

# ANDROID STATIC ANALYSIS REPORT



# Bark (6.28.0)

File Name: 6.28.0.apk

Package Name: com.pt.bark

Scan Date: Aug. 2, 2024, 2 a.m.

Α	0		· C	
Δnn	Sec	IIritv	Score	١

# **50/100 (MEDIUM RISK)**

Grade:

В

Trackers Detection:

3/432

### **\$** FINDINGS SEVERITY

£ HIGH	<b>▲</b> MEDIUM	<b>i</b> INFO	<b>✓</b> SECURE	<b>ℚ</b> HOTSPOT
2	43	1	2	2



**File Name:** 6.28.0.apk **Size:** 123.69MB

**MD5**: 3e5151062258e6a6637324ca8fb1d923

#### **i** APP INFORMATION

App Name: Bark

Package Name: com.pt.bark

Main Activity: com.pt.bark.launch.LauncherActivity

Target SDK: 33 Min SDK: 26 Max SDK:

Android Version Name: 6.28.0 Android Version Code: 508

#### **APP COMPONENTS**

Activities: 17
Services: 23
Receivers: 22
Providers: 5
Exported Activities: 5
Exported Services: 9
Exported Receivers: 12
Exported Providers: 0

#### **\*** CERTIFICATE INFORMATION

Binary is signed

v1 signature: False

v2 signature: True v3 signature: False

v4 signature: False

X.509 Subject: C=IN, ST=TS, L=HYD, O=PT, OU=PT, CN=Bark

Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2015-11-25 11:23:23+00:00 Valid To: 2040-11-18 11:23:23+00:00

Issuer: C=IN, ST=TS, L=HYD, O=PT, OU=PT, CN=Bark

Serial Number: 0x648c38e3 Hash Algorithm: sha256

md5: d94664e97ccd7a91dbc43dd26070492c sha1: 473f919a69bbad3457af2f0e3afc34e513f103f1

sha256: 8fc32f54be27d340891f7781c769d24a228b40d7709633d7ba7667f19c6391d6

sha512: 3a546102ae24ea98167fc83b6183c30cc9e3889d953d4f009513785391eff16846109725d5057eb9b1f9a3c02c808de0a6b63198b726e3784de91218fdc8ac10

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 8473cf238ce7243e213d6d71e502b4aec702d1230527fe32bf585b959ad7ac38

Found 1 unique certificates



PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.RECEIVE_MMS	dangerous	receive MMS	Allows application to receive and process MMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.MANAGE_EXTERNAL_STORAGE	dangerous	Allows an application a broad access to external storage in scoped storage	Allows an application a broad access to external storage in scoped storage. Intended to be used by few apps that need to manage files on behalf of the users.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.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_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
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.android.browser.permission.READ_HISTORY_BOOKMARKS	unknown	Unknown permission	Unknown permission from android reference
android.permission.QUERY_ALL_PACKAGES	normal	enables querying any normal app on the device.	Allows query of any normal app on the device, regardless of manifest declarations.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.pt.bark.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

# ক্ল APKID ANALYSIS

FILE	DETAILS		
classes.dex	FINDINGS	DETAILS	
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.DEVICE check Build.TAGS check	
	Compiler	r8 without marker (suspicious)	

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

#### BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.pt.bark.launch.LauncherActivity	Schemes: barkchild://,
com.pt.bark.uninstall.UninstallActivity	Schemes: barkuninstall://, Hosts: uninstall,

