



## ANDROID STATIC ANALYSIS REPORT



 Quabble (2.3.5)

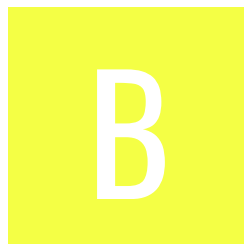
File Name: com.museLIVE.quabbleapp\_2030051.apk

Package Name: com.museLIVE.quabbleapp

Scan Date: Aug. 31, 2025, 7:30 a.m.






App Security Score: 50/100 (MEDIUM RISK)

Grade:



Trackers Detection: 8/432

## FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
4	28	3	3	1

## FILE INFORMATION

**File Name:** com.museLIVE.quabbleapp\_2030051.apk

**Size:** 119.52MB

**MD5:** 8765a7fe1c32c7ea31d2aee05bdfd0ab

**SHA1:** 5a45f649366d2271bf1852c1c20c2ee1f8096aa0

**SHA256:** 804a3de07bd7280fdb79829ff074a119051aa37d99954b47bf915f289ddab393

## APP INFORMATION

**App Name:** Quabble

**Package Name:** com.museLIVE.quabbleapp

**Main Activity:** com.museLIVE.quak\_flutter.MainActivity

**Target SDK:** 34

**Min SDK:** 28

**Max SDK:**

**Android Version Name:** 2.3.5

Android Version Code: 2030051

## APP COMPONENTS

Activities: 20

Services: 20

Receivers: 22

Providers: 9

Exported Activities: 4

Exported Services: 3

Exported Receivers: 8

Exported Providers: 0

## CERTIFICATE INFORMATION

Binary is signed

v1 signature: False

v2 signature: False

v3 signature: True

v4 signature: False

X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Signature Algorithm: rsassa\_pkcs1v15

Valid From: 2023-04-05 23:39:03+00:00

Valid To: 2053-04-05 23:39:03+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0x3ded0d2db9174a8fedf0b48f83e61941bdeaf8a4

Hash Algorithm: sha256

md5: 06283988a9f56d716ea5fd0f2500d67c

sha1: cc3f6eeb8f9017e11e0bf88e5e793bd6ee196fdf

sha256: cee4b4d1b54b9a25be01b653fb314bbfc4e635bdb56e771b29415f695bf509aa

sha512: 3a6a20e609068acbd1ce74559bcec30c9f8c3c8e2999a0eb1f2fbd9e94541f3309ad5b3e8efd109afbd8dba0eb9742620a8a5ac4129ae4b101b3cf7b3948bdf

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 579449ffaaf9d9f6d34c544c6c20b881921abf130697c5d8ccd3d0d0f451e33d

Found 1 unique certificates

## ☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.VIDEO_CAPTURE	unknown	Unknown permission	Unknown permission from android reference
android.permission.AUDIO_CAPTURE	unknown	Unknown permission	Unknown permission from android reference
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.USE_EXACT_ALARM	normal	allows using exact alarms without user permission.	Allows apps to use exact alarms just like with SCHEDULE_EXACT_ALARM but without needing to request this permission from the user. This is only intended for use by apps that rely on exact alarms for their core functionality. You should continue using SCHEDULE_EXACT_ALARM if your app needs exact alarms for a secondary feature that users may or may not use within your app. Keep in mind that this is a powerful permission and app stores may enforce policies to audit and review the use of this permission. Such audits may involve removal from the app store if the app is found to be misusing this permission.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.museLIVE.quabbleapp.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
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.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_AD SERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_AD SERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.museLIVE.quabbleapp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

## APKID ANALYSIS

FILE	DETAILS
------	---------

FILE	DETAILS	
classes.dex	<b>FINDINGS</b>	<b>DETAILS</b>
	yara_issue	yara issue - dex file recognized by apkid but not yara module
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check network operator name check device ID check ro.hardware check ro.kernel.qemu check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	unknown (please file detection issue!)

FILE	DETAILS	
classes2.dex	FINDINGS	DETAILS
	yara_issue	yara issue - dex file recognized by apkid but not yara module
	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	unknown (please file detection issue!)

## BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.museLIVE.quak_flutter.MainActivity	Schemes: quabbleapp://, https://, Hosts: open, quabble.app.link, quabble-alternate.app.link, quabble.test-app.link, quabble-alternate.test-app.link,

ACTIVITY	INTENT
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.museLIVE.quabbleapp,

## NETWORK SECURITY

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

## CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	<a href="#">info</a>	Application is signed with a code signing certificate

## MANIFEST ANALYSIS

HIGH: 2 | WARNING: 18 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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	App Link assetlinks.json file not found [android:name=com.museLIVE.quak_flutter.MainActivity] [android:host=https://quabble.test-app.link]	high	App Link asset verification URL (https://quabble.test-app.link/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 200). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
4	<p>App Link assetlinks.json file not found</p> <p>[android:name=com.museLIVE.quak_flutter.MainActivity]</p> <p>[android:host=https://quabble-alternate.test-app.link]</p>	high	<p>App Link asset verification URL (https://quabble-alternate.test-app.link/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 200). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.</p>
5	<p>Service (com.ryanheise.audioservice.AudioService) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: android.permission.FOREGROUND_SERVICE</p> <p>[android:exported=true]</p>	warning	<p>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.</p>

NO	ISSUE	SEVERITY	DESCRIPTION
6	Broadcast Receiver (io.flutter.plugins.firebase.messaging.FlutterFirebaseMessagingReceiver) 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.
7	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.
8	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.
9	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.



