MOBSF

ANDROID STATIC ANALYSIS REPORT

Aira Explorer (2.6.15)

File Name:	Aira Explorer.apk
Package Name:	io.aira.explorer
Scan Date:	Nov. 17, 2024, 11:37 p.m.
App Security Score:	51/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	23	3	2	1

FILE INFORMATION

File Name: Aira Explorer.apk
Size: 9.09MB
MD5: f2cc133ab594eb61e4319bce4e43b906
SHA1: 601b981112fe295f526710ead25f82c31e28ac94
SHA256: cf4c0ade560daec1eb9bc9744b9543cf327556c38a7e098654e05cdcdc1bfc8a

APP INFORMATION

App Name: Aira Explorer
Package Name: io.aira.explorer

Main Activity: io.aira.explorer.MainActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 2.6.15
Android Version Code: 4463

APP COMPONENTS

Activities: 16
Services: 15
Receivers: 8
Providers: 7
Exported Activities: 4
Exported Services: 2
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
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: 2021-10-11 23:48:00+00:00
Valid To: 2051-10-11 23:48:00+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x126a88dfb62ff25c136530ebf0465505353354c
Hash Algorithm: sha256
md5: dfddea7a51ecc98c9dd36d02ad9fc683
sha1: 2921fc01a4cff743b4da69901a890a90e0efde70
sha256: bcf9012e24b13bb268f142bab91ede5cf3bf8da20358224061efb6fb0bd18b8c
sha512: 80f0e1c7f2ddb555a53a07c0550ef1698393c760a5f27861d3eb451627ef5de6e27f3df372c683b4b52c56faaf8db7eba5d88fd2290e44649396a6c6920ff487
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 5dfb2eb14fcdf276974fc4ee7131b8e8bfb8c4e39ed062004a791b68b9276c8a
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
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.CAPTURE_VIDEO_OUTPUT	normal	allows capturing of video output.	Allows an application to capture video output.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_MEDIA_PROJECTION	normal	allows foreground services for media projection.	Allows a regular application to use Service.startForeground with the type "mediaProjection".
android.permission.FOREGROUND_SERVICE_MICROPHONE	normal	permits foreground services with microphone use.	Allows a regular application to use Service.startForeground with the type "microphone".
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.
android.permission.MANAGE_OWN_CALLS	normal	enables a calling app to manage its own calls.	Allows a calling application which manages it own calls through the self-managed ConnectionService APIs.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.ACCESS_ADSERVICES_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_ADSERVICES_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.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
io.aira.explorer.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

classes.dex

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check
Compiler	r8 without marker (suspicious)

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
network operator name check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check
Build.HARDWARE check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
io.aira.explorer.MainActivity	Schemes: https://, Hosts: explorer.aira.io, explorer-auth.aira.io, link.aira.io, qwds-alternate.app.link, Mime Types: image/*,
com.auth0.android.provider.RedirectActivity	Schemes: test://, aira://, Hosts: test-domain, *login.aira.io, Path Prefixes: /android/io.aira.explorer/callback,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

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

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 12 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	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	Activity (com.auth0.android.provider.RedirectActivity) 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	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.
5	TaskAffinity is set for activity (com.hiennv.flutter_callkit_incoming.CallkitIncomingActivity)	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.hiennv.flutter_callkit_incoming.CallkitIncomingActivity) 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.hiennv.flutter_callkit_incoming.CallkitIncomingBroadcastReceiver) 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	Service (com.hiennv.flutter_callkit_incoming.CallkitSoundPlayerService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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.
10	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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
11	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
12	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.
13	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.