#### **△** NETWORK SECURITY

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

#### **CERTIFICATE ANALYSIS**

#### HIGH: 0 | WARNING: 0 | INFO: 1

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

#### **Q** MANIFEST ANALYSIS

HIGH: 0 | WARNING: 31 | INFO: 0 | SUPPRESSED: 0

HIGH: U	WARNING: 31   INFO: U   SUPPRESSED: U		
NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Activity (com.pt.bark.phone.PhoneSetupActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	TaskAffinity is set for activity (com.pt.bark.screenshot.ScreenShotActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
5	TaskAffinity is set for activity (com.pt.bark.vpn.VpnPromptActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
6	Activity (com.pt.bark.uninstall.UninstallActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Broadcast Receiver (com.pt.bark.receivers.ExplicitMediaMonitoringReceiver) 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.
8	Broadcast Receiver (com.pt.bark.receivers.AppUpdateReceiver) 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.
9	Broadcast Receiver (com.pt.bark.receivers.RebootReceiver) 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.
10	Broadcast Receiver (com.pt.bark.receivers.WakeUpReceiver) 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.
11	Broadcast Receiver (com.pt.bark.phone.BootstrapReceiver) 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.
12	Broadcast Receiver (com.pt.bark.receivers.DetectNetwork) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Service (com.pt.bark.services.ObserversStartService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
14	Service (com.pt.bark.services.accessibility.BarkAccessibilityService) is Protected by a permission, but the protection level of the permission should be checked.  Permission: android.permission.BIND_ACCESSIBILITY_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.
15	Service (com.pt.bark.services.BarkJobService) 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.
16	Service (com.pt.bark.observer.browser.v2.ChromeObserverV2) 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.
17	Service (com.pt.bark.observer.browser.v2.DefaultBrowserObserverV2) is Protected by a permission, but the protection level of the permission should be checked.  Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
18	Service (com.pt.bark.observer.browser.v2.SamsungBrowserObserverV2) 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.
19	Service (com.pt.bark.observer.message.v2.SmsObserverV2) 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.
20	Service (com.pt.bark.vpn.BarkVpnService) is Protected by a permission, but the protection level of the permission should be checked.  Permission: android.permission.BIND_VPN_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.
21	Broadcast Receiver (com.onesignal.notifications.receivers.FCMBroadcastReceiver) 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.
22	Activity (com.onesignal.notifications.activities.NotificationOpenedActivityHMS) 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
23	Broadcast Receiver (com.onesignal.notifications.receivers.NotificationDismissReceiver) 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.
24	Broadcast Receiver (com.onesignal.notifications.receivers.BootUpReceiver) 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.
25	Broadcast Receiver (com.onesignal.notifications.receivers.UpgradeReceiver) 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.
26	Activity (com.onesignal.notifications.activities.NotificationOpenedActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
27	Activity (com.onesignal.notifications.activities.NotificationOpenedActivityAndroid22AndOlder) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
28	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.
29	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.
30	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.
31	High Intent Priority (999) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

#### </> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/amazonaws/auth/CognitoCachingCredentialsProvider.java com/amazonaws/auth/policy/conditions/ConditionFactory.java com/amazonaws/auth/policy/conditions/S3ConditionFactory.java com/amazonaws/mobileconnectors/cognito/internal/storage/SQLiteL ocalStorage.java com/amazonaws/mobileconnectors/s3/transferutility/TransferService.java com/amazonaws/mobileconnectors/s3/transferutility/TransferTable.ja va com/amazonaws/services/s3/model/S3Object.java com/amazonaws/services/s3/model/S3Object.java com/amazonaws/services/s3/model/S3ObjectSummary.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/manager/RequestManagerRetriever.java com/onesignal/inAppMessages/internal/display/impl/WebViewManag er.java com/onesignal/inAppMessages/internal/prompt/InAppMessagePromptTypes.java com/onesignal/inAppMessages/internal/prompt/impl/InAppMessagePrompt.java com/onesignal/notifications/internal/Notification.java com/onesignal/notifications/internal/Notification.java com/onesignal/notifications/internal/bundle/impl/NotificationBundle Processor.java com/onesignal/notifications/internal/common/NotificationConstants.java com/onesignal/notifications/internal/common/NotificationConstants.java com/onesignal/notifications/internal/common/NotificationConstants.java com/onesignal/notifications/internal/common/NotificationPelper.java com/pt/bark/helper/accessibility/InstagramHelper.java com/pt/bark/helper/accessibility/InstagramHelper.java com/pt/bark/helper/accessibility/InstagramHelper.java com/pt/bark/helper/accessibility/InstagramHelper.java com/pt/bark/helper/accessibility/InstagramHelper.java com/pt/bark/helper/accessibility/InstagramHelper.java com/pt/bark/helper/accessibility/InstagramHelper.java com/pt/bark/helper/accessibility/InstagramHelper.java com/pt/bark/helper/accessibility/InstagramHelper.java com/pt/bark/helper/accessi
				ai/onnxruntime/OrtEnvironment.java com/amazonaws/auth/CognitoCachingCredentialsProvider.java com/amazonaws/mobileconnectors/cognito/internal/storage/Cognito SyncStorage.java com/amazonaws/mobileconnectors/cognito/internal/storage/SQLiteL ocalStorage.java com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java