NO	ISSUE	SEVERITY	DESCRIPTION
10	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.
11	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.
12	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.
13	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.
14	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.
15	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
16	<p>Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]</p>	warning	<p>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.</p>
17	<p>Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]</p>	warning	<p>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.</p>

NO	ISSUE	SEVERITY	DESCRIPTION
18	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
19	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
20	High Intent Priority (999) - {1} Hit(s) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

## </> CODE ANALYSIS

HIGH: 1 | WARNING: 9 | INFO: 3 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a0/c.java a1/a.java bitter/jnibridge/JNIBridge.java c1/h.java cc/d.java com/appsflyer/appsflyersdk/AppsflyerSdkPlug in.java com/appsflyer/internal/AFc1qSDK.java com/appsflyer/internal/AFf1kSDK.java com/appsflyer/internal/AFg1jSDK.java com/baseflow/geolocator/GeolocatorLocation Service.java com/baseflow/geolocator/a.java com/baseflow/geolocator/b.java com/baseflow/geolocator/j.java com/baseflow/geolocator/m.java com/dexterous/flutterlocalnotifications/Flutter LocalNotificationsPlugin.java com/dexterous/flutterlocalnotifications/Sched uledNotificationReceiver.java com/onesignal/common/c.java com/onesignal/debug/internal/logging/a.java com/pichillilorenzo/flutter_inappwebview_an droid/MyCookieManager.java com/pichillilorenzo/flutter_inappwebview_an droid/Util.java com/pichillilorenzo/flutter_inappwebview_an droid/chrome_custom_tabs/ChromeCustomTa bsActivity.java com/pichillilorenzo/flutter_inappwebview_an droid/chrome_custom_tabs/CustomTabsHelp er.java com/pichillilorenzo/flutter_inappwebview_an droid/content_blocker/ContentBlockerHandler .java com/pichillilorenzo/flutter_inappwebview_an droid/in_app_browser/InAppBrowserActivity.j

NO	ISSUE	SEVERITY	STANDARDS	FILES
				<div>ava</div> <div>com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserManager.java</div> <div>com/pichillilorenzo/flutter_inappwebview_android/service_worker/ServiceWorkerManager.java</div> <div>com/pichillilorenzo/flutter_inappwebview_android/types/WebViewAssetLoaderExt.java</div> <div>com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/FlutterWebView.java</div> <div>com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebView.java</div> <div>com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InputAwareWebView.java</div> <div>com/unity3d/player/f.java</div> <div>com/unity3d/player/n.java</div> <div>com/xraph/plugin/flutter_unity_widget/CustomUnityPlayer.java</div> <div>com/xraph/plugin/flutter_unity_widget/FlutterUnityWidgetController.java</div> <div>com/xraph/plugin/flutter_unity_widget/FlutterUnityWidgetPlugin.java</div> <div>com/xraph/plugin/flutter_unity_widget/OverrideUnityActivity.java</div> <div>com/xraph/plugin/flutter_unity_widget/UnityPlayerUtils.java</div> <div>d0/a.java</div> <div>d1/d.java</div> <div>d3/e.java</div> <div>d3/f.java</div> <div>e1/a.java</div> <div>e4/b.java</div> <div>e7/i.java</div> <div>f/d.java</div> <div>f3/a.java</div> <div>f4/a.java</div>

NO	ISSUE	SEVERITY	STANDARDS	FILES
				h1/a.java h1/b.java h3/j.java h3/m.java io/flutter/Log.java io/flutter/app/FlutterActivityDelegate.java io/flutter/embedding/android/FlutterActivity.j ava io/flutter/embedding/android/FlutterImageVie w.java io/flutter/embedding/android/FlutterSplashVi ew.java io/flutter/embedding/android/FlutterSurfaceVi ew.java io/flutter/embedding/android/FlutterTextureV iew.java io/flutter/embedding/android/FlutterView.jav a io/flutter/embedding/android/KeyboardMana ger.java io/flutter/embedding/engine/FlutterEngine.jav a io/flutter/embedding/engine/FlutterJNI.java io/flutter/embedding/engine/dart/DartExecut or.java io/flutter/embedding/engine/dart/DartMessen ger.java io/flutter/embedding/engine/deferredcompon ents/PlayStoreDeferredComponentManager.ja va io/flutter/embedding/engine/loader/FlutterLo ader.java io/flutter/embedding/engine/loader/Resource Extractor.java io/flutter/embedding/engine/plugins/shim/Shi mPluginRegistry.java io/flutter/embedding/engine/plugins/shim/Shi mRegistrar.java io/flutter/embedding/engine/plugins/util/Gen eratedPluginRegister.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	<a href="#">The App logs information. Sensitive information should never be logged.</a>	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	io/flutter/embedding/engine/renderer/FlutterRenderer.java io/flutter/embedding/engine/systemchannels/AccessibilityChannel.java io/flutter/embedding/engine/systemchannels/DeferredComponentChannel.java io/flutter/embedding/engine/systemchannels/KeyEventChannel.java io/flutter/embedding/engine/systemchannels/LifecycleChannel.java io/flutter/embedding/engine/systemchannels/LocalizationChannel.java io/flutter/embedding/engine/systemchannels/MouseCursorChannel.java io/flutter/embedding/engine/systemchannels/NavigationChannel.java io/flutter/embedding/engine/systemchannels/PlatformChannel.java io/flutter/embedding/engine/systemchannels/PlatformViewsChannel.java io/flutter/embedding/engine/systemchannels/RestorationChannel.java io/flutter/embedding/engine/systemchannels/SettingsChannel.java io/flutter/embedding/engine/systemchannels/SpellCheckChannel.java io/flutter/embedding/engine/systemchannels/SystemChannel.java io/flutter/embedding/engine/systemchannels/TextInputChannel.java io/flutter/plugin/common/BasicMessageChannel.java io/flutter/plugin/common/EventChannel.java io/flutter/plugin/common/MethodChannel.java io/flutter/plugin/editing/InputConnectionAdapter.java io/flutter/plugin/editing/ListenableEditingState.java io/flutter/plugin/editing/TextEditingDelta.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/flutter/plugin/editing/TextInputPlugin.java io/flutter/plugin/platform/PlatformViewWrapper.java io/flutter/plugin/platform/PlatformViewsController.java io/flutter/plugin/platform/SingleViewPresentation.java io/flutter/plugins/GeneratedPluginRegistrant.java io/flutter/plugins/androidintent/IntentSender.java io/flutter/plugins/androidintent/MethodCallHandlerImpl.java io/flutter/plugins/firebase/messaging/ContextHolder.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundExecutor.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundService.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingReceiver.java io/flutter/plugins/firebase/messaging/JobIntentService.java io/flutter/plugins/googlemobileads/FluidAdManagerBannerAd.java io/flutter/plugins/googlemobileads/FlutterAdManagerInterstitialAd.java io/flutter/plugins/googlemobileads/FlutterAppOpenAd.java io/flutter/plugins/googlemobileads/FlutterInterstitialAd.java io/flutter/plugins/googlemobileads/FlutterMobileAdsWrapper.java io/flutter/plugins/googlemobileads/FlutterNativeAd.java io/flutter/plugins/googlemobileads/FlutterRewardedAd.java io/flutter/plugins/googlemobileads/GoogleMobileAdsViewFactory.java io/flutter/plugins/googlemobileads/nativetem



