ANDROID STATIC ANALYSIS REPORT

RTRT.me (8.0.4)

File Name:	me.rtrt.app2_804000160.apk
Package Name:	me.rtrt.app2
Scan Date:	Sept. 1, 2025, 2:30 p.m.

App Security Score:	52/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
3	19	4	3	2

FILE INFORMATION

File Name: me.rtrt.app2_804000160.apk
Size: 14.89MB
MD5: 104a0a7a97803041c6eb40d516bffa17
SHA1: def3a59a5763921a2c0499548180c350601e48d0
SHA256: 0da4733c2d2c6a6efcb880d809ce64e3d9c5e1daf96280f0416f856b1f3cedff

APP INFORMATION

App Name: RTRT.me
Package Name: me.rtrt.app2
Main Activity: me.rtrt.app2.MainActivity
Target SDK: 34
Min SDK: 22
Max SDK:
Android Version Name: 8.0.4
Android Version Code: 804000160

APP COMPONENTS

Activities: 10
Services: 18
Receivers: 20
Providers: 7
Exported Activities: 2
Exported Services: 3
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: CN=Jeremy Dill
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-11-12 16:34:36+00:00
Valid To: 2064-10-30 16:34:36+00:00
Issuer: CN=Jeremy Dill
Serial Number: 0x54638c1c

```
Hash Algorithm: sha1
md5: 70158b04f7272969df7c2915d473e462
sha1: 011b23fbc997c565632c6a66c58992610e08aed3
sha256: cd6be1ea321750ae5e9b8ae6dc6bd8760b5f8f6c9d0dd71c3e9f2f17dbe3bb7f
sha512: dd23442ee57a7c19cde6cee7bb65cdc895266bd0d8568d5aac699f4a1c69099307d4ece506423a3ee9153e1f48d8162c93d5dc7f75634014b9bf0a2cd9985408
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 2878395918a0cfe558c7c75a8978897a6621c42073ea3564e28a792f7ab5c4f9
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.
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_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications

PERMISSION	STATUS	INFO	DESCRIPTION
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.
com.huawei.permission.external_app_settings.USE_COMPONENT	signature	permission specific to Huawei devices	It is used to grant apps the ability to access certain system-level features or components that are otherwise restricted for security reasons. This permission ensures that only trusted applications can interact with sensitive parts of the Huawei system.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
me.rtrt.app2.permission.PushHandlerActivity	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
com.huawei.hms.permission.ACTIVITY_RECOGNITION	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE_HEALTH	normal	enables foreground services with health-related functionality.	Allows a regular application to use Service.startForeground with the type "health".

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".
oppo.permission.OPPO_COMPONENT_SAFE	signature	permission specific to OPPO devices	It is used to grant apps the ability to access certain system-level features or components that are otherwise restricted for security reasons. This permission ensures that only trusted applications can interact with sensitive parts of the OPPO system.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
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.
me.rtrt.app2.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference
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.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.BOARD check
possible Build.SERIAL check
SIM operator check
ro.kernel.qemu check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS	
	FINDINGS	DETAILS
classes2.dex	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible Build.SERIAL check Build.TAGS check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8 without marker (suspicious)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
me.rtrt.app2.MainActivity	Schemes: rtrtme://, https://, Hosts: rtrt.me, Path Prefixes: /ulink/_RT/,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **2** | INFO: **1**

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

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.1-5.1.1, [minSdk=22]	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	Broadcast Receiver (nl.xservices.plugins.ShareChooserPendingIntent) 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.
3	Activity (com.adobe.phonegap.push.PushHandlerActivity) is Protected by a permission. Permission: me.rtrt.app2.permission.PushHandlerActivity protectionLevel: signature [android:exported=true]	info	An Activity is found to be exported, but is protected by permission.
4	Activity (com.adobe.phonegap.push.BackgroundHandlerActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: me.rtrt.app2.permission.BackgroundHandlerActivity [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. 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.
5	Service (com.adobe.phonegap.push.FCMService) 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.
6	Activity (com.transistorsoft.locationmanager.activity.TSLocationManagerActivity) 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
7	Service (com.transistorsoft.tsbackgroundfetch.FetchJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
8	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.
9	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
10	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ch/qos/logback/classic/android/LogcatAppender.java ch/qos/logback/classic/net/SimpleSocketServer.java ch/qos/logback/classic/pattern/TargetLengthBasedClassNameAbbreviator.java ch/qos/logback/classic/spi/ThrowableProxy.java ch/qos/logback/core/joran/util/ConfigurationWatchListUtil.java ch/qos/logback/core/net/DefaultSocketConnector.java ch/qos/logback/core/net/SocketConnectorBase.java ch/qos/logback/core/recovery/ResilientOutputStreamBase.java ch/qos/logback/core/spi/ContextAwareBase.java ch/qos/logback/core/spi/ContextAwareImpl.