdk/onetouch/core/PayPalLineItem.java com/ppstrong/weeye/play/CloudShortVideoControlMode.java com/ppstrong/weeye/view/activity/device/VoiceBellCallActivity.java com/ppstrong/weeye/view/activity/message/NewMsgActivity.java com/ppstrong/weeye/view/activity/setting/share/DeviceShareActivity.java com/tencent/mm/opensdk/constants/ConstantsAPI.java com/tencent/mmkv/MMKVContentProvider.java com/uuzuche/lib_zxing/decoding/Intents.java com/vivo/push/model/a.java com/xiaomi/clientreport/data/Config.java com/xiaomi/mipush/sdk/Constants.java io/reactivex/internal/schedulers/SchedulerPoolFactory.java org/conscrypt/OpenSSLECKeyFactory.java org/conscrypt/OpenSSLRSAKeyFactory.java org/eclipse/paho/client/mqttv3/internal/wire/MqttConnack.java org/eclipse/paho/client/mqttv3/internal/wire/MqttConnect.java org/eclipse/paho/client/mqttv3/internal/wire/MqttDisconnect.java org/eclipse/paho/client/mqttv3/internal/wire/MqttPingReq.java org/eclipse/paho/client/mqttv3/internal/wire/MqttPingResp.java rx/internal/schedulers/NewThreadWorker.java
6	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/alibaba/sdk/android/oss/common/utils/BinaryUtil.java com/alipay/security/mobile/module/a/a.java com/alipay/security/mobile/module/a/a/b.java com/alipay/security/mobile/module/a/a/c.java com/amazonaws/mobileconnectors/cognitoidentityprovider/CognitoUser.java com/amazonaws/mobileconnectors/cognitoidentityprovider/util/CognitoDeviceHelper.java com/meari/base/util/AesBtye16Helper.java com/meari/base/util/HmacshaUtil.java com/meari/sdk/utils/HmacshaUtil.java com/ta/utdid2/device/c.java com/tencent/bugly/proguard/ap.java com/xiaomi/push/bd.java com/xiaomi/push/bf.java org/eclipse/paho/client/mqttv3/internal/websocket/WebSocketHandshake.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/alibaba/fastjson/util/AntiCollisionHashMap.java com/alipay/sdk/data/c.java com/alipay/sdk/tid/b.java com/alipay/sdk/util/n.java com/amazonaws/retry/PredefinedRetryPolicies.java com/dctrain/module_add_device/presenter/SmartWiFiPresenter.java com/hjq/permissions/PermissionFragment.java com/meari/sdk/MeariUser.java com/meari/sdk/utils/SdkUtils.java com/paypal/android/sdk/onetouch/core/fpti/FptiManager.java com/paypal/android/sdk/onetouch/core/fpti/FptiToken.java com/ppstrong/weeye/presenter/setting/UpdateDevicePresenter.java com/ppstrong/weeye/view/activity/device/SingleVideoPlayActivity.java com/ta/utdid2/a/a/e.java com/ta/utdid2/device/c.java com/xiaomi/push/bf.java com/xiaomi/push/cd.java com/xiaomi/push/gw.java org/eclipse/paho/client/mqttv3/internal/websocket/WebSocketFrame.java
8	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/alipay/sdk/sys/b.java com/braintreepayments/api/internal/AnalyticsSender.java com/tencent/bugly/proguard/ab.java lib/android/paypal/com/magnessdk/a/b.java lib/android/paypal/com/magnessdk/h.java
9	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/alibaba/sdk/android/oss/common/OSSSQLiteHelper.java com/alipay/sdk/tid/a.java com/amazonaws/mobileconnectors/s3/transferutility/TransferTable.java com/braintreepayments/api/internal/AnalyticsDatabase.java com/danikula/videocache/sourcestorage/DatabaseSourceInfoStorage.java com/meari/base/util/db/AlertMsgDb.java com/meari/base/util/db/CustomerDbHelper.java com/meari/base/util/db/DataBaseManager.java com/meari/base/util/db/OpenHelper.java com/meari/base/util/db/PwdHelper.java com/meari/base/util/db/RecentContactsDb.java com/meari/device/jingle/db/JingleMsgDao.java com/meari/device/jingle/db/JingleMsgDb.java com/meari/sdk/http/cache/CacheHelper.java com/meari/sdk/http/cache/DataBaseDao.java com/tencent/bugly/proguard/o.java com/tencent/bugly/proguard/x.java com/xiaomi/push/providers/a.java org/eclipse/paho/android/service/DatabaseMessageStore.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/alibaba/sdk/android/oss/common/utils/BinaryUtil.java com/amazonaws/services/s3/AmazonS3Client.java com/amazonaws/services/s3/internal/MD5DigestCalculatingInputStream.java com/amazonaws/util/Md5Utils.java com/danikula/videocache/ProxyCacheUtils.java com/luck/picture/lib/loader/SandboxFileLoader.java com/meari/base/util/CommonUtils.java com/meari/base/util/db/DataBaseManager.java com/meari/sdk/UserRequestManager.java com/meari/sdk/utils/Md5.java com/meari/sdk/utils/SdkUtils.java com/tencent/mm/opensdk/utils/b.java com/vivo/push/util/u.java com/xiaomi/push/be.java com/xiaomi/push/bf.java com/xiaomi/push/ct.java
11	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/alibaba/sdk/android/oss/common/utils/HttpdnsMini.java com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java com/alipay/android/phone/mrpc/core/q.java com/danikula/videocache/HttpProxyCacheServer.java com/test/TestNetWorkActivity.java com/vivo/push/BuildConfig.java com/vivo/push/PushClient.java com/xiaomi/push/ae.java com/xiaomi/push/az.java lib/android/paypal/com/magnessdk/a/b.java org/conscrypt/CertificatePriorityComparator.java org/conscrypt/ChainStrengthAnalyzer.java org/conscrypt/EvpMdRef.java org/conscrypt/OAEPParameters.java org/conscrypt/OpenSSLCipherRSA.java org/conscrypt/OpenSSLProvider.java org/conscrypt/OpenSSLSignature.java org/conscrypt/TrustManagerImpl.java org/conscrypt/ct/CTConstants.java
12	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/tencent/bugly/crashreport/CrashReport.java
13	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/amazonaws/iot/BuildConfig.java com/amazonaws/mobile/auth/core/BuildConfig.java com/amazonaws/mobile/client/BuildConfig.java
14	Weak Encryption algorithm used	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/alipay/sdk/encrypt/b.java com/heytap/mcssdk/utils/c.java com/meari/sdk/utils/DesUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
15	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/meari/sdk/utils/DesUtils.java
16	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/huantansheng/easyphotos/ui/EasyPhotosActivity.java com/huantansheng/easyphotos/utils/bitmap/BitmapUtils.java com/huantansheng/easyphotos/utils/file/FileUtils.java com/ppstrong/weeye/presenter/setting/FaceAddPresenter.java com/ppstrong/weeye/presenter/setting/FaceManagePresenter.java com/soundcloud/android/crop/CropUtil.java
17	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/alipay/sdk/tid/b.java com/braintreepayments/browserswitch/PersistentStore.java com/meari/base/util/DevicePreUtil.java
18	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	lib/android/paypal/com/magnessdk/c.java
19	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	com/alipay/android/phone/mrpc/core/b.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libsoundtouch.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	arm64-v8a/libwebrtc_apms.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
3	arm64-v8a/libgpac.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
4	arm64-v8a/libconscrypt_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64-v8a/libppr.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.
6	arm64-v8a/libfaac.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
7	arm64-v8a/libremix.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	arm64-v8a/libmp4wraper.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
9	arm64-v8a/libBugly_Native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
10	arm64-v8a/libmrav.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	arm64-v8a/libmmkv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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', '__memcpy_chk', '__strlen_chk', '__strchr_chk', '__strcat_chk', '__memmove_chk', '__memset_chk', '__read_chk', '__strncpy_chk', '__strcpy_chk']	False warning Symbols are available.
12	arm64-v8a/libcrashlytics.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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']	False warning Symbols are available.
13	arm64-v8a/libppsaudio.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	arm64-v8a/libnative-imagetranscoder.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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']	False warning Symbols are available.
15	arm64-v8a/libhv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.
16	arm64-v8a/libmrble.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	arm64-v8a/libyuv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
18	arm64-v8a/libppsdk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
19	arm64-v8a/libcurl.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	arm64-v8a/libgifimage.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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']	False warning Symbols are available.
21	arm64-v8a/libBugly.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
22	arm64-v8a/libPPCS_API.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	arm64-v8a/libimagepipeline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
24	arm64-v8a/libcrashlytics-handler.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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']	False warning Symbols are available.
25	arm64-v8a/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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: ['__memset_chk', '__memmove_chk', '__strchr_chk', '__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__strlen_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	arm64-v8a/libnative-filters.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
27	arm64-v8a/libIOTCAPIs.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