NO	ISSUE	SEVERITY	STANDARDS	FILES
				plates/FlutterNativeTemplateFontStyle.java io/flutter/plugins/googlemobileads/nativetem plates/FlutterNativeTemplateType.java io/flutter/plugins/googlemobileads/usermess agingplatform/UserMessagingPlatformManag er.java io/flutter/plugins/imagepicker/FileUtils.java io/flutter/plugins/imagepicker/ImageResizer.ja va io/flutter/plugins/inapppurchase/BillingClient FactoryImpl.java io/flutter/plugins/inapppurchase/MethodCall HandlerImpl.java io/flutter/plugins/inapppurchase/PluginPurch aseListener.java io/flutter/plugins/pathprovider/PathProviderP lugin.java io/flutter/plugins/sharedpreferences/SharedPr eferencesPlugin.java io/flutter/plugins/urllauncher/UrlLauncherPlu gin.java io/flutter/plugins/audioplayer/AudioPlayerPlu gin.java io/flutter/plugins/webviewflutter/InstanceMan ager.java io/flutter/view/AccessibilityBridge.java io/flutter/view/AccessibilityViewEmbedder.jav a io/flutter/view/FlutterNativeView.java io/flutter/view/FlutterView.java io/sentry/android/core/u.java io/sentry/flutter/SentryFlutterPlugin.java io/sentry/x5.java k1/q.java k2/i.java k3/a.java k4/a.java m8/a.java m8/c.java n0/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				nc/i.java n0/c.java o0/d.java o0/e.java oa/c.java org/fmod/FMODAudioDevice.java org/fmod/a.java p2/j.java p3/e0.java p3/l0.java p3/m0.java p3/v.java q0/a.java q2/b.java r/d.java r4/k.java r8/f.java rc/c.java s2/a.java s2/n.java s2/o.java s2/p.java t0/a.java u/f.java u4/a.java vb/a.java w/a.java w1/e.java w2/a.java w2/l.java x0/b.java x1/a.java x2/a.java y0/k0.java y0/o.java y0/o0.java y0/r.java y2/e0.java y2/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				y2/j0.java y3/c.java yb/b0.java yb/d0.java
2	<a href="#">App can read/write to External Storage. Any App can read data written to External Storage.</a>	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	yb/i.java io/flutter/plugins/pathprovider/Messages.java z2/d.java io/flutter/plugins/pathprovider/PathProviderP z2/g.java lugh1.java z200.java p3/l0.java z6/r.java x2/a.java
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	x1/b.java y1/f.java
4	<a href="#">This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.</a>	info	OWASP MASVS: MSTG-STORAGE-10	com/unity3d/player/UnityPlayer.java io/flutter/plugin/editing/InputConnectionAdap tor.java io/flutter/plugin/platform/PlatformPlugin.java nc/m0.java
5	<a href="#">The App uses an insecure Random Number Generator.</a>	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/appsflyer/internal/AFa1zSDK.java com/appsflyer/internal/AFc1fSDK.java com/onesignal/common/AndroidUtils.java d5/q1.java e6/r0.java f/d.java h6/b.java io/sentry/metrics/h.java jd/a.java p3/l0.java y2/n.java
6	<a href="#">MD5 is a weak hash known to have hash collisions.</a>	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	h3/m.java z2/e.java
				com/appsflyer/appsflyersdk/AppsFlyerConsta

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	<a href="#">Files may contain hardcoded sensitive information like usernames, passwords, keys etc.</a>	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	nts.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/dexterous/flutterlocalnotifications/models/NotificationDetails.java com/onesignal/inAppMessages/internal/prompt/impl/b.java com/onesignal/notifications/bridges/a.java com/onesignal/notifications/internal/c.java com/onesignal/notifications/receivers/FCMBroadcastReceiver.java com/pichillilorenzo/flutter_inappwebview_android/credential_database/URLCredentialContract.java com/pichillilorenzo/flutter_inappwebview_android/types/ClientCertResponse.java com/pichillilorenzo/flutter_inappwebview_android/types/HttpAuthResponse.java com/pichillilorenzo/flutter_inappwebview_android/types/URLCredential.java io/flutter/app/FlutterActivityDelegate.java io/flutter/embedding/android/FlutterActivityLaunchConfigs.java io/flutter/embedding/engine/loader/ApplicationInfoLoader.java io/flutter/embedding/engine/loader/FlutterLoader.java io/flutter/embedding/engine/systemchannels/SettingsChannel.java io/flutter/plugin/editing/SpellCheckPlugin.java io/flutter/plugins/firebase/crashlytics/Constants.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundExecutor.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingUtils.java io/flutter/plugins/googlemobileads/FlutterRequestAgentProvider.java io/flutter/plugins/imagepicker/ImagePickerCache.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/flutter/plugins/inappurchase/InAppPurchaseHelper.java p1/d.java ra/a.java ua/e.java
8	<a href="#">SHA-1 is a weak hash known to have hash collisions.</a>	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	ec/a.java io/sentry/util/s.java y3/a.java
9	<a href="#">App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.</a>	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/onesignal/session/internal/outcomes/impl/m.java com/pichillilorenzo/flutter_inappwebview_android/credential_database/CredentialDatabaseHelper.java d1/c.java d9/c.java k2/n.java y4/m0.java y4/t0.java yb/i.java
10	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	f3/j.java l3/b.java y2/b.java y2/l0.java y2/o0.java z3/z.java
11	<a href="#">This App may have root detection capabilities.</a>	secure	OWASP MASVS: MSTG-RESILIENCE-1	e7/w.java io/sentry/android/core/internal/util/n.java
12	<a href="#">The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.</a>	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	j6/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
13	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	io/flutter/plugins/imagepicker/ImagePickerDelegate.java y0/o0.java
14	<a href="#">This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.</a>	secure	OWASP MASVS: MSTG-NETWORK-4	ge/e.java ge/f.java
15	<a href="#">This App may request root (Super User) privileges.</a>	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/n.java