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ch/qos/logback/core/subst/Node.java com/adobe/phonegap/push/BackgroundActionButtonHandler.java com/adobe/phonegap/push/BackgroundHandlerActivity.java com/adobe/phonegap/push/FCMService.java com/adobe/phonegap/push/PushDismissedHandler.java com/adobe/phonegap/push/PushHandlerActivity.java com/adobe/phonegap/push/PushPlugin.java com/applurk/nativetimer/NativeTimerAdapterImpl.java com/customtabplugin/ChromeCustomTabPlugin.java com/darktalker/cordova/screenshot/Screenshot.java com/huawei/agconnect/AGConnectInstance.java com/huawei/agconnect/config/impl/Utils.java com/huawei/agconnect/config/impl/c.java com/huawei/agconnect/config/impl/e.java com/huawei/agconnect/config/impl/h.java com/huawei/agconnect/config/impl/k.java com/huawei/agconnect/core/a/b.java com/huawei/agconnect/core/a/c.java com/huawei/agconnect/core/a/d.java com/huawei/agconnect/core/provider/AGConnectInitializeProvider.java com/huawei/hmf/tasks/a/g.java com/huawei/hms/activity/BridgeActivity.java com/huawei/hms/activity/ForegroundBusDelegate.java com/huawei/hms/activity/internal/ForegroundInnerHeader.java com/huawei/hms/adapter/AvailableAdapter.java com/huawei/hms/adapter/BaseAdapter.java com/huawei/hms/adapter/BinderAdapter.java com/huawei/hms/adapter/InnerBinderAdapter.java com/huawei/hms/adapter/OuterBinderAdapter.java com/huawei/hms/adapter/ui/BaseResolutionAdapter.java com/huawei/hms/adapter/ui/NotInstalledHmsAdapter.java com/huawei/hms/adapter/ui/UpdateAdapter.java com/huawei/hms/android/HwBuildEx.java com/huawei/hms/android/SystemUtils.java com/huawei/hms/api/BindingFailedResolution.java com/huawei/hms/api/FailedBinderCallBack.java com/huawei/hms/api/HuaweiApiClientImpl.java com/huawei/hms/api/HuaweiMobileServicesUtil.java com/huawei/hms/api/IPCCallback.java com/huawei/hms/api/IPCTransport.java com/huawei/hms/api/ResolutionDelegate.java com/huawei/hms/api/b.java com/huawei/hms/availableupdate/a.java com/huawei/hms/base/ui/a.java com/huawei/hms/common/HuaweiApi.java com/huawei/hms/common/api/AvailabilityException.java com/huawei/hms/common/data/DataHolder.java com/huawei/hms/common/internal/BaseHmsClient.java com/huawei/hms/common/internal/ConnectionErrorMess

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ages.java com/huawei/hms/common/internal/DialogRedirect.java com/huawei/hms/common/internal/HmsClient.java com/huawei/hms/common/internal/RequestHeader.java com/huawei/hms/common/internal/RequestManager.java com/huawei/hms/common/internal/ResponseHeader.java com/huawei/hms/common/internal/ResponseWrap.java com/huawei/hms/common/internal/TaskApiCall.java com/huawei/hms/common/util/AGCUtils.java com/huawei/hms/common/util/Base64Utils.java com/huawei/hms/core/aidl/MessageCodec.java com/huawei/hms/device/a.java com/huawei/hms/framework/common/Logger.java com/huawei/hms/hatool/z.java com/huawei/hms/locationSdk/a.java com/huawei/hms/locationSdk/a1.java com/huawei/hms/locationSdk/b1.java com/huawei/hms/locationSdk/c0.java com/huawei/hms/locationSdk/c1.java com/huawei/hms/locationSdk/d0.java com/huawei/hms/locationSdk/d1.java com/huawei/hms/locationSdk/e.java com/huawei/hms/locationSdk/e1.java com/huawei/hms/locationSdk/f0.java com/huawei/hms/locationSdk/f1.java com/huawei/hms/locationSdk/g.java com/huawei/hms/locationSdk/g0.java com/huawei/hms/locationSdk/g1.java com/huawei/hms/locationSdk/h.java com/huawei/hms/locationSdk/h1.java com/huawei/hms/locationSdk/i0.java com/huawei/hms/locationSdk/i1.java com/huawei/hms/locationSdk/j0.java com/huawei/hms/locationSdk/k.java com/huawei/hms/locationSdk/k0.java com/huawei/hms/locationSdk/k1.java com/huawei/hms/locationSdk/l0.java com/huawei/hms/locationSdk/m0.java com/huawei/hms/locationSdk/m1.java com/huawei/hms/locationSdk/n.java com/huawei/hms/locationSdk/n0.java com/huawei/hms/locationSdk/n1.java com/huawei/hms/locationSdk/o0.java com/huawei/hms/locationSdk/p0.java com/huawei/hms/locationSdk/q.java com/huawei/hms/locationSdk/q0.java com/huawei/hms/locationSdk/r0.java com/huawei/hms/locationSdk/s0.java com/huawei/hms/locationSdk/t0.java com/huawei/hms/locationSdk/u0.java com/huawei/hms/locationSdk/v0.java com/huawei/hms/locationSdk/w0.java com/huawei/hms/locationSdk/x0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/huawei/hms/locationSdk/x0.java com/huawei/hms/locationSdk/y0.java com/huawei/hms/locationSdk/z0.java com/huawei/hms/stats/a.java com/huawei/hms/stats/c.java com/huawei/hms/support/api/ErrorResultImpl.java com/huawei/hms/support/api/PendingResultImpl.java com/huawei/hms/support/api/client/ResolvingResultCallbacks.java com/huawei/hms/support/api/client/ResultCallbacks.java com/huawei/hms/support/api/core/ConnectService.java com/huawei/hms/support/api/location/common/HMSLocationLog.java com/huawei/hms/support/api/location/common/LocationClientStateManager.java com/huawei/hms/support/api/location/common/LocationRequestHelper.java com/huawei/hms/support/api/location/common/PermissionUtil.java com/huawei/hms/support/api/location/common/exception/ServiceErrorCodeAdaptor.java com/huawei/hms/support/common/ActivityMgr.java com/huawei/hms/support/hianalytics/HiAnalyticsUtil.java com/huawei/hms/support/hianalytics/HiAnalyticsUtils.java com/huawei/hms/support/log/HMSDebugger.java com/huawei/hms/ui/AbstractDialog.java com/huawei/hms/update/note/AppSpoofResolution.java com/huawei/hms/update/note/DoNothingResolution.java com/huawei/hms/update/note/NotInstalledHmsResolution.java com/huawei/hms/update/ui/NotInstalledHmsDialogHelper.java com/huawei/hms/utils/FileUtil.java com/huawei/hms/utils/HMSBIInitializer.java com/huawei/hms/utils/HMSPackageManager.java com/huawei/hms/utils/IOUtils.java com/huawei/hms/utils/JsonUtil.java com/huawei/hms/utils/PackageManagerHelper.java com/huawei/hms/utils/ReadApkFileUtil.java com/huawei/hms/utils/SHA256.java com/huawei/hms/utils/UIUtil.java com/huawei/hms/utils/Util.java com/huawei/location/FB.java com/huawei/location/activity/model/Vw.java com/huawei/location/lite/common/log/logwrite/LogWrite.java com/huawei/location/lite/common/log/logwrite/LogWriteApi.java com/huawei/location/lite/common/log/logwrite/LogWriteManager.java com/huawei/riemann/common/api/location/SdmLocationClient.java com/huawei/riemann/gnsslocation/api/vdr/VdrLocationCli

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ent.java com/huawei/riemann/location/yn.java com/huawei/secure/android/common/activity/a.java com/huawei/secure/android/common/anonymization/Anonymizer.java com/huawei/secure/android/common/encrypt/keystore/rsa/RSASignKS.java com/huawei/secure/android/common/encrypt/utils/b.java com/huawei/secure/android/common/intent/SafeUri.java com/huawei/secure/android/common/ssl/util/BksUtil.java com/huawei/secure/android/common/ssl/util/g.java com/huawei/secure/android/common/util/EncodeUtil.java com/huawei/secure/android/common/util/HexUtil.java com/huawei/secure/android/common/util/IOUtil.java com/huawei/secure/android/common/util/LogsUtil.java com/huawei/secure/android/common/util/PermissionUtil.java com/huawei/secure/android/common/util/SafeBase64.java com/huawei/secure/android/common/util/SafePrintException.java com/huawei/secure/android/common/util/SafeString.java com/huawei/secure/android/common/util/SafeStringBuffer.java