28	arm64-v8a/libmrplayer.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	arm64-v8a/libAVAPIs.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
30	armeabi-v7a/libsoundtouch.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.
31	armeabi-v7a/libwebrtc_apms.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
32	armeabi-v7a/libgpac.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
33	armeabi-v7a/libconscrypt_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
34	armeabi-v7a/libppr.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
35	armeabi-v7a/libfaac.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
36	armeabi-v7a/libremix.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.
37	armeabi-v7a/libmp4wraper.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
38	armeabi-v7a/libBugly_Native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
39	armeabi-v7a/libmrav.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.
40	armeabi-v7a/libmmkv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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', '__memcpy_chk', '__strlen_chk', '__strchr_chk', '__strcat_chk', '__memmove_chk', '__memset_chk', '__strcpy_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
41	armeabi-v7a/libcrashlytics.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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.
42	armeabi-v7a/libppsaudio.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.
43	armeabi-v7a/libnative-imagetranscoder.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
44	armeabi-v7a/libhv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.
45	armeabi-v7a/libmrble.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.
46	armeabi-v7a/libyuv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
47	armeabi-v7a/libppsdk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
48	armeabi-v7a/libcurl.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.
49	armeabi-v7a/libgifimage.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
50	armeabi-v7a/libBugly.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
51	armeabi-v7a/libPPCS_API.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
52	armeabi-v7a/libimagepipeline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
53	armeabi-v7a/libcrashlytics-handler.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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	armeabi-v7a/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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.
55	armeabi-v7a/libnative-filters.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
56	armeabi-v7a/libIOTCAPIs.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
57	armeabi-v7a/libmrplayer.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.
58	armeabi-v7a/libAVAPIs.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
59	arm64-v8a/libsoundtouch.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.
60	arm64-v8a/libwebrtc_apms.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
61	arm64-v8a/libgpac.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
62	arm64-v8a/libconscrypt_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
63	arm64-v8a/libppr.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.
64	arm64-v8a/libfaac.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
65	arm64-v8a/libremix.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
66	arm64-v8a/libmp4wraper.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
67	arm64-v8a/libBugly_Native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
68	arm64-v8a/libmrav.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.
69	arm64-v8a/libmmkv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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', '__memcpy_chk', '__strlen_chk', '__strchr_chk', '__strcat_chk', '__memmove_chk', '__memset_chk', '__read_chk', '__strncpy_chk', '__strcpy_chk']	False warning Symbols are available.
70	arm64-v8a/libcrashlytics.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
71	arm64-v8a/libppsaudio.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.
72	arm64-v8a/libnative-imagetranscoder.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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']	False warning Symbols are available.
73	arm64-v8a/libhv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
74	arm64-v8a/libmrble.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.
75	arm64-v8a/libyuv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
76	arm64-v8a/libppsdk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
77	arm64-v8a/libcurl.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.
78	arm64-v8a/libgifimage.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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']	False warning Symbols are available.
79	arm64-v8a/libBugly.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
80	arm64-v8a/libPPCS_API.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
81	arm64-v8a/libimagepipeline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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	arm64-v8a/libcrashlytics-handler.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
83	arm64-v8a/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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: ['__memset_chk', '__memmove_chk', '__strchr_chk', '__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__strlen_chk']	False warning Symbols are available.
84	arm64-v8a/libnative-filters.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
85	arm64-v8a/libIOTCAPIs.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
86	arm64-v8a/libmrplayer.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.
87	arm64-v8a/libAVAPIs.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
88	armeabi-v7a/libsoundtouch.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
89	armeabi-v7a/libwebrtc_apms.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
90	armeabi-v7a/libgpac.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
91	armeabi-v7a/libconscrypt_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
92	armeabi-v7a/libppr.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.
93	armeabi-v7a/libfaac.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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	armeabi-v7a/libremix.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
95	armeabi-v7a/libmp4wraper.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.
96	armeabi-v7a/libBugly_Native.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
97	armeabi-v7a/libmrav.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
98	armeabi-v7a/libmmkv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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', '__memcpy_chk', '__strlen_chk', '__strchr_chk', '__strcat_chk', '__memmove_chk', '__memset_chk', '__strcpy_chk']	False warning Symbols are available.
99	armeabi-v7a/libcrashlytics.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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.
100	armeabi-v7a/libppsaudio.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
101	armeabi-v7a/libnative-imagetranscoder.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
102	armeabi-v7a/libhv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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.
103	armeabi-v7a/libmrble.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
104	armeabi-v7a/libyuv.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
105	armeabi-v7a/libppsdk.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
106	armeabi-v7a/libcurl.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
107	armeabi-v7a/libgifimage.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
108	armeabi-v7a/libBugly.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
109	armeabi-v7a/libPPCS_API.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
110	armeabi-v7a/libimagepipeline.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
111	armeabi-v7a/libcrashlytics-handler.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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.
112	armeabi-v7a/libcrashlytics-common.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	No RELRO high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
113	armeabi-v7a/libnative-filters.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
114	armeabi-v7a/libIOTCAPIs.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.
115	armeabi-v7a/libmrplayer.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
116	armeabi-v7a/libAVAPIs.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	16/24	android.permission.ACCESS_NETWORK_STATE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.RECORD_AUDIO, android.permission.READ_PHONE_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.WRITE_SETTINGS, android.permission.INTERNET, android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.READ_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.GET_TASKS
Other Common Permissions	13/45	android.permission.BLUETOOTH, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.ACCESS_NOTIFICATION_POLICY, android.permission.ACCESS_LOCATION_EXTRA_COMMANDS, android.permission.CHANGE_NETWORK_STATE, android.permission.CHANGE_WIFI_STATE, android.permission.FLASHLIGHT, android.permission.FOREGROUND_SERVICE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.BLUETOOTH_ADMIN