## NIAP ANALYSIS v1.3

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

## BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
---------	-----------	-------	-------

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	d1/d.java e1/a.java e4/a.java e4/b.java f0/m.java io/flutter/embedding/engine/deferredcomponents/PlayStoreDeferredComponentManager.java io/flutter/plugins/pathprovider/PathProviderPlugin.java io/sentry/a5.java io/sentry/cache/c.java io/sentry/p.java io/sentry/w.java j4/a.java x2/a.java y0/o0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	a1/b.java com/appsflyer/internal/AFb1iSDK.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/pichillilorenzo/flutter_inappwebview_android/Util.java com/unity3d/player/n.java dd/k.java dd/m.java e4/b.java f0/m.java h3/m.java i3/j.java io/sentry/cache/c.java io/sentry/config/e.java io/sentry/util/e.java io/sentry/w.java l3/a.java r3/k.java x2/a.java y0/o0.java y6/g.java y6/h0.java z2/g.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	i4/a.java x2/a.java
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFi1mSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1qSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java p3/a.java p3/e0.java p3/l0.java



RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	cc/d.java com/appsflyer/internal/AFi1mSDK.java com/appsflyer/internal/AFi1sSDK.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/onesignal/common/AndroidUtils.java com/onesignal/location/internal/permissions/c.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/EverythingMeHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/HuaweiHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/NovaHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/OPPOHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SonyHomeBadger.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java nc/e.java p3/a.java p3/l0.java p3/m0.java p3/q0.java r2/a.java s2/a.java s2/n.java ua/e.java y6/h0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	cc/d.java com/appsflyer/internal/AFc1cSDK.java com/appsflyer/internal/AFc1jSDK.java com/appsflyer/internal/AFf1sSDK.java com/dexterous/flutterlocalnotifications/FlutterLocalNotificationsPlugin.java com/onesignal/common/AndroidUtils.java com/onesignal/location/internal/permissions/c.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/OPPOHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SonyHomeBadger.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ChromeCustomTabsActivity.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ChromeCustomTabsChannelDelegate.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/TrustedWebActivity.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserManager.java io/flutter/plugins/androidintent/MethodCallHandlerImpl.java io/flutter/plugins/imagepicker/ImagePickerDelegate.java io/flutter/plugins/urllauncher/UrlLauncher.java nc/e.java p3/a.java p3/e0.java p3/l0.java p3/m0.java p3/q0.java r2/a.java rc/b.java s2/a.java s2/n.java s2/p.java u1/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java com/pichillilorenzo/flutter_inappwebview_android/Util.java io/sentry/transport/o.java y2/e0.java y6/s.java
00089	Connect to a URL and receive input stream from the server	command network	com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java io/sentry/transport/o.java k2/l.java y3/c.java y6/s.java
00030	Connect to the remote server through the given URL	network	com/pichillilorenzo/flutter_inappwebview_android/Util.java io/sentry/transport/o.java y6/s.java
00109	Connect to a URL and get the response code	network command	com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java io/sentry/transport/o.java k2/l.java y6/s.java
00094	Connect to a URL and read data from it	command network	com/pichillilorenzo/flutter_inappwebview_android/Util.java y6/s.java
00108	Read the input stream from given URL	network command	y6/s.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/onesignal/common/AndroidUtils.java com/onesignal/location/internal/permissions/c.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserManager.java io/flutter/plugins/url_launcher/UrlLauncher.java nc/e.java p3/I0.java p3/m0.java r2/a.java s2/a.java s2/n.java s2/p.java u1/a.java
00003	Put the compressed bitmap data into JSON object	camera	com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebView.java pc/b.java y2/e0.java
00091	Retrieve data from broadcast	collection	com/appsflyer/internal/AFc1jSDK.java com/onesignal/core/activities/PermissionsActivity.java com/onesignal/notifications/receivers/FCMBroadcastReceiver.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ActionBroadcastReceiver.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ChromeCustomTabsActivity.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserActivity.java nc/e.java p3/e0.java ua/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00012	Read data and put it into a buffer stream	file	h3/m.java io/sentry/config/e.java io/sentry/util/e.java io/sentry/w.java z2/g.java
00009	Put data in cursor to JSON object	file	k2/n.java p3/l0.java
00004	Get filename and put it to JSON object	file collection	i3/f.java k2/n.java r3/c.java v3/a.java
00028	Read file from assets directory	file	io/flutter/embedding/engine/loader/ResourceExtractor.java y6/c.java
00015	Put buffer stream (data) to JSON object	file	p3/l0.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/AFh1cSDK.java com/onesignal/common/f.java k2/p.java nc/o0.java p3/l0.java
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFi1oSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java p3/e0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFi1oSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java p3/e0.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1sSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java p3/e0.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFi1oSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java p3/e0.java
00187	Query a URI and check the result	collection sms calllog calendar	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java p3/e0.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFi1oSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java p3/e0.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1sSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java p3/e0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1jSDK.java
00132	Query The ISO country code	telephony collection	k2/p.java z6/n0.java
00161	Perform accessibility service action on accessibility node info	accessibility service	io/flutter/view/AccessibilityBridge.java io/flutter/view/AccessibilityViewEmbedder.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java
00209	Get pixels from the latest rendered image	collection	io/flutter/embedding/android/FlutterImageView.java
00210	Copy pixels from the latest rendered image into a Bitmap	collection	io/flutter/embedding/android/FlutterImageView.java
00014	Read file into a stream and put it into a JSON object	file	i3/j.java l3/a.java r3/k.java
00162	Create InetAddress object and connecting to it	socket	ge/a.java ge/f.java
00163	Create new Socket and connecting to it	socket	ge/a.java ge/f.java
00016	Get location info of the device and put it to JSON object	location collection	k2/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00102	Set the phone speaker on	command	sb/b.java
00056	Modify voice volume	control	sb/b.java
00104	Check if the given path is directory	file	io/flutter/embedding/engine/deferredcomponents/PlayStoreDeferredComponentManager.java
00123	Save the response to JSON after connecting to the remote server	network command	com/pichillilorenzo/flutter_inappwebview_android/Util.java
00137	Get last known location of the device	location collection	k2/p.java
00115	Get last known location of the device	collection location	k2/p.java
00202	Make a phone call	control	s2/p.java
00203	Put a phone number into an intent	control	s2/p.java
00125	Check if the given file path exist	file	i3/f.java

## FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for <a href="https://firebaseremoteconfig.googleapis.com/v1/projects/14159949311/namespaces/firebase:fetch?key=AlzaSyAawQC9ONnkWcNrevU5BVT1Orda3QfOCZg">https://firebaseremoteconfig.googleapis.com/v1/projects/14159949311/namespaces/firebase:fetch?key=AlzaSyAawQC9ONnkWcNrevU5BVT1Orda3QfOCZg</a> . This is indicated by the response: {'state': 'NO_TEMPLATE'}



## 🚫 ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.INTERNET, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE
Other Common Permissions	6/44	android.permission.MODIFY_AUDIO_SETTINGS, android.permission.FOREGROUND_SERVICE, android.permission.ACCESS_NOTIFICATION_POLICY, com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

### Malware Permissions:

Top permissions that are widely abused by known malware.

### Other Common Permissions:

Permissions that are commonly abused by known malware.

## ! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION
--------	----------------

## 🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
help.branch.io	ok	<b>IP:</b> 104.18.20.218 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Francisco <b>Latitude:</b> 37.775700 <b>Longitude:</b> -122.395203 <b>View:</b> <a href="#">Google Map</a>
graph-video.s	ok	No Geolocation information available.
sinapps.s	ok	No Geolocation information available.
api.eu.amplitude.com	ok	<b>IP:</b> 18.194.171.138 <b>Country:</b> Germany <b>Region:</b> Hessen <b>City:</b> Frankfurt am Main <b>Latitude:</b> 50.115520 <b>Longitude:</b> 8.684170 <b>View:</b> <a href="#">Google Map</a>
issuetracker.google.com	ok	<b>IP:</b> 142.250.201.174 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
.facebook.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	<b>IP:</b> 142.250.189.14 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
graph.s	ok	No Geolocation information available.
default.url	ok	No Geolocation information available.
sdl sdk.s	ok	No Geolocation information available.
www.w3.org	ok	<b>IP:</b> 104.18.23.19 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Francisco <b>Latitude:</b> 37.775700 <b>Longitude:</b> -122.395203 <b>View:</b> <a href="#">Google Map</a>
github.com	ok	<b>IP:</b> 140.82.114.3 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Francisco <b>Latitude:</b> 37.775700 <b>Longitude:</b> -122.395203 <b>View:</b> <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
facebook.com	ok	<b>IP:</b> 31.13.70.36 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Los Angeles <b>Latitude:</b> 34.052231 <b>Longitude:</b> -118.243683 <b>View:</b> <a href="#">Google Map</a>
sconversions.s	ok	No Geolocation information available.
simpimpression.s	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.
developer.android.com	ok	<b>IP:</b> 142.250.217.142 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
10.0.2.2	ok	<b>IP:</b> 10.0.2.2 <b>Country:</b> - <b>Region:</b> - <b>City:</b> - <b>Latitude:</b> 0.000000 <b>Longitude:</b> 0.000000 <b>View:</b> <a href="#">Google Map</a>
sattr.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
developers.facebook.com	ok	<b>IP:</b> 31.13.70.1 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Los Angeles <b>Latitude:</b> 34.052231 <b>Longitude:</b> -118.243683 <b>View:</b> <a href="#">Google Map</a>
branch.app.link	ok	<b>IP:</b> 18.238.109.80 <b>Country:</b> United States of America <b>Region:</b> Washington <b>City:</b> Seattle <b>Latitude:</b> 47.627499 <b>Longitude:</b> -122.346199 <b>View:</b> <a href="#">Google Map</a>
www.example.com	ok	<b>IP:</b> 23.220.73.43 <b>Country:</b> Colombia <b>Region:</b> Antioquia <b>City:</b> Medellin <b>Latitude:</b> 6.251840 <b>Longitude:</b> -75.563591 <b>View:</b> <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
api3-eu.branch.io	ok	<b>IP:</b> 18.155.173.13 <b>Country:</b> United States of America <b>Region:</b> Washington <b>City:</b> Seattle <b>Latitude:</b> 47.627499 <b>Longitude:</b> -122.346199 <b>View:</b> <a href="#">Google Map</a>
bnc.lt	ok	<b>IP:</b> 18.238.109.128 <b>Country:</b> United States of America <b>Region:</b> Washington <b>City:</b> Seattle <b>Latitude:</b> 47.627499 <b>Longitude:</b> -122.346199 <b>View:</b> <a href="#">Google Map</a>
cdn.branch.io	ok	<b>IP:</b> 18.238.109.76 <b>Country:</b> United States of America <b>Region:</b> Washington <b>City:</b> Seattle <b>Latitude:</b> 47.627499 <b>Longitude:</b> -122.346199 <b>View:</b> <a href="#">Google Map</a>
api2.amplitude.com	ok	<b>IP:</b> 54.186.227.18 <b>Country:</b> United States of America <b>Region:</b> Oregon <b>City:</b> Portland <b>Latitude:</b> 45.523449 <b>Longitude:</b> -122.676208 <b>View:</b> <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
api.onesignal.com	ok	<b>IP:</b> 104.16.160.145 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Francisco <b>Latitude:</b> 37.775700 <b>Longitude:</b> -122.395203 <b>View:</b> <a href="#">Google Map</a>
developer.apple.com	ok	<b>IP:</b> 17.253.83.133 <b>Country:</b> Singapore <b>Region:</b> Singapore <b>City:</b> Singapore <b>Latitude:</b> 1.289670 <b>Longitude:</b> 103.850067 <b>View:</b> <a href="#">Google Map</a>
slaunches.s	ok	No Geolocation information available.
ns.adobe.com	ok	No Geolocation information available.
schemas.microsoft.com	ok	<b>IP:</b> 13.107.246.71 <b>Country:</b> Netherlands <b>Region:</b> Noord-Holland <b>City:</b> Amsterdam <b>Latitude:</b> 52.374031 <b>Longitude:</b> 4.889690 <b>View:</b> <a href="#">Google Map</a>
sapp.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
regionconfig.eu.amplitude.com	ok	<b>IP:</b> 18.238.96.4 <b>Country:</b> United States of America <b>Region:</b> Washington <b>City:</b> Seattle <b>Latitude:</b> 47.627499 <b>Longitude:</b> -122.346199 <b>View:</b> <a href="#">Google Map</a>
api2.branch.io	ok	<b>IP:</b> 18.238.109.16 <b>Country:</b> United States of America <b>Region:</b> Washington <b>City:</b> Seattle <b>Latitude:</b> 47.627499 <b>Longitude:</b> -122.346199 <b>View:</b> <a href="#">Google Map</a>
www.facebook.com	ok	<b>IP:</b> 31.13.70.36 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Los Angeles <b>Latitude:</b> 34.052231 <b>Longitude:</b> -118.243683 <b>View:</b> <a href="#">Google Map</a>
regionconfig.amplitude.com	ok	<b>IP:</b> 18.155.173.65 <b>Country:</b> United States of America <b>Region:</b> Washington <b>City:</b> Seattle <b>Latitude:</b> 47.627499 <b>Longitude:</b> -122.346199 <b>View:</b> <a href="#">Google Map</a>
svalidate.s	ok	No Geolocation information available.