com/huawei/secure/android/common/util/SafeStringBuilder.java com/huawei/secure/android/common/util/ZipUtil.java com/huawei/secure/android/common/util/a.java com/huawei/secure/android/common/webview/SafeGetUrl.java com/huawei/secure/android/common/webview/SafeWebView.java com/huawei/secure/android/common/webview/UriUtil.java com/huawei/wisesecurity/kfs/crypto/key/KeyStoreKeyManager.java com/huawei/wisesecurity/kfs/ha/BIChecker.java com/huawei/wisesecurity/kfs/ha/HaReporter.java com/huawei/wisesecurity/kfs/interceptors/ReqHeaderInterceptor.java com/huawei/wisesecurity/kfs/util/KfsDeviceUtil.java com/huawei/wisesecurity/kfs/util/RandomUtil.java com/huawei/wisesecurity/ucs/common/log/LogUcs.java com/huawei/wisesecurity/ucs/common/log/LogUcsDefault.java com/intentfilter/androidpermissions/helpers/Logger.java com/journeyapps/barcodescanner/CameraPreview.java com/journeyapps/barcodescanner/CaptureManager.java com/journeyapps/barcodescanner/DecoderThread.java com/journeyapps/barcodescanner/camera/AutoFocusManager.java com/journeyapps/barcodescanner/camera/CameraConfigurationUtils.java com/journeyapps/barcodescanner/camera/CameraInstance

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	.java com/journeyapps/barcodescanner/camera/CameraManager.java com/journeyapps/barcodescanner/camera/CenterCropStrategy.java com/journeyapps/barcodescanner/camera/FitCenterStrategy.java com/journeyapps/barcodescanner/camera/LegacyPreviewScalingStrategy.java com/journeyapps/barcodescanner/camera/PreviewScalingStrategy.java com/skwas/cordova/datetimepicker/DateTimePicker.java com/transistorsoft/cordova/backgroundfetch/CDVBackgroundFetch.java com/transistorsoft/cordova/bggeo/CDVBackgroundGeolocation.java com/transistorsoft/locationmanager/BootReceiver.java com/transistorsoft/locationmanager/a/A.java com/transistorsoft/locationmanager/activity/TSLocationManagerActivity.java com/transistorsoft/locationmanager/adapter/BackgroundGeolocation.java com/transistorsoft/locationmanager/adapter/TSConfig.java com/transistorsoft/locationmanager/config/TSAuthorization.java com/transistorsoft/locationmanager/config/TSBackgroundPermissionRationale.java com/transistorsoft/locationmanager/config/TSNotification.java com/transistorsoft/locationmanager/config/TransistorAuthorizationToken.java com/transistorsoft/locationmanager/data/LocationModel.java com/transistorsoft/locationmanager/data/sqlite/GeofenceDAO.java com/transistorsoft/locationmanager/data/sqlite/LocationOpenHelper.java com/transistorsoft/locationmanager/data/sqlite/SQLiteLocationDAO.java com/transistorsoft/locationmanager/device/DeviceInfo.java com/transistorsoft/locationmanager/device/DeviceSettings.java com/transistorsoft/locationmanager/event/ActivityChangeEvent.java com/transistorsoft/locationmanager/event/AuthorizationEvent.java com/transistorsoft/locationmanager/event/GeofenceEvent.java com/transistorsoft/locationmanager/event/GeofencesChangeEvent.java com/transistorsoft/locationmanager/event/HeartbeatEvent.java com/transistorsoft/locationmanager/event/LocationProvid

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/transistorsoft/locationmanager/event/LocationProviderChangeEvent.java com/transistorsoft/locationmanager/event/MotionChangeEvent.java com/transistorsoft/locationmanager/event/TerminateEvent.java com/transistorsoft/locationmanager/geofence/TSGeofence.java com/transistorsoft/locationmanager/geofence/TSGeofenceManager.java com/transistorsoft/locationmanager/http/HttpResponse.java com/transistorsoft/locationmanager/http/HttpService.java com/transistorsoft/locationmanager/location/SingleLocationReceiver.java com/transistorsoft/locationmanager/location/SingleLocationRequest.java com/transistorsoft/locationmanager/location/TSLocation.java com/transistorsoft/locationmanager/location/TSLocationManager.java com/transistorsoft/locationmanager/location/TSWatchPositionRequest.java com/transistorsoft/locationmanager/logger/TSLog.java com/transistorsoft/locationmanager/logger/TSLogReader.java com/transistorsoft/locationmanager/logger/TSSQLiteAppender.java com/transistorsoft/locationmanager/logger/a.java com/transistorsoft/locationmanager/plugin/TSPlugin.java com/transistorsoft/locationmanager/provider/TSProviderManager.java com/transistorsoft/locationmanager/rpc/a.java com/transistorsoft/locationmanager/scheduler/ScheduleEvent.java com/transistorsoft/locationmanager/scheduler/TSScheduleManager.java com/transistorsoft/locationmanager/service/AbstractService.java com/transistorsoft/locationmanager/service/ActivityRecognitionService.java com/transistorsoft/locationmanager/service/BackgroundTaskService.java com/transistorsoft/locationmanager/service/ForegroundNotification.java com/transistorsoft/locationmanager/service/GeofencingService.java com/transistorsoft/locationmanager/service/LocationRequestService.java com/transistorsoft/locationmanager/service/PolygonGeofencingService.java com/transistorsoft/locationmanager/service/TrackingService.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/transistorsoft/locationmanager/settings/Settings.java com/transistorsoft/locationmanager/util/BackgroundTaskManager.java com/transistorsoft/locationmanager/util/BackgroundTaskWorker.java com/transistorsoft/locationmanager/util/BuildConfigUtils.java com/transistorsoft/locationmanager/util/HeadlessEventBroadcaster.java com/transistorsoft/locationmanager/util/LocationAuthorization.java com/transistorsoft/locationmanager/util/TSNotification.java com/transistorsoft/locationmanager/workers/GeofenceWorker.java com/transistorsoft/tsbackgroundfetch/BGTask.java com/transistorsoft/tsbackgroundfetch/BackgroundFetch.java com/transistorsoft/tsbackgroundfetch/BackgroundFetchConfig.java com/transistorsoft/tsbackgroundfetch/BootReceiver.java com/transistorsoft/tsbackgroundfetch/FetchAlarmReceiver.java com/transistorsoft/tsbackgroundfetch/FetchJobService.java com/transistorsoft/tsbackgroundfetch/LifecycleManager.java com/transistorsoft/xms/g/actions/SearchIntents.java com/transistorsoft/xms/g/common/ConnectionResult.java com/transistorsoft/xms/g/common/ErrorDialogFragment.java com/transistorsoft/xms/g/common/ExtensionApiAvailability.java com/transistorsoft/xms/g/common/ExtensionPlayServicesNotAvailableException.java com/transistorsoft/xms/g/common/ExtensionPlayServicesRepairableException.java com/transistorsoft/xms/g/common/ExtensionPlayServicesUtil.java com/transistorsoft/xms/g/common/SupportErrorDialogFragment.java com/transistorsoft/xms/g/common/UserRecoverableException.java com/transistorsoft/xms/g/common/api/ApiException.java com/transistorsoft/xms/g/common/api/AvailabilityException.java com/transistorsoft/xms/g/common/api/BooleanResult.java com/transistorsoft/xms/g/common/api/CommonStatusCodes.java com/transistorsoft/xms/g/common/api/ExtensionApiClient.java com/transistorsoft/xms/g/common/api/OptionalPendingResult.java com/transistorsoft/xms/g/common/api/PendingResult.