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
open.weixin.qq.com	IP: 203.205.232.110 Country: China Region: Guangdong City: Shenzhen
android.bugly.qq.com	IP: 129.226.103.217 Country: Hong Kong Region: Hong Kong City: Hong Kong
oss-cn-hangzhou.aliyuncs.com	IP: 118.31.219.236 Country: China Region: Zhejiang City: Hangzhou
cschat-ccs.aliyun.com	IP: 140.205.60.46 Country: China Region: Zhejiang City: Hangzhou
long.open.weixin.qq.com	IP: 109.244.216.15 Country: China Region: Beijing City: Beijing
develop.meari.com.cn	IP: 47.97.155.107 Country: China Region: Zhejiang City: Hangzhou
api.weixin.qq.com	IP: 43.129.2.204 Country: China Region: Beijing City: Beijing
apis-cn-hangzhou.meari.com.cn	IP: 47.110.186.157 Country: China Region: Zhejiang City: Hangzhou

DOMAIN	COUNTRY/REGION
meari-hz-pre.oss-cn-hangzhou.aliyuncs.com	IP: 118.31.232.217 Country: China Region: Zhejiang City: Hangzhou
mobilegw.alipay.com	IP: 205.204.122.81 Country: Hong Kong Region: Hong Kong City: Hong Kong
47.110.186.157	IP: 47.110.186.157 Country: China Region: Zhejiang City: Hangzhou
oss.aliyuncs.com	IP: 118.178.29.5 Country: China Region: Zhejiang City: Hangzhou
www.baidu.com	IP: 103.235.47.103 Country: Hong Kong Region: Hong Kong City: Hong Kong
pre-apis.meari.com.cn	IP: 121.40.191.136 Country: China Region: Zhejiang City: Hangzhou
www.meari.com.cn	IP: 47.89.50.193 Country: Hong Kong Region: Hong Kong City: Hong Kong
m.alipay.com	IP: 110.76.30.76 Country: China Region: Zhejiang City: Hangzhou
h.trace.qq.com	IP: 129.226.102.234 Country: Hong Kong Region: Hong Kong City: Hong Kong