NO	ISSUE	SEVERITY	STANDARDS	com/bumptech/glide/load/data/LocalUriFetcher.java FührESumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener
2	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/bumptech/glide/load/engine/Decode/path_java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/Glide/Exception.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/ibitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/IbiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/IbiskLruCacheWrapper.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/FiteLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/DefaultOnHeaderDecodedListene r.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderPars er.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderPars er.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/giff/GifDrawableEncoder.java com/bumptech/glide/load/resource/giff/GifDrawableEncoder.java com/bumptech/glide/load/resource/giff/GifDrawableEncoder.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/SequestManagerFragment.java com/bumptech/glide/manager/SequestManagerFragment.java com/bumptech/glide/manager/SequestManagerFragment.java com/bumptech/glide/manager/SupportRequestManagerFragment.

NO	ISSUE	SEVERITY	STANDARDS	com/pt/bark/helper/accessibility/BaseAccessibilityHelper.java Filits/bark/receivers/DetectNetwork.java com/pt/bark/receivers/GeofenceReceiver.java
				com/pt/bark/receivers/RebootReceiver.java com/pt/bark/receivers/WakeUpReceiver.java com/pt/bark/services/GeofenceWorker.java com/pt/bark/services/accessibility/BarkAccessibilityService.java com/pt/bark/workers/ImageHistoryWorker.java com/pt/bark/workers/MmsHistoryWorker.java com/pt/bark/workers/MmsHistoryWorker.java com/pt/bark/workers/SmsHistoryWorker.java com/pt/bark/workers/SmsHistoryWorker.java com/pt/bark/workers/UploadWorker.java com/pt/bark/workers/VideoHistoryWorker.java com/pt/bark/workers/VideoHistoryWorker.java com/pt/bark/workers/VideoHistoryWorker.java io/sentry/SystemOutLogger.java io/sentry/systemOutLogger.java io/sentry/transport/StdoutTransport.java rx/internal/util/IndexedRingBuffer.java rx/plugins/RxJavaHooks.java
3	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	us/bark/sdk/location/BarkLocationManager,java com/amazonaws/services/s3/AmazonS3Client.java com/amazonaws/services/s3/internal/MD5DigestCalculatingInputStre am.java com/amazonaws/util/Md5Utils.java
4	App uses SOLite Database and execute raw SOL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/amazonaws/mobileconnectors/cognito/internal/storage/SQLiteL ocalStorage.java com/amazonaws/mobileconnectors/s3/transferutility/TransferTable.ja va com/onesignal/core/internal/database/impl/OSDatabase.java com/onesignal/session/internal/outcomes/impl/OutcomeTableProvid er.java com/pt/bark/databases/MessagesDB.java
5	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/amazonaws/retry/PredefinedRetryPolicies.java com/onesignal/common/AndroidUtils.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/pt/bark/network/BarkRestClient.java com/pt/bark/network/screentime/ScreenTimeRestClient.java
7	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/pt/bark/vpn/BarkVpnService.java
8	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/sun/jna/Native.java
9	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	io/sentry/util/StringUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	The file or SharedPreference is World Readable. Any. App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/pt/bark/persistence/PersistenceManager.java
11	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	io/sentry/android/core/DefaultAndroidEventProcessor.java
12	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/DefaultAndroidEventProcessor.java io/sentry/android/core/internal/util/RootChecker.java
13	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/RootChecker.java
14	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/onesignal/inAppMessages/internal/display/impl/WebViewManag er.java com/pt/bark/databases/DashboardFragment.java
15	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/onesignal/inAppMessages/internal/display/impl/WebViewManag er.java