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/transistorsoft/xms/g/common/api/PendingResults.java com/transistorsoft/xms/g/common/api/Releasable.java com/transistorsoft/xms/g/common/api/ResolvableApiException.java com/transistorsoft/xms/g/common/api/ResolvingResultCallbacks.java com/transistorsoft/xms/g/common/api/Response.java com/transistorsoft/xms/g/common/api/Result.java com/transistorsoft/xms/g/common/api/ResultCallback.java com/transistorsoft/xms/g/common/api/ResultCallbacks.java com/transistorsoft/xms/g/common/api/ResultTransform.java com/transistorsoft/xms/g/common/api/Scope.java com/transistorsoft/xms/g/common/api/Status.java com/transistorsoft/xms/g/common/api/TransformedResult.java com/transistorsoft/xms/g/common/api/UnsupportedApiCallException.java com/transistorsoft/xms/g/common/data/AbstractDataBuffer.java com/transistorsoft/xms/g/common/data/DataBuffer.java com/transistorsoft/xms/g/common/data/DataBufferObserver.java com/transistorsoft/xms/g/common/data/DataBufferUtils.java com/transistorsoft/xms/g/common/data/Freezable.java com/transistorsoft/xms/g/common/data/FreezableUtils.java com/transistorsoft/xms/g/common/images/Size.java com/transistorsoft/xms/g/common/images/WebImage.java com/transistorsoft/xms/g/location/ActivityRecognition.java com/transistorsoft/xms/g/location/ActivityRecognitionClient.java com/transistorsoft/xms/g/location/ActivityRecognitionResult.java com/transistorsoft/xms/g/location/ActivityTransition.java com/transistorsoft/xms/g/location/ActivityTransitionEvent.java com/transistorsoft/xms/g/location/ActivityTransitionRequest.java com/transistorsoft/xms/g/location/ActivityTransitionResult.java com/transistorsoft/xms/g/location/DetectedActivity.java com/transistorsoft/xms/g/location/FusedLocationProviderClient.java com/transistorsoft/xms/g/location/Geofence.java com/transistorsoft/xms/g/location/GeofenceStatusCodes.java com/transistorsoft/xms/g/location/GeofencingClient.java com/transistorsoft/xms/g/location/GeofencingEvent.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/transistorsoft/xms/g/location/GeofencingRequest.java com/transistorsoft/xms/g/location/LocationAvailability.java com/transistorsoft/xms/g/location/LocationCallback.java com/transistorsoft/xms/g/location/LocationRequest.java com/transistorsoft/xms/g/location/LocationResult.java com/transistorsoft/xms/g/location/LocationServices.java com/transistorsoft/xms/g/location/LocationSettingsRequest.java com/transistorsoft/xms/g/location/LocationSettingsResponse.java com/transistorsoft/xms/g/location/LocationSettingsResult.java com/transistorsoft/xms/g/location/LocationSettingsStates.java com/transistorsoft/xms/g/location/LocationSettingsStatusCodes.java com/transistorsoft/xms/g/location/LocationStatusCodes.java com/transistorsoft/xms/g/location/SettingsClient.java com/transistorsoft/xms/g/security/ProviderInstaller.java com/transistorsoft/xms/g/tasks/CancellationToken.java com/transistorsoft/xms/g/tasks/CancellationTokenSource.java com/transistorsoft/xms/g/tasks/Continuation.java com/transistorsoft/xms/g/tasks/OnCanceledListener.java com/transistorsoft/xms/g/tasks/OnCompleteListener.java com/transistorsoft/xms/g/tasks/OnFailureListener.java com/transistorsoft/xms/g/tasks/OnSuccessListener.java com/transistorsoft/xms/g/tasks/SuccessContinuation.java com/transistorsoft/xms/g/tasks/Task.java com/transistorsoft/xms/g/tasks/TaskCompletionSource.java com/transistorsoft/xms/g/tasks/TaskExecutors.java com/transistorsoft/xms/g/tasks/Tasks.java com/transistorsoft/xms/g/utils/Utils.java com/transistorsoft/xms/g/utils/XObject.java com/transistorsoft/xms/g/utils/XmsLog.java com/wellseek/cordova/SelectorCordovaPlugin.java cordova/plugin/PowerOptimization/PowerOptimization.java cordova/plugin/PowerOptimization/ProtectedApps.java cordova/plugins/Diagnostic.java cordova/plugins/Diagnostic_Bluetooth.java cordova/plugins/Diagnostic_Camera.java cordova/plugins/Diagnostic_Location.java cordova/plugins/Diagnostic_Notifications.java cordova/plugins/Diagnostic_Wifi.java cordova/plugins/screenorientation/CDVOrientation.java de/appplant/cordova/plugin/notification/Notification.java de/appplant/cordova/plugin/notification/NotificationVolumeManager.java de/appplant/cordova/plugin/notification/action/ActionGroup.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				de/appplant/cordova/plugin/notification/receiver/AbstractNotificationReceiver.java de/appplant/cordova/plugin/notification/util/AssetUtil.java defpackage/Crypto.java defpackage/NativeStorage.java io/ionic/links/IonicDeeplink.java io/sqlc/SQLiteAndroidDatabase.java io/sqlc/SQLiteConnectorDatabase.java io/sqlc/SQLitePlugin.java me/leolin/shortcutbadger/ShortcutBadger.java org/greenrobot/eventbus/Logger.java org/slf4j/helpers/Util.java uk/co/workingedge/phonegap/plugin/CordovaLogger.java uk/co/workingedge/phonegap/plugin/LaunchNavigatorPlugin.java
2	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	ch/qos/logback/classic/joran/action/ConfigurationAction.java ch/qos/logback/classic/sift/ContextBasedDiscriminator.java ch/qos/logback/core/CoreConstants.java ch/qos/logback/core/net/ssl/SSL.java ch/qos/logback/core/rolling/helper/DateTokenConverter.java ch/qos/logback/core/rolling/helper/IntegerTokenConverter.java com/adobe/phonegap/push/FCMService.java com/adobe/phonegap/push/PushConstants.java com/huawei/hms/framework/common/hianalytics/HianalyticsBaseData.java com/huawei/hms/location/LocationAvailability.java com/huawei/hms/location/LocationResult.java com/huawei/hms/support/api/location/common/LocationClientStateManager.java com/huawei/hms/support/hianalytics/HiAnalyticsConstant.java com/huawei/location/lite/common/agc/AGCManager.java com/huawei/location/lite/common/config/ConfigManager.java com/huawei/location/lite/common/util/filedownload/DownloadConstants.java com/huawei/wisesecurity/kfs/util/KfsDeviceUtil.java com/wellseek/cordova/SelectorCordovaPlugin.java de/appplant/cordova/plugin/badge/BadgeImpl.java de/appplant/cordova/plugin/notification/NotificationVolumeManager.java uk/co/workingedge/phonegap/plugin/LaunchNavigatorPlugin.java