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
47.91.65.244	ok	**IP:** 47.91.65.244 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
api-m.sandbox.paypal.com	ok	**IP:** 199.232.53.35 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
apis-eu-frankfurt.meari.com.cn	ok	**IP:** 3.127.202.130 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
assets.staging.braintreepayments.com	ok	**IP:** 184.105.254.110 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.850029 **Longitude:** -87.650047 **View:** Google Map
xmlpull.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
meari-us.s3.us-west-1.amazonaws.com	ok	**IP:** 52.219.116.233 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
open.weixin.qq.com	ok	**IP:** 203.205.232.110 **Country:** China **Region:** Guangdong **City:** Shenzhen **Latitude:** 22.545540 **Longitude:** 114.068298 **View:** Google Map
upload.ffmpeg.org	ok	**IP:** 213.36.253.119 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map
api.xmpush.xiaomi.com	ok	**IP:** 20.47.97.231 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
api-m.paypal.com	ok	**IP:** 199.232.53.35 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.paypal.com	ok	**IP:** 66.211.168.123 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.385639 **Longitude:** -121.885277 **View:** Google Map
uri.paypal.com	ok	No Geolocation information available.
image.cnamedomain.com	ok	No Geolocation information available.
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	**IP:** 216.58.204.68 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ru.register.xmpush.global.xiaomi.com	ok	**IP:** 20.47.97.231 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
mobilegw.aaa.alipay.net	ok	No Geolocation information available.
www.stage2du13.stage.paypal.com	ok	**IP:** 34.67.10.182 **Country:** United States of America **Region:** Iowa **City:** Council Bluffs **Latitude:** 41.261940 **Longitude:** -95.860832 **View:** Google Map
android.bugly.qq.com	ok	**IP:** 129.226.103.217 **Country:** Hong Kong **Region:** Hong Kong **City:** Hong Kong **Latitude:** 22.285521 **Longitude:** 114.157692 **View:** Google Map
www.slf4j.org	ok	**IP:** 159.100.250.151 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
crashpad.chromium.org	ok	**IP:** 142.250.187.211 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
oss-cn-hangzhou.aliyuncs.com	ok	**IP:** 118.31.219.236 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
audio.meari.com.cn	ok	**IP:** 47.91.95.246 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
resolver.msg.xiaomi.net	ok	**IP:** 3.65.189.43 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
47.254.52.55	ok	**IP:** 47.254.52.55 **Country:** United States of America **Region:** California **City:** San Mateo **Latitude:** 37.547424 **Longitude:** -122.330589 **View:** Google Map
www.jivesoftware.com	ok	**IP:** 23.235.209.143 **Country:** United States of America **Region:** California **City:** El Segundo **Latitude:** 33.922234 **Longitude:** -118.405518 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.msmaster.qa.paypal.com	ok	No Geolocation information available.
static-us.s3.us-west-2.amazonaws.com	ok	**IP:** 3.5.80.15 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
cschat-ccs.aliyun.com	ok	**IP:** 140.205.60.46 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
apis-us-west.meari.com.cn	ok	**IP:** 18.118.60.199 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
mclient.alipay.com	ok	**IP:** 163.181.154.238 **Country:** United States of America **Region:** California **City:** San Mateo **Latitude:** 37.547424 **Longitude:** -122.330589 **View:** Google Map
mobilegw.alipaydev.com	ok	**IP:** 198.11.186.9 **Country:** United States of America **Region:** California **City:** San Mateo **Latitude:** 37.547424 **Longitude:** -122.330589 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
long.open.weixin.qq.com	ok	**IP:** 109.244.216.15 **Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map
static-eus.s3.eu-central-1.amazonaws.com	ok	**IP:** 52.219.170.14 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
develop.meari.com.cn	ok	**IP:** 47.97.155.107 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
api.weixin.qq.com	ok	**IP:** 43.129.2.204 **Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
s3.amazonaws.com	ok	**IP:** 16.182.37.72 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developers.braintreepayments.com	ok	**IP:** 199.232.53.21 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
checkout.paypal.com	ok	**IP:** 192.229.221.25 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.034081 **Longitude:** -77.488503 **View:** Google Map
www.isiwi.it	ok	**IP:** 86.107.36.11 **Country:** Italy **Region:** Lazio **City:** Cassino **Latitude:** 41.487621 **Longitude:** 13.831510 **View:** Google Map
schemas.xmlsoap.org	ok	**IP:** 13.107.213.64 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
www.ffmpeg.org	ok	**IP:** 79.124.17.100 **Country:** Bulgaria **Region:** Sofia (stolitsa) **City:** Sofia **Latitude:** 42.697510 **Longitude:** 23.324150 **View:** Google Map
www.paypalobjects.com	ok	**IP:** 192.229.221.25 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.034081 **Longitude:** -77.488503 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