#### SHARED LIBRARY BINARY ANALYSIS

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

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	armeabi- v7a/libonnxruntime4j_jni.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	armeabi-v7a/libjnidispatch.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	armeabi-v7a/libsentry- android.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False Warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	armeabi- v7a/libonnxruntime.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	\$ORIGIN high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags, rpath to remove RUNPATH.	True info The binary has the following fortified functions: ['strlen_chk', 'vsnprintf_chk', 'nemcpy_chk', 'read_chk', 'memmove_chk', 'strchr_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	armeabi-v7a/librltun.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	/home/chris/projects/trl- tunnel/libbuilder/android- armv7/libcurlInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- armv7/opensslInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- armv7/caresInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- armv7/zlibInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android-armv7/sentryInstall/lib high  The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags,-rpath to remove RUNPATH.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

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

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	x86_64/libonnxruntime4j_jni.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86_64/libjnidispatch.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	x86_64/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	x86_64/libonnxruntime.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	\$ORIGIN high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags, rpath to remove RUNPATH.	True info The binary has the following fortified functions: ['strlen_chk', 'vsnprintf_chk', 'memcpy_chk', 'read_chk', 'memmmove_chk', 'strchr_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	x86_64/librltun.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	/home/chris/projects/trl- tunnel/libbuilder/android- x86_64/libcurlInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- x86_64/openssIInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- x86_64/caresInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- x86_64/zlibInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android-x86_64/sentryInstall/lib high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags,-rpath to remove RUNPATH.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	x86_64/libsentry.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['vsnprintf_chk', 'strlen_chk', 'read_chk', 'memcpy_chk', 'memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	arm64- v8a/libonnxruntime4j_jni.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	arm64-v8a/libjnidispatch.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .gotplt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	arm64-v8a/libsentry- android.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	arm64-v8a/libonnxruntime.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	\$ORIGIN high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags, rpath to remove RUNPATH.	True info The binary has the following fortified functions: ['_strlen_chk', '_vsnprintf_chk', '_read_chk', '_memmove_chk', '_strchr_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	arm64-v8a/librltun.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	/home/chris/projects/trl- tunnel/libbuilder/android- arm64/libcurlInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- arm64/opensslInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- arm64/caresInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- arm64/zlibInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android-arm64/sentryInstall/lib high  The binary has RPATH set. In certain cases, an attacker can abuse this feature to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RPATH is when it is linked to private libraries in the same package. Remove the compiler option - rpath to remove RPATH.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	arm64-v8a/libsentry.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_memmove_chk', '_memcpy_chk', '_read_chk', '_rstrlen_chk']	False Warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	x86/libonnxruntime4j_jni.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	x86/libjnidispatch.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	x86/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	x86/libonnxruntime.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	\$ORIGIN high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags, rpath to remove RUNPATH.	True info The binary has the following fortified functions: ['_strlen_chk', '_vsnprintf_chk', '_memcpy_chk', '_read_chk', '_memmove_chk', '_strchr_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	x86/librltun.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	/home/chris/projects/trl- tunnel/libbuilder/android- x86/libcurlInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- x86/opensslInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- x86/caresInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- x86/zlibInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android-x86/sentryInstall/lib high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags,- rpath to remove RUNPATH.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	x86/libsentry.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
25	armeabi- v7a/libonnxruntime4j_jni.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False Warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	armeabi-v7a/libjnidispatch.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

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

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
28	armeabi- v7a/libonnxruntime.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	\$ORIGIN high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags, rpath to remove RUNPATH.	True info The binary has the following fortified functions: ['strlen_chk', 'vsnprintf_chk', '_memcpy_chk', '_read_chk', '_memmove_chk', '_strchr_chk']	False Warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	armeabi-v7a/librltun.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .gotplt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	/home/chris/projects/trl- tunnel/libbuilder/android- armv7/libcurlInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- armv7/opensslInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- armv7/caresInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- armv7/zlibInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android-armv7/sentryInstall/lib high  The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags,-rpath to remove RUNPATH.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