3	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	ch/qos/logback/core/android/AndroidContextUtil.java nl/xservices/plugins/SocialSharing.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/danielsogl/cordova/clipboard/Clipboard.java nl/xservices/plugins/SocialSharing.java
5	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/huawei/agconnect/core/BuildConfig.java com/huawei/hms/api/HuaweiApiAvailability.java com/huawei/hms/api/HuaweiApiClientImpl.java com/huawei/hms/base/device/BuildConfig.java com/huawei/hms/common/PackageConstants.java com/huawei/hms/framework/common/BuildConfig.java com/huawei/hms/framework/common/PackageManagerCompat.java com/huawei/hms/framework/common/hianalytics/HianalyticsHelper.java com/huawei/hms/framework/network/frameworkcompat/BuildConfig.java com/huawei/hms/framework/network/grs/BuildConfig.java com/huawei/hms/framework/network/grs/g/k/a.java com/huawei/hms/framework/network/grs/h/a.java com/huawei/hms/hatool/g1.java com/huawei/hms/hatool/v.java com/huawei/hms/hatool/z.java com/huawei/hms/location/BuildConfig.java com/huawei/hms/location/base/BuildConfig.java com/huawei/hms/support/api/PendingResultImpl.java com/huawei/hms/support/hianalytics/HiAnalyticsUtil.java com/huawei/hms/support/hianalytics/a.java com/huawei/location/router/BuildConfig.java com/huawei/secure/android/common/base/a.java com/huawei/secure/android/common/encrypt/a.java com/huawei/secure/android/common/intent/BuildConfig.java com/huawei/secure/android/common/ssl/a.java com/huawei/secure/android/common/ssl/util/BksUtil.java com/huawei/secure/android/common/util/e.java com/huawei/wisesecurity/kfs/BuildConfig.java com/huawei/wisesecurity/ucs/credential/CredentialClient.java com/huawei/wisesecurity/ucs_credential/l.java
6	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/journeyapps/barcodescanner/CaptureManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	ch/qos/logback/classic/android/SQLiteAppender.java com/transistorsoft/locationmanager/data/sqlite/GeofenceDAO.java com/transistorsoft/locationmanager/data/sqlite/LocationOpenHelper.java com/transistorsoft/locationmanager/data/sqlite/SQLiteLocationDAO.java com/transistorsoft/locationmanager/logger/TSSQLiteAppender.java io/sqlc/SQLiteAndroidDatabase.java
8	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/huawei/hms/common/internal/TransactionIdCreater.java cordova/plugins/Diagnostic.java de/appplant/cordova/plugin/notification/util/LaunchUtils.java
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	cordova/plugins/Diagnostic.java
10	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	ch/qos/logback/core/net/ssl/SSLContextFactoryBean.java com/huawei/secure/android/common/ssl/SecureX509TrustManager.java
11	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/huawei/agconnect/config/impl/i.java
12	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/adobe/phonegap/push/FCMService.java
13	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/huawei/hms/hatool/e.java com/huawei/secure/android/common/encrypt/hash/PBKDF2.java
14	Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	com/huawei/secure/android/common/webview/SafeWebView.java

SHARED LIBRARY BINARY ANALYSIS

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

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	x86_64/libucs-credential.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memset_chk', '__memcpy_chk']	True info Symbols are stripped.
6	x86_64/libtslocationmanager.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	armeabi-v7a/libucs-credential.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memset_chk', '__memcpy_chk']	True info Symbols are stripped.
10	armeabi-v7a/libtslocationmanager.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	x86/libucs-credential.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memset_chk', '__memcpy_chk']	True info Symbols are stripped.
14	x86/libtslocationmanager.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	x86/libsqlc-native-driver.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
16	arm64-v8a/libTransform.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	arm64-v8a/libucs-credential.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__memset_chk']	True info Symbols are stripped.
18	arm64-v8a/libtslocationmanager.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

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

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

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

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

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

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

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	ch/qos/logback/classic/android/SQLiteAppender.java ch/qos/logback/core/FileAppender.java ch/qos/logback/core/android/AndroidContextUtil.java ch/qos/logback/core/rolling/helper/Compressor.java ch/qos/logback/core/rolling/helper/FileFinder.java ch/qos/logback/core/rolling/helper/RenameUtil.java com/darktalker/cordova/screenshot/Screenshot.java com/huawei/location/activity/model/Vw.java com/journeyapps/barcodescanner/CaptureManager.java com/transistorsoft/locationmanager/logger/TSSQLiteAppender.java de/appplant/cordova/plugin/notification/util/AssetUtil.java io/sqlc/SQLiteConnectorDatabase.java io/sqlc/SQLitePlugin.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/adobe/phonegap/push/FCMService.java com/customtabplugin/ChromeCustomTabPlugin.java com/transistorsoft/locationmanager/device/DeviceSettings.java cordova/plugin/PowerOptimization/PowerOptimization.java cordova/plugins/Diagnostic_Notifications.java cordova/plugins/DozeOptimize/DozeOptimize.java de/appplant/cordova/plugin/localnotification/LocalNotification.java de/appplant/cordova/plugin/notification/Notification.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java nl/xservices/plugins/SocialSharing.java uk/co/workingedge/LaunchNavigator.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/customtabplugin/ChromeCustomTabPlugin.java com/transistorsoft/locationmanager/device/DeviceSettings.java cordova/plugin/PowerOptimization/PowerOptimization.java cordova/plugins/Diagnostic_Notifications.java cordova/plugins/DozeOptimize/DozeOptimize.java de/appplant/cordova/plugin/localnotification/LocalNotification.java nl/xservices/plugins/SocialSharing.java uk/co/workingedge/LaunchNavigator.java