s3-us-west-1.amazonaws.com	ok	**IP:** 52.219.220.168 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.amazon.com	ok	**IP:** 13.224.73.178 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Manchester **Latitude:** 53.480949 **Longitude:** -2.237430 **View:** Google Map
apis.cloudedge360.com	ok	**IP:** 52.29.42.85 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
mcgw.alipay.com	ok	**IP:** 79.133.176.237 **Country:** Russian Federation **Region:** Omskaya oblast' **City:** Omsk **Latitude:** 55.000000 **Longitude:** 73.400002 **View:** Google Map
apis-cn-hangzhou.meari.com.cn	ok	**IP:** 47.110.186.157 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
www.openssl.org	ok	**IP:** 34.36.58.177 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
meari-hz-pre.oss-cn-hangzhou.aliyuncs.com	ok	**IP:** 118.31.232.217 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
127.0.0.1	ok	**IP:** 127.0.0.1 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
cloudedge-5d659.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
mobilegw.alipay.com	ok	**IP:** 205.204.122.81 **Country:** Hong Kong **Region:** Hong Kong **City:** Hong Kong **Latitude:** 22.285521 **Longitude:** 114.157692 **View:** Google Map
cn.register.xmpush.xiaomi.com	ok	**IP:** 20.47.97.231 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
gpac.io	ok	**IP:** 109.234.164.247 **Country:** France **Region:** Auvergne-Rhone-Alpes **City:** Clermont-Ferrand **Latitude:** 45.779659 **Longitude:** 3.086280 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
mobilegw-1-64.test.alipay.net	ok	No Geolocation information available.
mobilegw.stable.alipay.net	ok	No Geolocation information available.
api.sandbox.braintreegateway.com	ok	**IP:** 76.223.15.98 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
c.sandbox.paypal.com	ok	**IP:** 199.232.53.21 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
wappaygw.alipay.com	ok	**IP:** 79.133.176.236 **Country:** Russian Federation **Region:** Omskaya oblast' **City:** Omsk **Latitude:** 55.000000 **Longitude:** 73.400002 **View:** Google Map
b.stats.paypal.com	ok	**IP:** 34.147.177.40 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
47.110.186.157	ok	**IP:** 47.110.186.157 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
astat.bugly.cros.wr.pvp.net	ok	**IP:** 170.106.118.26 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
api.braintreegateway.com	ok	**IP:** 76.223.13.31 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
idmb.register.xmpush.global.xiaomi.com	ok	**IP:** 20.47.97.231 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
www.ngs.ac.uk	ok	**IP:** 130.246.140.235 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Appleton **Latitude:** 51.709511 **Longitude:** -1.361360 **View:** Google Map
play.google.com	ok	**IP:** 172.217.169.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
astat.bugly.qcloud.com	ok	**IP:** 119.28.121.133 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
register.xmpush.global.xiaomi.com	ok	**IP:** 20.47.97.231 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
oss.aliyuncs.com	ok	**IP:** 118.178.29.5 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
www.baidu.com	ok	**IP:** 103.235.47.103 **Country:** Hong Kong **Region:** Hong Kong **City:** Hong Kong **Latitude:** 22.285521 **Longitude:** 114.157692 **View:** Google Map
oss-cn-.aliyuncs.comor	ok	No Geolocation information available.
pre-apis.meari.com.cn	ok	**IP:** 121.40.191.136 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.onvif.org	ok	**IP:** 190.92.159.115 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
api.sandbox.paypal.com	ok	**IP:** 173.0.93.150 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.385639 **Longitude:** -121.885277 **View:** Google Map
c.paypal.com	ok	**IP:** 199.232.53.21 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
h5.m.taobao.com	ok	**IP:** 79.133.176.233 **Country:** Russian Federation **Region:** Omskaya oblast' **City:** Omsk **Latitude:** 55.000000 **Longitude:** 73.400002 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.meari.com.cn	ok	**IP:** 47.89.50.193 **Country:** Hong Kong **Region:** Hong Kong **City:** Hong Kong **Latitude:** 22.285521 **Longitude:** 114.157692 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
download.tsi.telecom-paristech.fr	ok	**IP:** 137.194.2.87 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map
static-sgs.s3.ap-southeast-1.amazonaws.com	ok	**IP:** 52.219.125.19 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
m.alipay.com	ok	**IP:** 110.76.30.76 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
dashif.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
fr.register.xmpush.global.xiaomi.com	ok	**IP:** 3.75.3.160 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
new.api.ad.xiaomi.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
h.trace.qq.com	ok	**IP:** 129.226.102.234 **Country:** Hong Kong **Region:** Hong Kong **City:** Hong Kong **Latitude:** 22.285521 **Longitude:** 114.157692 **View:** Google Map
apis.meari.com.cn	ok	**IP:** 3.127.202.130 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
acs.amazonaws.com	ok	No Geolocation information available.