</> CODE ANALYSIS

HIGH: **1** | WARNING: **8** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a3/a.java a5/b.java a7/a.java b2/b.java b2/i0.java b2/k.java b2/m0.java b2/o0.java b2/q.java b2/u0.java ba/a.java c2/b.java c5/a.java c5/n.java c5/o.java c5/p.java cd/c.java ce/a.java com/auth0/android/provider/a.java com/auth0/android/provider/b.java com/auth0/android/request/internal/a.java com/auth0/android/request/internal/l.java com/baseflow/geolocator/GeolocatorLocationService.java com/baseflow/geolocator/a.java com/bumptech/glide/b.java com/cloudwebrtc/webrtc/CameraEventsHandler.java com/cloudwebrtc/webrtc/FlutterRTCVideoRenderer.java com/cloudwebrtc/webrtc/FlutterWebRTCPlugin.java com/cloudwebrtc/webrtc/GetUserMediaImpl.java com/cloudwebrtc/webrtc/MethodCallHandlerImpl.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/cloudwebrtc/webrtc/PeerConnectionObserver.java com/cloudwebrtc/webrtc/audio/AudioUtils.java com/cloudwebrtc/webrtc/record/MediaRecorderImpl.java com/cloudwebrtc/webrtc/record/VideoFileRenderer.java com/cloudwebrtc/webrtc/utils/MediaConstraintsUtils.java com/hiennv/flutter_callkit_incoming/CallkitIncomingBroadcastReceiver.java com/hiennv/flutter_callkit_incoming/SharedPreferencesUtilsKt.java com/pichillilorenzo/flutter_inappwebview_android/MyCookieManager.java com/pichillilorenzo/flutter_inappwebview_android/Util.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/ChromeCustomTabsActivity.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java com/pichillilorenzo/flutter_inappwebview_android/content_blocker/ContentBlockerHandler.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserActivity.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserManager.java com/pichillilorenzo/flutter_inappwebview_android/service_worker/ServiceWorkerManager.java com/pichillilorenzo/flutter_inappwebview_android/types/WebViewAssetLoaderExt.java com/pichillilorenzo/flutter_inappwebview_android/webview/JavaScriptBridgeInterface.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/DisplayListenerProxy.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/FlutterWebView.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebView.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebViewChromeClient.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebViewClient.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebViewClientCompat.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebViewRenderProcessClient.java com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InputAwareWebView.java da/a.java e3/b.java e4/a.java e5/a.java e6/a.java e9/r.java ea/a.java f0/g1.java f0/w0.java f2/c.java f3/c.java f5/d.java f5/e.java fa/g.java fa/q.java fa/r.java g/e.java g2/c.java g2/h.java g2/j.java g3/a.java g4/a.java g4/c.java h0/t0.java h5/b.java h5/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				h5/l.java hn/c.java i4/a.java i5/c.java i5/e.java i9/a.java i9/d.java io/flutter/Log.java io/flutter/app/FlutterActivityDelegate.java io/flutter/embedding/android/FlutterActivity.java io/flutter/embedding/android/FlutterActivityAndFragmentDelegate.java io/flutter/embedding/android/FlutterFragment.java io/flutter/embedding/android/FlutterFragmentActivity.java io/flutter/embedding/android/FlutterImageView.java io/flutter/embedding/android/FlutterSurfaceView.java io/flutter/embedding/android/FlutterTextureView.java io/flutter/embedding/android/FlutterView.java io/flutter/embedding/android/KeyEmbedderResponder.java io/flutter/embedding/android/KeyboardManager.java io/flutter/embedding/engine/FlutterEngine.java io/flutter/embedding/engine/FlutterEngineConnectionRegistry.java io/flutter/embedding/engine/FlutterJNI.java io/flutter/embedding/engine/dart/DartExecutor.java io/flutter/embedding/engine/dart/DartMessenger.java io/flutter/embedding/engine/deferredcomponents/PlayStoreDeferredComponentManager.java io/flutter/embedding/engine/loader/FlutterLoader.java io/flutter/embedding/engine/loader/ResourceExtractor.java io/flutter/embedding/engine/plugins/shim/ShimPluginRegistry.java io/flutter/embedding/engine/plugins/shim/ShimRegistrar.java io/flutter/embedding/engine/plugins/util/GeneratedPluginRegister.java io/flutter/embedding/engine/renderer/FlutterRenderer.java io/flutter/embedding/engine/systemchannels/AccessibilityChannel.java io/flutter/embedding/engine/systemchannels/BackGestureChannel.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/InputConnectionAdaptor.java io/flutter/plugin/editing/ListenableEditingState.java io/flutter/plugin/editing/TextEditingDelta.java io/flutter/plugin/editing/TextInputPlugin.java io/flutter/plugin/platform/ImageReaderPlatformViewRenderTarget.java io/flutter/plugin/platform/PlatformPlugin.java io/flutter/plugin/platform/PlatformViewWrapper.java io/flutter/plugin/platform/PlatformViewsController.java io/flutter/plugin/platform/SingleViewPresentation.java io/flutter/plugin/platform/SingleViewWindowManager.java io/flutter/plugins/GeneratedPluginRegistrant.java io/flutter/plugins/camerax/InstanceManager.java io/flutter/plugins/camerax/ObserverFlutterApiWrapper.java io/flutter/plugins/firebase/firebaseremoteconfig/FirebaseRemoteConfigPlugin.java io/flutter/plugins/firebase/firestore/FlutterFirebaseFirestoreMessageCodec.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/flutter/plugins/firebase/firestore/FlutterFirebaseFirestorePlugin.java io/flutter/plugins/firebase/firestore/utils/ExceptionConverter.java io/flutter/plugins/firebase/firestore/utils/PigeonParser.java