00175	Get notification manager and cancel notifications	notification	com/adobe/phonegap/push/PushPlugin.java de/appplant/cordova/plugin/localnotification/LocalNotification.java de/appplant/cordova/plugin/notification/Manager.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/adobe/phonegap/push/FCMService.java com/adobe/phonegap/push/PushPlugin.java com/customtabplugin/ChromeCustomTabPlugin.java com/huawei/location/lite/common/util/APKUtil.java com/transistorsoft/locationmanager/device/DeviceSettings.java cordova/plugin/PowerOptimization/PowerOptimization.java cordova/plugins/Diagnostic_Notifications.java cordova/plugins/DozeOptimize/DozeOptimize.java de/appplant/cordova/plugin/localnotification/LocalNotification.java de/appplant/cordova/plugin/notification/util/AssetUtil.java me/leolin/shortcutbadger/impl/EverythingMeHomeBadger.java me/leolin/shortcutbadger/impl/HuaweiHomeBadger.java me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java
00088	Create a secure socket connection to the given host address	command network	com/huawei/secure/android/common/SecureSSLSocketFactory.java com/huawei/secure/android/common/ssl/SSFCompatiableSystemCA.java com/huawei/secure/android/common/ssl/SecureSSLSocketFactory.java com/huawei/secure/android/common/ssl/SecureSSLSocketFactoryNew.java
00016	Get location info of the device and put it to JSON object	location collection	com/huawei/hms/support/api/location/common/LocationJsonUtil.java com/huawei/location/activity/model/Vw.java com/huawei/location/nlp/network/OnlineLocationService.java com/transistorsoft/locationmanager/location/TSLocation.java com/transistorsoft/locationmanager/location/TSLocationManager.java
00147	Get the time of current location	collection location	com/huawei/location/activity/model/Vw.java com/transistorsoft/locationmanager/location/TSLocationManager.java
00014	Read file into a stream and put it into a JSON object	file	com/huawei/location/activity/model/Vw.java com/huawei/location/ephemeris/yn.java com/huawei/location/vdr/data/ephemeris/yn.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	ch/qos/logback/core/joran/GenericConfigurator.java ch/qos/logback/core/joran/action/PropertyAction.java ch/qos/logback/core/rolling/helper/Compressor.java ch/qos/logback/core/util/FileUtil.java com/huawei/hms/framework/common/CreateFileUtil.java com/huawei/hms/hatool/t0.java com/huawei/hms/utils/SHA256.java com/huawei/location/activity/model/Vw.java com/huawei/location/crowdsourcing/LW.java com/huawei/location/crowdsourcing/upload/LW.java com/huawei/location/crowdsourcing/upload/Vw.java com/huawei/location/crowdsourcing/upload/http/LW.java com/huawei/location/ephemeris/yn.java com/huawei/location/lite/common/http/response/ResponseInfo.java com/huawei/location/tiles/cache/Vw.java com/huawei/location/tiles/utils/LW.java com/huawei/location/tiles/utils/yn.java com/huawei/location/vdr/data/ephemeris/yn.java com/huawei/secure/android/common/encrypt/hash/FileSHA256.java com/huawei/secure/android/common/ssl/SecureX509TrustManager.java com/huawei/secure/android/common/ssl/util/BksUtil.java com/huawei/secure/android/common/util/ZipUtil.java com/huawei/wisesecurity/ucs_credential/r.java okio/Okio__JvmOkioKt.java
00005	Get absolute path of file and put it to JSON object	file	com/darktalker/cordova/screenshot/Screenshot.java com/huawei/location/activity/model/Vw.java io/sqlc/SQLiteConnectorDatabase.java io/sqlc/SQLitePlugin.java
00012	Read data and put it into a buffer stream	file	ch/qos/logback/core/rolling/helper/Compressor.java ch/qos/logback/core/util/FileUtil.java com/huawei/hms/utils/SHA256.java com/huawei/location/tiles/utils/LW.java com/huawei/secure/android/common/util/ZipUtil.java
00009	Put data in cursor to JSON object	file	com/transistorsoft/locationmanager/data/sqlite/GeofenceDAO.java com/transistorsoft/locationmanager/data/sqlite/SQLiteLocationDAO.java io/sqlc/SQLiteAndroidDatabase.java
00004	Get filename and put it to JSON object	file collection	cordova/plugins/Diagnostic.java
00056	Modify voice volume	control	com/cordova/volumeControl/VolumeControl.java de/appplant/cordova/plugin/notification/NotificationVolumeManager.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/adobe/phonegap/push/BackgroundActionButtonHandler.java com/adobe/phonegap/push/BackgroundHandlerActivity.java com/adobe/phonegap/push/PushHandlerActivity.java com/transistorsoft/locationmanager/http/HttpService.java com/transistorsoft/locationmanager/location/TSLocation.java de/appplant/cordova/plugin/notification/receiver/AbstractClickReceiver.java io/ionic/links/IonicDeeplink.java
00121	Create a directory	file command	com/huawei/hms/locationSdk/f0.java
00125	Check if the given file path exist	file	com/huawei/hms/locationSdk/f0.java
00096	Connect to a URL and set request method	command network	com/huawei/hms/hatool/a0.java
00089	Connect to a URL and receive input stream from the server	command network	com/adobe/phonegap/push/FCMService.java com/huawei/hms/hatool/a0.java de/appplant/cordova/plugin/notification/util/AssetUtil.java
00109	Connect to a URL and get the response code	network command	com/huawei/hms/hatool/a0.java
00123	Save the response to JSON after connecting to the remote server	network command	com/adobe/phonegap/push/FCMService.java
00030	Connect to the remote server through the given URL	network	com/adobe/phonegap/push/FCMService.java de/appplant/cordova/plugin/notification/util/AssetUtil.java
00130	Get the current WIFI information	wifi collection	com/huawei/hms/framework/common/NetworkUtil.java com/huawei/location/crowdsourcing/record/yn.java
00094	Connect to a URL and read data from it	command network	com/huawei/location/crowdsourcing/upload/http/Vw.java de/appplant/cordova/plugin/notification/util/AssetUtil.java
00065	Get the country code of the SIM card provider	collection	com/huawei/hms/framework/network/grs/local/model/CountryCodeBean.java com/huawei/location/lite/common/util/TelephonyUtil.java
00132	Query The ISO country code	telephony collection	com/huawei/hms/framework/network/grs/local/model/CountryCodeBean.java com/huawei/location/lite/common/util/TelephonyUtil.java
00112	Get the date of the calendar event	collection calendar	de/appplant/cordova/plugin/notification/Request.java
00189	Get the content of a SMS message	sms	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java