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://cloudedge-5d659.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
support@wgvtech.com	com/ppstrong/weeye/presenter/user/CustomerServicePresenterImpl.java
danikula@gmail.com	com/danikula/videocache/HttpUrlSource.java
cloudedge@meari.com	com/meari/device/hunting/view/ContactUSActivity.java
nsupport@meari.com support@meari.com supporto@isiwi.it info@vultech.it	com/meari/base/common/PolicyUtils.java

EMAIL	FILE
support@meari.com	com/meari/base/common/CommonFunction.java
support@meari.com	Android String Resource
appro@openssl.org	lib/arm64-v8a/libconscrypt_jni.so
ftp@example.com	lib/arm64-v8a/libcurl.so
ffmpeg-devel@ffmpeg.org	lib/arm64-v8a/libmrplayer.so
ftp@example.com	lib/armeabi-v7a/libcurl.so
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libmrplayer.so
appro@openssl.org	apktool_out/lib/arm64-v8a/libconscrypt_jni.so
ftp@example.com	apktool_out/lib/arm64-v8a/libcurl.so
ffmpeg-devel@ffmpeg.org	apktool_out/lib/arm64-v8a/libmrplayer.so
ftp@example.com	apktool_out/lib/armeabi-v7a/libcurl.so
ffmpeg-devel@ffmpeg.org	apktool_out/lib/armeabi-v7a/libmrplayer.so

TRACKERS

TRACKER	CATEGORIES	URL
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"add_input_onvif_pwd" : "OnVIF□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"device_cloud_storage_desc_key" : "□□□□□"
"traffic_in_user" : "□□□□□□□□□□□□□□□□□"
"com_device_pwd_tip" : "□□□□□□□□□□□□□□□□□□□□□"
"device_cloud_storage_desc_key" : "□□□□□"
"com_facebook_device_auth_instructions" : "□□facebook.com/device□□□□□□□□□□□□□□"
"device_setting_user" : "User"
"tip_valid_pwd" : "□□□□□□□□□□□□□2□□□□□□□□□□□□□□□□□□□□□□8-16□"
"device_setting_video_encryption_wrong_pwd" : "□□□□□□□□□□□□□"
"device_setting_video_encryption_pwd" : "□□□□□"
"user_remember_password" : "□□□□□"
"device_enter_preview_pwd" : "□□□□□□□□□□□□□□□□"
"toast_onvif_pwd_length" : "□□□□□□0-16□"
"device_bind_other_user" : "□□□□□□□□□□□□□□□□□□"
"device_setting_video_encryption_pwd_again" : "□□□□□□□"
"toast_null_password" : "□□□□□□□"
"device_pwd" : "□□□□□"
"add_input_onvif_pwd" : "□□□onvif□□□□"
"device_setting_video_encryption_pwd_again" : "□□□□□□□□□□□□□□□□□□□□"
"device_set_pwd" : "□□□□□"

POSSIBLE SECRETS
"wifi_no_pwd" : "□□WiFi"
"device_setting_video_encryption_pwd" : "□□□□□□□□□□□□□□□□"
"user_password" : "□□"
"device_setting_user" : "Eigenaar"
"device_pwd" : "Apparaatcryptie"
"add_input_onvif_pwd" : "□□□onvif□□□□"
"com_pwd_onvif" : "□□□□□□□ONVIF□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"toast_onvif_pwd_length" : "□□□□□□□□□□16□□□□□□□□□□□□"
"device_reset_pwd" : "□□□□□□□"
"user_password" : "Wachtwoord"
"tip_valid_pwd" : "□□□□□8-16□□□□□□□□□□□□□□□□□□□□□□"
"user_password" : "Passwort"
"device_setting_video_encryption_pwd_again" : "□□□□□□□"
"traffic_in_user" : "□□□□□□□□"
"device_cloud_storage_desc_key" : "Servicevoorwaarden"
"device_setting_user" : "Utente"
"device_setting_wifi_password" : "WIFI□□"
"add_show_password" : "□□□□"
"user_password" : "Senha"
"device_setting_poweron_password" : "□□□□□□□□"
"device_setting_poweronpassword" : "□□□□□□□□"