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	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/googlesignin/GoogleSignInPlugin.java io/flutter/plugins/imagepicker/FileUtils.java io/flutter/plugins/imagepicker/ImageResizer.java io/flutter/plugins/pathprovider/PathProviderPlugin.java io/flutter/plugins/sharedpreferences/LegacySharedPreferencesPlugin.java io/flutter/plugins/sharedpreferences/SharedPreferencesPlugin.java io/flutter/plugins/urllauncher/UrlLauncherPlugin.java io/flutter/plugins/webviewflutter/DisplayListenerProxy.java io/flutter/plugins/webviewflutter/InstanceManager.java io/flutter/view/AccessibilityBridge.java io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/FlutterNativeView.java io/flutter/view/FlutterView.java io/sentry/android/core/u.java io/sentry/android/replay/s.java io/sentry/android/replay/v.java io/sentry/flutter/SentryFlutter$updateOptions$24.java io/sentry/flutter/SentryFlutterPlugin.java io/sentry/flutter/SentryFlutterReplayRecorder.java j/f.java j/g.java j/k.java j/n.java j/q.java j/t.java j5/h.java j5/i.java j5/k.java j5/q.java j5/z.java j9/o.java ja/b.java k4/b.java k5/j.java k5/k.java k6/b.java kf/j5.java l3/b.java l4/e.java l4/j.java l5/e.java l5/i.java l6/a.java m5/a.java m5/b.java md/a.java md/e.java n/g.java n4/a.java n4/g.java n4/k.java n4/n.java n4/n0.java n5/c.java n5/d.java n5/f.java n5/s.java n5/t.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				n3/c.java nd/a.java o/c.java o1/e.java o1/f.java o1/l.java o1/n.java o1/q.java o1/x.java oc/a.java org/webrtc/audio/WebRtcAudioTrackUtils.java p/d0.java p/d1.java p/e1.java p/g1.java p/k0.java p/m0.java p/n0.java p/q0.java p/r0.java p/w.java p/z.java p1/a.java p5/a.java pc/a.java q3/a.java q5/c.java q5/d.java q5/h.java q5/j.java q5/k.java q5/n.java q5/x.java q6/a.java qc/b.java qc/d.java r1/c.java r1/d.java r1/h.java r3/i.java r9/g.java ra/c5.java s1/e.java s1/g.java s1/h.java s1/i.java s1/l.java s1/m.java sc/d.java t0/a0.java t1/a.java t1/e.java t3/q.java t9/b.java t9/b0.java t9/d.java t9/e0.java t9/f0.java t9/l.java t9/y.java t9/z.java ta/a.java td/i.java td/k.java u/c.java u2/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				u2/b.java u4/c.java u5/d.java u5/j.java u9/b0.java u9/e.java u9/g0.java u9/j.java u9/k.java u9/l0.java u9/o.java u9/x.java uc/a.java v/a.java v/b.java v0/d.java v9/o.java va/a.java w2/a.java w2/b.java w2/b0.java w2/f.java w2/i0.java w2/l0.java w2/n.java w2/o0.java w2/p.java w2/p0.java w2/s0.java w2/t0.java w2/v0.java w2/y0.java w3/a.java w3/e.java w5/e.java w5/f.java w5/k.java w5/l.java w5/n.java w5/o.java w9/g.java w9/n0.java w9/o1.java w9/q0.java w9/r0.java w9/s1.java w9/u1.java w9/w1.java wa/a.java wc/f0.java x1/i.java x1/p.java x2/d.java x4/c.java x4/k.java x4/n.java x5/e.java x6/k.java xa/c0.java xc/a.java xd/c.java xg/d.java y1/d.java y2/c.java y2/d.java y2/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				y2/e.java y9/a.java y9/c.java y9/d1.java y9/f0.java y9/g1.java y9/h1.java y9/i0.java y9/i1.java y9/j.java y9/k1.java y9/q1.java y9/t1.java ya/l.java ya/m.java ya/n.java yc/b0.java yc/d0.java yc/i.java z1/a.java z3/f.java z3/m.java z4/j.java z5/h.java
2	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/u.java
3	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/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 de/r2.java g5/g.java io/flutter/app/FlutterActivityDelegate.java io/flutter/embedding/android/FlutterActivityAndFragmentDelegate.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/auth/Constants.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingBackgroundExecutor.java io/flutter/plugins/firebase/messaging/FlutterFirebaseMessagingUtils.java io/flutter/plugins/imagepicker/ImagePickerCache.java io/flutter/plugins/sharedpreferences/SharedPreferencesPigeonOptions.java j5/d.java j5/p.java j5/x.java u/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	de/b2.java de/e0.java de/g0.java de/t1.java ee/i.java eg/a.java eg/b.java fg/a.java j7/q1.java k8/r0.java ke/f.java ke/h.java n8/b.java ra/dd.java sc/d.java
5	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/pichillilorenzo/flutter_inappwebview_android/credential_database/CredentialDatabaseHelper.java e7/m0.java e7/t0.java ra/mc.java ra/md.java ra/o.java ra/t.java ra/z4.java yc/i.java
6	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	g4/a.java io/flutter/plugins/pathprovider/Messages.java io/flutter/plugins/pathprovider/PathProviderPlugin.java io/sentry/android/core/r0.java p1/b.java pc/a.java qc/b.java qc/d.java
7	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	h0/v.java io/flutter/plugins/camerax/ImageCaptureHostApiImpl.java io/flutter/plugins/camerax/SystemServicesHostApiImpl.java io/flutter/plugins/imagepicker/ImagePickerDelegate.java qc/d.java sa/b.java u2/a.java
8	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/n.java xa/h.java
9	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	p8/a.java
10	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	ra/dd.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	io/flutter/plugin/editing/InputConnectionAdaptor.java io/flutter/plugin/platform/PlatformPlugin.java td/m0.java
12	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	gh/c.java gh/d.java gh/g.java gh/h.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/n.java
14	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	l4/k.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	b5/a.java c5/a.java c5/n.java c5/p.java com/hiennv/flutter_callkit_incoming/CallkitSoundPlayerService.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/imagepicker/ImagePickerDelegate.java io/flutter/plugins/urllauncher/UrlLauncher.java md/e.java n4/j.java n4/n0.java o1/b.java qc/b.java ra/dd.java ra/h8.java ra/r9.java td/e.java u/c.java u9/f.java xd/b.java ya/n.java