RULE ID	BEHAVIOUR	LABEL	FILES
00188	Get the address of a SMS message	sms	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00191	Get messages in the SMS inbox	sms	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00200	Query data from the contact list	collection contact	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00187	Query a URI and check the result	collection sms calllog calendar	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00201	Query data from the call log	collection calllog	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00039	Start a web server	control network	ch/qos/logback/classic/net/SimpleSocketServer.java
00018	Get JSON object prepared and fill in location info	location collection	com/transistorsoft/locationmanager/location/TSLocationManager.java
00092	Send broadcast	command	com/huawei/hms/adapter/BaseAdapter.java
00072	Write HTTP input stream into a file	command network file	com/huawei/hms/hatool/t0.java de/appplant/cordova/plugin/notification/util/AssetUtil.java
00108	Read the input stream from given URL	network command	com/huawei/hms/hatool/t0.java de/appplant/cordova/plugin/notification/util/AssetUtil.java
00043	Calculate WiFi signal strength	collection wifi	com/huawei/hms/framework/common/NetworkUtil.java
00183	Get current camera parameters and change the setting.	camera	com/journeyapps/barcodescanner/camera/CameraManager.java
00003	Put the compressed bitmap data into JSON object	camera	com/darktalker/cordova/screenshot/Screenshot.java
00033	Query the IMEI number	collection	com/huawei/wisesecurity/kfs/util/KfsDeviceUtil.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://rtrt-mobileapp.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/391170825022/namespaces/firebase:fetch?key=AIzaSyC1voIbtqBUy3hIo0isamH-kBaMhCb3xPk. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK, android.permission.RECORD_AUDIO, android.permission.ACCESS_NETWORK_STATE, android.permission.VIBRATE, android.permission.ACCESS_WIFI_STATE, android.permission.CAMERA
Other Common Permissions	10/44	android.permission.ACCESS_NOTIFICATION_POLICY, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.BLUETOOTH, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.ACTIVITY_RECOGNITION, android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.ACTIVITY_RECOGNITION, com.google.android.c2dm.permission.RECEIVE, android.permission.CHANGE_WIFI_STATE

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

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
shop.transistorsoft.com	ok	**IP:** 23.227.38.74 **Country:** Canada **Region:** Ontario **City:** Ottawa **Latitude:** 45.418877 **Longitude:** -75.696510 **View:** Google Map
logback.qos.ch	ok	**IP:** 31.97.181.89 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Bowness-on-Windermere **Latitude:** 54.363312 **Longitude:** -2.918590 **View:** Google Map
android.googlesource.com	ok	**IP:** 64.233.165.82 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.whatsapp.com	ok	**IP:** 157.240.11.53 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
citymapper.com	ok	**IP:** 141.101.90.104 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	**IP:** 159.100.250.151 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map
xml.org	ok	**IP:** 104.239.142.8 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
xmlpull.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
journeyapps.com	ok	**IP:** 18.238.96.96 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
rtrt-mobileapp.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
share.here.com	ok	**IP:** 18.155.173.29 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
maps.google.com	ok	**IP:** 216.58.207.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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
github.com	ok	**IP:** 140.82.112.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

EMAILS

EMAIL	FILE
someone@domain.com	nl/xservices/plugins/SocialSharing.java
info@transistorsoft.com	lib/arm64-v8a/libtslocationmanager.so

EMAIL	FILE
info@transistorsoft.com	lib/x86_64/libtslocationmanager.so
info@transistorsoft.com	lib/armeabi-v7a/libtslocationmanager.so
info@transistorsoft.com	lib/x86/libtslocationmanager.so
info@transistorsoft.com	apktool_out/lib/arm64-v8a/libtslocationmanager.so
info@transistorsoft.com	apktool_out/lib/x86_64/libtslocationmanager.so
info@transistorsoft.com	apktool_out/lib/armeabi-v7a/libtslocationmanager.so
info@transistorsoft.com	apktool_out/lib/x86/libtslocationmanager.so

TRACKERS

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

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://rtrt-mobileapp.firebaseio.com"
"google_crash_reporting_api_key" : "AIzaSyC1voIbtqBUy3hIo0isamH-kBaMhCb3xPk"
"file_provider_authority" : "com.transistorsoft.tslocationmanager.fileprovider"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"
"google_api_key" : "AIzaSyC1voIbtqBUy3hIo0isamH-kBaMhCb3xPk"
"library_zxingandroidembedded_author" : "JourneyApps"

POSSIBLE SECRETS
3517262215D8D3008CBF888750B6418EDC4D562AC33ED6874E0D73ABA667BC3C
E49D5C2C0E11B3B1B96CA56C6DE2A14EC7DAB5CCC3B5F300D03E5B4DBA44F539
0123456789ABCDEFabcdef
b368b110e3b565fe97c91f786e11bc48754cc8e4e6f21d8a94a68ac6ad67aaaf
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
4bdecdf772491e35c4e8b48f88aee22bae1311984f2e1da4dfad0b78ee7f5163
30820122300d06092a864886f70d01010105000382010f003082010a0282010100a3d269348ac59923f65e8111c337605e29a1d1bc54fa96c1445050dd14d8d63b10f9f0230bb87ef348183660bedcabfdec045e235ed96935799fcdb4af5c97717ff3b0954eaf1b723225b3a00f81cbd67ce6dc5a4c07f7741ad3bf1913a480c6e267ab1740f409edd2dc33c8b718a8e30e56d9a93f321723c1d0c9ea62115f996812ceef186954595e39a19b74245542c407f7dddb1d12e6eedcfc0bd7cd945ef7255ad0fc9e796258e0fb5e52a23013d15033a32b4071b65f3f924ae5c5761e22327b4d2ae60f4158a5eb15565ba079de29b81540f5fbb3be101a95357f367fc661d797074ff3826950029c52223e4594673a24a334cae62d63b838ba3df9770203010001
5fed96c85bd58c58aadbd465c172a4c9a794d8eb2f86cbc7bcee6caf4c7a2c5f
3081a0adab3018d57165e6dd24074bdbac640f6dbe21a9e24d3474a87ebf38b8
d80f18e8081b624cc64985f87f70118f1702985d2e10dbc985ee7be334fd3c7d
db48223fd9e143f7e133c57f5d08a4e38549ce3ebd921fe3b4003c26e5e35bed
ae2044fb577e65ee8bb576ca48a2f06e
f6040d0e807aaec325ecf44823765544e92905158169f694b282bf17388632cf95a83bae7d2d235c1f039b0df1dcca5fda619b6f7f459f2ff8d70ddb7b601592fe29fcae58c028f319b3b12495e67aa5390942a997a8cb572c8030b2df5c2b622608bea02b0c3e5d4dff3f72c9e3204049a45c0760cd3604af8d57f0e0c693cc