POSSIBLE SECRETS
"device_setting_wifi_password" : "WiFi□□□□□□"
"com_device_pwd_tip" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"device_setting_poweron_password" : "□□□□"
"user_remember_password" : "□□□□"
"device_setting_user" : "□□□"
"user_remember_password" : "□□□□□□□□□"
"google_crash_reporting_api_key" : "AIzaSyASz7Fo4491jy1gfdEiga6PXGF2qMpvPpQ"
"com_device_pwd_tip" : "□□□□□□□□□□□□□□□□□□"
"com_wifi_pwd_check" : "□□□□□□□"
"device_pwd" : "□□□□"
"device_setting_user" : "Proprietário"
"facebook_client_token" : "0e17df3232aa2d5610135ffc9cb2d5db"
"com_wifi_pwd_check" : "□□□□"
"device_reset_pwd" : "□□□□□□□□□□□□□□□□□□□□"
"user_reset_password" : "□□□□□□□□□□□□"
"device_setting_user" : "Użytkwonik"
"device_setting_user" : "□□□"
"device_setting_video_encryption_enter_pwd" : "□□□□"
"com.google.firebase.crashlytics.mapping_file_id" : "00000000000000000000000000000000"
"device_setting_tip_valid_pwd" : "□□□□□□□□4-16□A-Z□A-Z"
"tip_two_pwd_not_same" : "□□□□□□Retype□□□□□□□□□□□□□"

POSSIBLE SECRETS
"device_setting_user" : "Propietario"
"toast_null_password" : "□□□□□□□□□□□□□□□□□□□□"
"device_setting_user" : "Propriétaire"
"device_set_pwd" : "□□□□□□□□□□□□□□□□"
"toast_null_password" : "□□□□□□□"
"user_password" : "Пароль"
"device_enter_preview_pwd" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"add_show_password" : "□□□□□□□□□□□□"
"device_setting_video_encryption_enter_pwd" : "□□□□□□□□□□□□"
"com_wifi_pwd_check" : "□□□□"
"device_cloud_storage_desc_key" : "□□□□"
"user_reset_password" : "□□□□"
"device_enter_preview_pwd" : "□□□□□□□□□□□□□□□□"
"device_reset_pwd" : "□□□□□□□"
"tip_two_pwd_not_same" : "□□□□□□□□"
"device_setting_poweronpassword" : "□□□□□□□"
"device_setting_tip_valid_pwd" : "□□□□□4-16□a-z□A-Z"
"device_setting_poweronpassword" : "□□□□□□□"
"device_bind_other_user" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"toast_onvif_pwd_length" : "□□□□□0-16□"
"tip_two_pwd_not_same" : "□□□□□□□□"

POSSIBLE SECRETS
"user_password" : "Password"
"device_setting_wifi_password" : "WIFI□□"
"user_password" : "□□□□□"
"com_pwd_onvif" : "□□□□□□□□□□□□□□□onvif□□"
"user_password" : "Hasło"
"device_set_pwd" : "□□□□"
"device_setting_user" : "Пользователь"
"com_pwd_onvif" : "□□□□□□□□□□□□□□□onvif□□"
"google_api_key" : "AIzaSyASz7Fo4491jy1gfdEiga6PXGF2qMpvPpQ"
"device_cloud_storage_desc_key" : "Nutzungsbedingungen"
"com_facebook_device_auth_instructions" : "facebook.com/device□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"user_password" : "□□"
"device_setting_video_encryption_wrong_pwd" : "□□□□□□□□□□□□□□□□□□□□□□□"
"add_show_password" : "□□□□"
"device_setting_video_encryption_enter_pwd" : "□□□□"
"device_setting_tip_valid_pwd" : "□□□□□4-16□a-z□A-Z"
"com_wifi_pwd_check" : "Kennwortprüfung"
"device_pwd" : "Geräteverschlüsselung."
"device_setting_video_encryption_wrong_pwd" : "□□□□□□□□□□□□"
"device_setting_user" : "Uživatel"
"firebase_database_url" : "https://cloudedge-5d659.firebaseio.com"

POSSIBLE SECRETS
"user_reset_password" : "□□□□"
"device_setting_video_encryption_pwd" : "□□□□"
"device_setting_poweron_password" : "□□□□"
"device_setting_user" : "Konto"
"tip_valid_pwd" : "□□□□□8-16□□□□□□□□□□□□□□□□□□□□□□□□"
"com_wifi_pwd_check" : "Wachtwoordverificatie"
"user_password" : "Heslo"
"device_pwd" : "□□□□□□□□"
"device_bind_other_user" : "□□□□□□□□□□□□□□□□□"
"device_setting_poweron_password" : "Power-on-wachtwoord"
b70e0cbd6bb4bf7f321390b94a03c1d356c21122343280d6115c1d21
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
470fa2b4ae81cd56ecbcda9735803434cec591fa
Y29tLm1jcy5hY3Rpb24uUkVDRUlWRV9TREtfTUVTU0FHRQ==
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
51953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