DOMAIN	STATUS	GEOLOCATION
aomedia.org	ok	<b>IP:</b> 185.199.111.153 <b>Country:</b> United States of America <b>Region:</b> Pennsylvania <b>City:</b> California <b>Latitude:</b> 40.065632 <b>Longitude:</b> -79.891708 <b>View:</b> <a href="#">Google Map</a>

## TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	<a href="https://reports.exodus-privacy.eu.org/trackers/12">https://reports.exodus-privacy.eu.org/trackers/12</a>
Facebook Login	Identification	<a href="https://reports.exodus-privacy.eu.org/trackers/67">https://reports.exodus-privacy.eu.org/trackers/67</a>
Facebook Share		<a href="https://reports.exodus-privacy.eu.org/trackers/70">https://reports.exodus-privacy.eu.org/trackers/70</a>
Google AdMob	Advertisement	<a href="https://reports.exodus-privacy.eu.org/trackers/312">https://reports.exodus-privacy.eu.org/trackers/312</a>
Google CrashLytics	Crash reporting	<a href="https://reports.exodus-privacy.eu.org/trackers/27">https://reports.exodus-privacy.eu.org/trackers/27</a>
Google Firebase Analytics	Analytics	<a href="https://reports.exodus-privacy.eu.org/trackers/49">https://reports.exodus-privacy.eu.org/trackers/49</a>
OneSignal		<a href="https://reports.exodus-privacy.eu.org/trackers/193">https://reports.exodus-privacy.eu.org/trackers/193</a>
Sentry	Crash reporting	<a href="https://reports.exodus-privacy.eu.org/trackers/447">https://reports.exodus-privacy.eu.org/trackers/447</a>



POSSIBLE SECRETS
"facebook_client_token" : "bd2300e96a817dffaf51b578fb3e5703"
"google_api_key" : "AlzaSyAawQC9ONnkWcNrevU5BVT1Orda3QfOCZg"
"google_crash_reporting_api_key" : "AlzaSyAawQC9ONnkWcNrevU5BVT1Orda3QfOCZg"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afb17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
igtly1RPdtSwwFM0MzyB8nIIZ5v2CDGgVI3q8yVZqtR6IDXyW0WRS0Qe3gwz+vAY
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
5go+5djzPwtL428hPcvMvoz2IsnUZf/hKfz19p3YdYFOxVa6hNCHvBHHDAAKyIvFa
uJP+jOkstXYybMCjk2UNbhttr8UNt74vp0QYS1O6gudZhXLs5QWRNg4TXtm9Zlmd
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
z+xFAIC1JJ/Cxy2NWKsDbM4NUy8C7neyeQZVK5Q+YiU=
Cm9abA75+yjPIHfzXp8tlbRygnDIUgXcqbjtuqZQZF0=
ml62XAU6hkSJHBt5knDDIPT1Fqr4dlfaZ+n4XjM0AiKKuoUuq7VAlzpsb6e8DhEf
O5il9ZZjBEgliHjallNs+C68w5c7XQAr0WlqU8TcTvl=