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

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
31	x86_64/libonnxruntime4j_jni.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
32	x86_64/libjnidispatch.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .gotplt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
33	x86_64/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
34	x86_64/libonnxruntime.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	\$ORIGIN high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags, rpath to remove RUNPATH.	True info The binary has the following fortified functions: ['strlen_chk', 'vsnprintf_chk', 'read_chk', 'memmove_chk', 'strchr_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
35	x86_64/librltun.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .gotplt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	/home/chris/projects/trl- tunnel/libbuilder/android- x86_64/libcurlInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- x86_64/openssIInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- x86_64/caresInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- x86_64/zliblnstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android-x86_64/sentryInstall/lib high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags,-rpath to remove RUNPATH.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
36	x86_64/libsentry.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['vsnprintf_chk', 'strlen_chk', 'read_chk', 'memcpy_chk', 'memmove_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
37	arm64- v8a/libonnxruntime4j_jni.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
38	arm64-v8a/libjnidispatch.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .gotplt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
39	arm64-v8a/libsentry- android.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_vsnprintf_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
40	arm64-v8a/libonnxruntime.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	\$ORIGIN high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags, rpath to remove RUNPATH.	True info The binary has the following fortified functions: ['_strlen_chk', '_vsnprintf_chk', '_memcpy_chk', '_read_chk', '_memmove_chk', '_strchr_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
41	arm64-v8a/librltun.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	/home/chris/projects/trl- tunnel/libbuilder/android- arm64/libcurlInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- arm64/openssIInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- arm64/caresInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- arm64/zlibInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android-arm64/sentryInstall/lib high The binary has RPATH set. In certain cases, an attacker can abuse this feature to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RPATH is when it is linked to private libraries in the same package. Remove the compiler option - rpath to remove RPATH.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
42	arm64-v8a/libsentry.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['_memmove_chk', '_memcpy_chk', '_vsnprintf_chk', '_read_chk', '_strlen_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
43	x86/libonnxruntime4j_jni.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
44	x86/libjnidispatch.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack- protector- all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
45	x86/libsentry-android.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
46	x86/libonnxruntime.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	\$ORIGIN high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags, rpath to remove RUNPATH.	True info The binary has the following fortified functions: ['_strlen_chk', '_vsnprintf_chk', '_read_chk', '_memmove_chk', '_strchr_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
47	x86/libritun.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	/home/chris/projects/trl- tunnel/libbuilder/android- x86/libcurlInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- x86/opensslInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- x86/caresInstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android- x86/zliblnstall/lib:/home/chris/projects/trl- tunnel/libbuilder/android-x86/sentryInstall/lib high The binary has RUNPATH set. In certain cases, an attacker can abuse this feature and or modify environment variables to run arbitrary libraries for code execution and privilege escalation. The only time a library should set RUNPATH is when it is linked to private libraries in the same package. Remove the compiler optionenable-new-dtags,- rpath to remove RUNPATH.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
48	x86/libsentry.so	True info The binary has NX bit set. This marks a memory page non- executable making attacker injected shellcode non- executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option - D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

# ■ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION	
----	------------	-------------	---------	-------------	--

### **\*: ::** ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	14/24	android.permission.READ_SMS, android.permission.RECEIVE_SMS, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.READ_CONTACTS, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.READ_PHONE_STATE, android.permission.WAKE_LOCK, android.permission.VIBRATE
Other Common Permissions	6/45	android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.FOREGROUND_SERVICE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID

### 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

## **Q** DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
bark-android-child.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
www.bing.com	ok	IP: 2.23.97.178 Country: Austria Region: Wien City: Vienna Latitude: 48.208488 Longitude: 16.372080 View: Google Map
ieeexplore.ieee.org	ok	IP: 13.32.110.76 Country: United States of America Region: California City: Los Angeles Latitude: 34.052231 Longitude: -118.243683 View: Google Map
s3.amazonaws.com	ok	IP: 16.182.35.88  Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map

DOMAIN	STATUS	GEOLOCATION
api.onesignal.com	ok	IP: 104.16.160.145  Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 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
screentime.bark.us	ok	IP: 54.235.67.74  Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
www.ngs.ac.uk	ok	IP: 130.246.140.235  Country: United Kingdom of Great Britain and Northern Ireland Region: England City: Appleton Latitude: 51.709511 Longitude: -1.361360 View: Google Map
www.google.com	ok	IP: 142.251.36.228  Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.amazon.com	ok	IP: 13.32.134.214  Country: United States of America Region: California City: Los Angeles Latitude: 34.052231 Longitude: -118.243683 View: Google Map