POSSIBLE SECRETS
QrMgt8GGYI6T52ZY5AnhtxkLzb8egpFn3j5JELI8H6wtACbUnZ5cc3aYTsTRbmkAkRJeYbtx92LPBWm7nBO9UIl7y5i5MQNmUZNf5QENurR5tGyo7yJ2G0MBjWvy6iAtlAbacKP0SwOUeUWx5dsBdyhxa7Id1APtybSdDgicBDuNjI0mlZFUzZSS9dmN8lBD0WTVOMz0pRZbR3cysomRXOO1ghqjJdTcyDIxzpNAEszN8RMGjrzyU7Hjbmwi6YNK
9b8f518b086098de3d77736f9458a3d2f6f95a37
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
bc29be30292a4309877807e101afbd51
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
b6cbad6cbd5ed0d209afc69ad3b7a617efaae9b3c47eabe0be42d924936fa78c8001b1fd74b079e5ff9690061dacfa4768e981a526b9ca77156ca36251cf2f906d105481374998a7e6e6e18f75ca98b8ed2eaf86ff402c874cca0a263053f22237858206867d210020daa38c48b20cc9dfd82b44a51aeb5db459b22794e2d649
db642562724de5aea559c8e1e82f1ef9
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
e6b1bdcb890370f2f2419fe06d0fdf7628ad0083d52da1ecfe991164711bbf9297e75353de96f1740695d07610567b1240549af9cbd87d06919ac31c859ad37ab6907c311b4756e1e208775989a4f691bff4bbbc58174d2a96b1d0d970a05114d7ee57dfc33b1bafaf6e0d820e838427018b6435f903df04ba7fd34d73f843df9434b164e0220baabb10c8978c3f4c6b7da79d8220a968356d15090dea07df9606f665cbec14d218dd3d691cce2866a58840971b6a57b76af88b1a65fdffd2c080281a6ab20be5879e0330eb7ff70871ce684e7174ada5dc3159c461375a0796b17ce7beca83cf34f65976d237aee993db48d34a4e344f4d8b7e99119168bdd7
b77158d5dfa2f933de42e6f9c6b6b537
b4050a850c04b3abf54132565044b0b7d7bfd8ba270b39432355ffb4
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DDBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A93AD2CAFFFFFFFFFFFFFFFF
013602400437880159360205O5
UHk4V0M5OGdoMzFzakFHa3J3bGtxb1VrTUxMdk5jY0Q
cc2751449a350f668590264ed76692694a80308a
515d6767-01b7-49e5-8273-c8d11b0f331d
35a69fd1-6527-4566-b190-921f9a651488

POSSIBLE SECRETS
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
bef4b5c3ab2204fbaf0a60eb456e9234
bd376388b5f723fb4c22dfe6cd4375a05a07476444d5819985007e34
BCC35D4D3606F154F0402AB7634E8490C0B244C2675C3C6238986987024F0C02
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
308202eb30820254a00302010202044d36f7a4300d06092a864886f70d01010505003081b9310b3009060355040613023836311230100603550408130947756 16e67646f6e673111300f060355040713085368656e7a68656e31353033060355040a132c54656e63656e7420546563686e6f6c6f6779285368656e7a68656e2920436f6d70616e79204c696d69746564313a3038060355040b133154656e63656e74204775616e677a686f752052657365617263682061 6e64204 46576656c6f706d656e742043656e7465723110300e06035504031307546 56e63656e74301e170d313130313139313433393332 5a170d343130313131313433393332 5a3081b9310b3009060355040613023836311230100603550408 13094775616e67646f6e673111300f060355040713085368656e7a68656e31353033060355040a132c54656e63656e7420546563686e6f6c6f6779285368656e7a68656e2920436f6d70616e79204c696d69746564313a3038060355040 b133154656e63656e74204775616e677a686f752052657365617263682061 6e6420446576656c6f706d656e742043656e7465723110300e06035504031307546 56e63656e7430819f300d06092a864886f70d010101050003818d00308 18902818100c05f34b231b083fb1323670bfbe7bdab40c0c0a6efc87ef2072a1ff0d60cc67c8edb0d0847f210bea6cbfaa241be70c86daf56be08b723c859e52428a064555d80db448cdcacc1aea2501eba06f8bad12a4fa49d85cacd7abeb6 8945a5cb5e061629b52e3254c373550ee4e40cb7c8ae6f7a8151ccd8df582d446f39ae0c5e930203010001300d06092a864886f70d01010505000381810 09c8d9d7f2f908c42081b4c764c377109a8b2c70582422125ce545842d5f520aea 69550b6bd8bfd94e987b75a3077eb04ad341f481aac266e89d3864456e69fba13df018acdc168b9a19dfd7ad9d9cc6f6ace57c746515f71234df3a053e33ba93ece5cd0fc15f3e389a3f365588a9fcb439e069d3629cd7732a13fff7b891499
c56fb7d591ba6704df047fd98f535372fea00211

PLAYSTORE INFORMATION

Title: CloudEdge

Score: 4.3784018 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Lifestyle **Play Store URL:** com.cloudedge.smarteye

Developer Details: Hangzhou Meari Technology Co., Ltd., Hangzhou+Meari+Technology+Co.,+Ltd., No. 768 Jiang Hong Road, Binjiang, Hangzhou, China, None, support@mearitek.com,

Release Date: Nov 23, 2017 **Privacy Policy:** Privacy link

Description:

Meanwhile you will received the instant push message via "CloudEdge" alarm system once the motion detected, so you can do accordingly for the safety protection measures.Your family and enterprise be with you, wherever you are.The main function: 1. Real video playing 2. Playback image checking 3. Time & message reminding 4. Share the video image

---

Report Generated by - MobSF v3.9.4 Beta

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.

© 2024 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.