POSSIBLE SECRETS
470fa2b4ae81cd56ecbcd9735803434cec591fa
ML9A2VCkghGr4j9IIk2plgQeFzpoPp+ogmQdRjzLv80=
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
6zld8d9NaX80sl0M8SJ9SnojSxUu8C5CZiLILGnPeUQ=
P15x9IMUDXyyNpUGLmOqAZQoNBvbyJrmT9y8WtTTpOumBqbGOWGo0g3udSuM87xK
8BESx6lpu/rT8vpssHW7TVG8DbeYQuIEHs4g7WxmlH0=
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xILmFuZHIjaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
c56fb7d591ba6704df047fd98f535372fea00211
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed

POSSIBLE SECRETS

308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d01010405003074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b300906035504061302553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d010104050003820101006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a

39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643

8a3c4b262d721acd49a4bf97d5213199c86fa2b9

YqTS1o+C7XbcWZ1ePdCg6lS0viYMM7HzMu7AOHCWvWhuNgyk3szL95200diFQtK9

5jsrpfMyqRCbSKE996yDJ4loI5qc646KRWjOLMSbw18UnvhA6jyNpaXxK5q8Rhj

0QJdUleGFbUoMnZD5fazqxL5C8zhAUBMAOI+v3NY80=

n4163G8iyqIKefOY/ulEeKjctFj1OQ1ggOIXf5yF8QdKTrTHzFKlCjSxQhxSHW08

frdByYsbmru5qm4CvqXIK0tqT/G3yjsT+Pliwl69Mdg=

HoawD5bopn0ma7odT68Aadbw04A5xMOxr41zcgTyqd8=

POSSIBLE SECRETS
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
9b8f518b086098de3d77736f9458a3d2f6f95a37
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
rdAhvKU2UpL3pac61I5593jAaYZYClyk7m7X/gWtAl4=
1j4REQrMq1PMMKcExjoDOWyg20MvDt1CpdYWmGJKkBHqeSdl3MLMTN450gavv1ax
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
19q79G2Hoay9HG8W07mTTjUi2VQ2m7mmzg4dFY+yKc8=
AlzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE
B3EEABB8EE11C2BE770B684D95219ECB
bmivrcLZaHzijOhh62Orf3BoYYHHdZV06MDdRRTWkIM=
8/+tyWwCNq6PB0rUMhC29myQhViveTsZErWXCGX5t00=
9xUiBAiiy8Ja1KXne+aVhWFydz8zlt4gmIBXdZB7YyQ=
1vYYgGa1kSZn3v+ZOQuFaiTzDZd9yTfr5T4txRDI4On2u8cPqYe1RveVsleWcOe5

POSSIBLE SECRETS
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
q1ESzGxy3mMibo5bVHy9HD4wURWKxH/5T27mG6V0M4=
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
115792089210356248762697446949407573530086143415290314195533631308867097853951
2PenHGVoRtCO3QQhfYSZVJz6AfJrwJ5fA2DWAmbwBK4=
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
aYvhO7fsfNuvttwNI2cSMeLS1U8tG39sTRI6fHheAX4=
pzDMLx6PDOtUoiq4sHYJQM6a/7OSGXuSt3rWDXG0BK02rgL9BLEjiNa6eKy3zt3D
IGLGd1/IOSwZNvJFVMee07xTqqB6gC2uy3r930ylvSk=
cc2751449a350f668590264ed76692694a80308a
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449

POSSIBLE SECRETS
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d0101040500308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d3335303930313233333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010019d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
p7ASQw11uHfpr3F0dNO7FI4pxn6scCXfF77Ws5Wp6CJNKFLIAI1vk4wHUcU9a/Df
mRDnAxmcvCylBH5WNtliGg9hBFiZxBdTgSZroxtalc7MFEUgKYH4Tzf+3NcKVcmn
vRn7gel+WCeFJoZ7qQQ1ZFwlsU3+f9F9Kf66GT9NZts=
CRusF084WLXIYQUHrYrs2r/R+2VKdiClv0NdEd7QrkclQLbsoBgPD6jF9jLeUeO0
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
115792089210356248762697446949407573529996955224135760342422259061068512044369
XDZeV64PENx+9tx6tUBxGqpVXuPWj1qf1leYJ9jGf1Q=

POSSIBLE SECRETS
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
yYeL9qjPbrCPTY9ceVqgR0oHzmGoUGeURTuU4UpOsMR57oewRJ2ijf5VjUsh44nU
hxygDHcsiGHhJW67le8OZpQ9Ae4yl4lOwjgTFo0BE4w=
uz1YArq5cHS8AYJUDc1zzIdIMbHyJKwb7tfYne2XDSTiUe1d6tP4aZb4XhmiO5Pa
mdZYlvc02sSKOzn2zFon1K3MqwwFkSMjVA38SM16TyQ=

## PLAYSTORE INFORMATION

**Title:** Quabble: Daily Mental Health

**Score:** 4.5882354 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** [com.museLIVE.quabbleapp](https://play.google.com/store/apps/details?id=com.museLIVE.quabbleapp)

**Developer Details:** museLIVE Inc., museLIVE+Inc., None, <https://quabble.app>, [quabble@muse.live](mailto:quabble@muse.live),