e9702f1e92e97fce49cdf81a5fa730a4e913554d09b3fe41e1d8a7fba00a8459
92974c6802419e4d18b5ec536cbfa167b8e8eff09ec4c8510a5b95750b1e0c82
173cf86fe9894a0f70dadd09d4fd88c380836099d4939f8c3754361bdc16a32b
7a5b85d3ee2e0991ca3502602e9389a98f55c0576b887125894a7ec03823f8d3
B92825C2BD5D6D6D1E7F39EECD17843B7D9016F611136B75441BC6F4D3F00F05
f8d927750a0952ffb5bd87dfb83d781ae65f7bed043a7886d1d3cdcfc94bb77a

POSSIBLE SECRETS
4230baa077b401374d0fc012375047e79ea0790d58d095ef18d97d95470c738d
5181942b9ebc31ce68dacb56c16fd79f
07ff9b7aeeff969173c45b285fe0fecdbaae244576ff7a2796a36f1c0c11adb4
24fbae40bcd50b759b26e3ba0f46aa25e932fa7da05f226d75ec507bcf53bce5
e2f856b9f9a4fd4cb2795aeaf83268e4bff189aaec05d691ffde76e075b82648
db53fcdc9ab71e9bdd4eab257fe1aba7989ad2b24fbe3a85dfef72ea1dd6bae2
403f14ad2f0e5eb3c4f3a0bcd5c1592cc4492662ad53191c92905255d4990656

PLAYSTORE INFORMATION

Title: RTRT.me

Score: 4.6893206 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** me.rtrt.app2

Developer Details: RTRT.me, 7290626085125482703, None, https://rtrt.me, help@rtrt.me,

Release Date: Nov 12, 2014 **Privacy Policy:** Privacy link

Description:

RTRT.me provides Real-Time Race Tracking and other services for world-class events. Participants and Spectators of premiere RTRT.me tracked events, this app is for you! Highlights: • Participant times, paces, estimates, and places in real-time • Interactive Course Map & Live Map Tracking • Easy tracking of multiple participants at the same time • Push Notifications as progress is made on course • Event Info and Messaging • Live Leaderboards • Social Sharing & Notifications PLEASE NOTE: Not all RTRT.me events are available in the RTRT.me app. Some included events may not use all features. Contact us or your event coordinator for availability. PLEASE NOTE: Continued use of GPS running in the background can dramatically decrease battery life. About Us: We are passionate about technology and determined to create the ultimate race experience for Participants, Spectators, Volunteers and Event Administrators around the globe.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 14:30:34	Generating Hashes	OK

2025-09-01 14:30:35	Extracting APK	OK
2025-09-01 14:30:35	Unzipping	OK
2025-09-01 14:30:35	Parsing APK with androguard	OK
2025-09-01 14:30:35	Extracting APK features using aapt/aapt2	OK
2025-09-01 14:30:35	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 14:30:37	Parsing AndroidManifest.xml	OK
2025-09-01 14:30:37	Extracting Manifest Data	OK
2025-09-01 14:30:37	Manifest Analysis Started	OK
2025-09-01 14:30:38	Performing Static Analysis on: RTRT.me (me.rtrt.app2)	OK
2025-09-01 14:30:39	Fetching Details from Play Store: me.rtrt.app2	OK
2025-09-01 14:30:39	Checking for Malware Permissions	OK
2025-09-01 14:30:39	Fetching icon path	OK
2025-09-01 14:30:39	Library Binary Analysis Started	OK
2025-09-01 14:30:39	Analyzing lib/arm64-v8a/libTransform.so	OK

2025-09-01 14:30:39	Analyzing lib/arm64-v8a/libucs-credential.so	OK
2025-09-01 14:30:39	Analyzing lib/arm64-v8a/libtslocationmanager.so	OK
2025-09-01 14:30:39	Analyzing lib/arm64-v8a/libsqlc-native-driver.so	OK
2025-09-01 14:30:39	Analyzing lib/x86_64/libucs-credential.so	OK
2025-09-01 14:30:39	Analyzing lib/x86_64/libtslocationmanager.so	OK
2025-09-01 14:30:39	Analyzing lib/x86_64/libsqlc-native-driver.so	OK
2025-09-01 14:30:39	Analyzing lib/armeabi-v7a/libTransform.so	OK
2025-09-01 14:30:39	Analyzing lib/armeabi-v7a/libucs-credential.so	OK
2025-09-01 14:30:39	Analyzing lib/armeabi-v7a/libtslocationmanager.so	OK
2025-09-01 14:30:39	Analyzing lib/armeabi-v7a/libsqlc-native-driver.so	OK
2025-09-01 14:30:39	Analyzing lib/armeabi/libsqlc-native-driver.so	OK
2025-09-01 14:30:39	Analyzing lib/x86/libucs-credential.so	OK
2025-09-01 14:30:39	Analyzing lib/x86/libtslocationmanager.so	OK
2025-09-01 14:30:39	Analyzing lib/x86/libsqlc-native-driver.so	OK

2025-09-01 14:30:39	Analyzing apktool_out/lib/arm64-v8a/libTransform.so	OK
2025-09-01 14:30:39	Analyzing apktool_out/lib/arm64-v8a/libucs-credential.so	OK
2025-09-01 14:30:39	Analyzing apktool_out/lib/arm64-v8a/libtslocationmanager.so	OK
2025-09-01 14:30:39	Analyzing apktool_out/lib/arm64-v8a/libsqlc-native-driver.so	OK
2025-09-01 14:30:39	Analyzing apktool_out/lib/x86_64/libucs-credential.so	OK
2025-09-01 14:30:39	Analyzing apktool_out/lib/x86_64/libtslocationmanager.so	OK
2025-09-01 14:30:39	Analyzing apktool_out/lib/x86_64/libsqlc-native-driver.so	OK
2025-09-01 14:30:39	Analyzing apktool_out/lib/armeabi-v7a/libTransform.so	OK
2025-09-01 14:30:39	Analyzing apktool_out/lib/armeabi-v7a/libucs-credential.so	OK
2025-09-01 14:30:39	Analyzing apktool_out/lib/armeabi-v7a/libtslocationmanager.so	OK
2025-09-01 14:30:39	Analyzing apktool_out/lib/armeabi-v7a/libsqlc-native-driver.so	OK
2025-09-01 14:30:39	Analyzing apktool_out/lib/armeabi/libsqlc-native-driver.so	OK
2025-09-01 14:30:39	Analyzing apktool_out/lib/x86/libucs-credential.so	OK
2025-09-01 14:30:39	Analyzing apktool_out/lib/x86/libtslocationmanager.so	OK

2025-09-01 14:30:39	Analyzing apktool_out/lib/x86/libsqlc-native-driver.so	OK
2025-09-01 14:30:39	Reading Code Signing Certificate	OK
2025-09-01 14:30:40	Running APKiD 2.1.5	OK
2025-09-01 14:30:44	Detecting Trackers	OK
2025-09-01 14:30:46	Decompiling APK to Java with JADX	OK
2025-09-01 14:30:59	Converting DEX to Smali	OK
2025-09-01 14:30:59	Code Analysis Started on - java_source	OK
2025-09-01 14:31:01	Android SBOM Analysis Completed	OK
2025-09-01 14:31:05	Android SAST Completed	OK
2025-09-01 14:31:05	Android API Analysis Started	OK
2025-09-01 14:31:09	Android API Analysis Completed	OK
2025-09-01 14:31:10	Android Permission Mapping Started	OK
2025-09-01 14:31:15	Android Permission Mapping Completed	OK
2025-09-01 14:31:15	Android Behaviour Analysis Started	OK

2025-09-01 14:31:19	Android Behaviour Analysis Completed	OK
2025-09-01 14:31:19	Extracting Emails and URLs from Source Code	OK
2025-09-01 14:31:21	Email and URL Extraction Completed	OK
2025-09-01 14:31:21	Extracting String data from APK	OK
2025-09-01 14:31:21	Extracting String data from SO	OK
2025-09-01 14:31:21	Extracting String data from Code	OK
2025-09-01 14:31:21	Extracting String values and entropies from Code	OK
2025-09-01 14:31:25	Performing Malware check on extracted domains	OK
2025-09-01 14:31:29	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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