DOMAIN	STATUS	GEOLOCATION
bark.us	ok	IP: 3.225.133.7  Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
acs.amazonaws.com	ok	No Geolocation information available.
www.openssl.org	ok	IP: 34.49.79.89 Country: United States of America Region: Texas City: Houston Latitude: 29.941401 Longitude: -95.344498 View: Google Map
www.bark.us	ok	IP: 44.214.215.19 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
sentry.bark.us	ok	IP: 54.227.147.95 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
docs.nvidia.com	ok	IP: 104.83.4.17 Country: Austria Region: Wien City: Vienna Latitude: 48.208488 Longitude: 16.372080 View: Google Map
s3-us-west-1.amazonaws.com	ok	IP: 52.219.194.104 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map

# FIREBASE DATABASES

FIREBASE URL	DETAILS
https://bark-android-child.firebaseio.com	info App talks to a Firebase Database.

## **EMAILS**

EMAIL	FILE
ftp@example.com 48ac93f53ca28191c797@sentry.bark	lib/armeabi-v7a/librltun.so
ftp@example.com 48ac93f53ca28191c797@sentry.bark	lib/x86_64/librltun.so
ftp@example.com 48ac93f53ca28191c797@sentry.bark	lib/arm64-v8a/librltun.so
ftp@example.com 48ac93f53ca28191c797@sentry.bark	lib/x86/librltun.so
ftp@example.com 48ac93f53ca28191c797@sentry.bark	apktool_out/lib/armeabi-v7a/librltun.so
ftp@example.com 48ac93f53ca28191c797@sentry.bark	apktool_out/lib/x86_64/librltun.so
ftp@example.com 48ac93f53ca28191c797@sentry.bark	apktool_out/lib/arm64-v8a/librltun.so
ftp@example.com 48ac93f53ca28191c797@sentry.bark	apktool_out/lib/x86/librltun.so

# # TRACKERS

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
OneSignal		https://reports.exodus-privacy.eu.org/trackers/193

TRACKER	CATEGORIES	URL
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

### HARDCODED SECRETS

# POSSIBLE SECRETS "google\_api\_key": "AlzaSyDmmFwRsOpvirgrslaDft-wkomplCtZvV4" "google\_crash\_reporting\_api\_key": "AlzaSyDmmFwRsOpvirgrslaDft-wkomplCtZvV4" "firebase\_database\_uri": "https://bark-android-child.firebaselo.com" 5181942b9ebc31ce68dacb56c16fd79f ebef3e65-6666-4de1-b779-8033f7Zfffe9 c682b8144a8dd52bc1ad63 7126014c-0f1e-4419-b331-4abd0a7f8fc5 258EAFA5-E914-47DA-95CA-CSAB0DC85B11 ae2044fb577e65ee8bb576c48a2f06e

### > PLAYSTORE INFORMATION

Title: Bark for Chromebooks

Score: 1.8529412 Installs: 10,000+ Price: 0 Android Version Support: Category: Tools Play Store URL: com.pt.bark

Developer Details: Bark Technologies, Inc., Bark+Technologies,+Inc., PO Box 18603 Atlanta, GA 31126, https://www.bark.us, help@bark.us,

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

### **Description:**

Bark uses advanced algorithms to detect and proactively alert parents to issues your family faces online, such as bullying, predators, sexual content, and more. You can stay on top of your child's location using our real-time map or location check-in features. We also monitor social media and also block access to specific web sites and harmful categories while only alerting you to potential problems. Bark's approach saves parents valuable time and helps build trust between families. Using our check-in feature, you can simply press a button to send your current location to your parent. This offers you peace of mind that your child has made it safely to their destination. To do this, the Bark app will need access to photos/videos, contacts, the list of installed apps on the device, and browsing history. We use Accessibility to monitor your child's third-party message data. Additionally, we use a VPN service to monitor your child's internet traffic for harmful content even when the app is not in use. Bark collects read and write call log data to enable contact monitoring even when the app is not in use

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

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