**Release Date:** Aug 6, 2023 **Privacy Policy:** [Privacy link](#)

### Description:

Maintain Daily Mental Health with Just One Joyful App! Quabble is the ultimate self care app for healthy minds! This wellness app makes mental wellness fun, easy, and part of your daily life. With unique routines, mental health games, and community support, it boosts self improvement while helping you manage sleep, meditation, anxiety, depression, journaling, and more—all in one app. No need to juggle multiple apps—just one joyful solution for better mental well-being! - 98% of regular users reported that our mind workouts have helped them manage their mental health - 184k+ mental wellness routines have been completed on Quabble so far What You'll Love About Quabble: 1. HOLISTIC MENTAL WELLNESS TOOLS: Our diverse mental health tools, including mind workouts, personalized wellness routines, goal tracking, virtual pet experiences, daily affirmations, daily motivation, and daily meditation, let you mix and match for a joyful, customized experience. This is the only mental health app you need for consistent mental wellness. 2. INTERACTIVE & CUSTOMIZABLE: Create your own uplifting spaces with Safe Place, Proud Dandelion, and Treasure Box to stay motivated and make mental health management even more joyful. Track your mood effortlessly with the Mood Tracker and nurture a balanced mind-body connection. 3. A CUTE COMPANION-CUM-GUIDE: Get a cute friend-cum-guide to support your daily mental wellness journey. Acting as your Mindfulness Coach, it brings joy while helping you combat anxiety and depression with engaging, therapeutic interactions. 4. ANONYMOUS CONNECTIONS & SUPPORT: Connect anonymously with the caring Quabble community in the Bamboo Forest for unconditional support. Share your journey, find guidance, and experience stress & anxiety relief through a safe, understanding space. - Some of our best mind workouts for holistic mental wellness: (We keep adding to the list) - Clair de Lune: Let Clair de Lune by Claude Debussy lull



you into a restful night's sleep. - Bamboo Forest: It is a place where you can express yourself without fear of judgment by anonymously connecting with the community. - Gratitude Jar: Regular gratitude practice boosts wellbeing, enhances mood, and improves symptoms of depression and anxiety. Use it as your personal gratitude journal for emotional resilience. - Proud Dandelion: As you reflect and write down one thing of yourself you're proud of each day, your dandelion grows, symbolizing your personal growth. - Safe Place: A powerful psychological tool using safe place visualization to cope with challenges. Pair it with sleep meditation for deep relaxation and mental peace. - 1-min Breathing: It activates your body's natural relaxation response by focusing on deep and rhythmic breaths. - Worry Box: It is a cognitive-based toolkit designed for stress and anxiety management. - Mindful Meditation: Mindful Meditation lets you take a break from your busy and stressful day in just 3 minutes. - Mood Diary: It is a proven tool that helps you understand your feelings better, making it easier to handle stress and control your emotions. Quabble Club subscription pricing and terms Enjoy Quabble Basic for free through our Scholarship. But, to unlock the full Quabble experience, join Quabble Club! We offer two auto-renewing subscription plans for Quabble Club: - \$3.99/month - \$19.99/year (less than \$1.7 a month) These prices are for United States customers. Pricing in other countries may vary, and actual charges may be converted to your local currency. The subscription will automatically renew unless turned off in your Device Settings at least 24 hours before the current period ends. Terms and conditions: <https://quabble.app/terms> Privacy policy: <https://quabble.app/privacy>

## SCAN LOGS

Timestamp	Event	Error
2025-08-31 07:30:04	Generating Hashes	OK
2025-08-31 07:30:04	Extracting APK	OK
2025-08-31 07:30:04	Unzipping	OK
2025-08-31 07:30:06	Parsing APK with androguard	OK
2025-08-31 07:30:06	Extracting APK features using aapt/aapt2	OK

2025-08-31 07:30:06	Getting Hardcoded Certificates/Keystores	OK
2025-08-31 07:30:10	Parsing AndroidManifest.xml	OK
2025-08-31 07:30:10	Extracting Manifest Data	OK
2025-08-31 07:30:10	Manifest Analysis Started	OK
2025-08-31 07:30:11	Performing Static Analysis on: Quabble (com.museLIVE.quabbleapp)	OK
2025-08-31 07:30:12	Fetching Details from Play Store: com.museLIVE.quabbleapp	OK
2025-08-31 07:30:13	Checking for Malware Permissions	OK
2025-08-31 07:30:13	Fetching icon path	OK
2025-08-31 07:30:13	Library Binary Analysis Started	OK
2025-08-31 07:30:13	Reading Code Signing Certificate	OK

2025-08-31 07:30:14	Running APKiD 2.1.5	OK
2025-08-31 07:30:18	Detecting Trackers	OK
2025-08-31 07:30:21	Decompiling APK to Java with JADX	OK
2025-08-31 07:59:08	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/8765a7fe1c32c7ea31d2aee05bdfd0ab/java_source', '-q', '-r', '--show-bad-code', '/home/mobsf/.MobSF/uploads/8765a7fe1c32c7ea31d2aee05bdfd0ab/8765a7fe1c32c7ea31d2aee05bdfd0ab.apk'], 999.9999764114618)
2025-08-31 07:59:08	Converting DEX to Smali	OK
2025-08-31 07:59:08	Code Analysis Started on - java_source	OK
2025-08-31 07:59:12	Android SBOM Analysis Completed	OK
2025-08-31 07:59:05	Android SAST Completed	OK
2025-08-31 07:59:05	Android API Analysis Started	OK
2025-08-31 07:59:15	Android API Analysis Completed	OK

2025-08-31 07:59:15	Android Permission Mapping Started	OK
2025-08-31 07:59:22	Android Permission Mapping Completed	OK
2025-08-31 07:59:23	Android Behaviour Analysis Started	OK
2025-08-31 07:59:32	Android Behaviour Analysis Completed	OK
2025-08-31 07:59:32	Extracting Emails and URLs from Source Code	OK
2025-08-31 07:59:34	Email and URL Extraction Completed	OK
2025-08-31 07:59:34	Extracting String data from APK	OK
2025-08-31 07:59:34	Extracting String data from Code	OK
2025-08-31 07:59:34	Extracting String values and entropies from Code	OK
2025-08-31 07:59:38	Performing Malware check on extracted domains	OK
2025-08-31 07:59:41	Saving to Database	OK

---

## Report Generated by - MobSF v4.4.0

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

© 2025 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).