RULE ID	BEHAVIOUR	LABEL	FILES
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/pichillilorenzo/flutter_inappwebview_android/webview/in_app_webview/InAppWebViewChromeClient.java g4/a.java o6/a.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	b5/a.java c5/a.java c5/n.java c5/p.java com/pichillilorenzo/flutter_inappwebview_android/in_app_browser/InAppBrowserManager.java io/flutter/plugins/urllauncher/UrlLauncher.java td/e.java u9/f.java
00036	Get resource file from res/raw directory	reflection	b5/a.java c5/a.java c5/n.java com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java d9/h0.java n4/n0.java o1/b.java p/q0.java ra/dd.java td/e.java u9/f.java
00132	Query The ISO country code	telephony collection	e9/n0.java
00092	Send broadcast	command	com/hiennv/flutter_callkit_incoming/FlutterCallkitIncomingPlugin.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/bumptech/glide/load/a.java com/fasterxml/jackson/core/JsonFactory.java com/fasterxml/jackson/core/TokenStreamFactory.java com/fasterxml/jackson/databind/ObjectReader.java com/pichillilorenzo/flutter_inappwebview_android/Util.java d9/g.java d9/h0.java e5/a.java g4/a.java h0/v.java io/sentry/android/core/SentryPerformanceProvider.java io/sentry/android/replay/g.java io/sentry/cache/b.java io/sentry/cache/c.java io/sentry/cache/e.java io/sentry/config/e.java io/sentry/h.java io/sentry/util/e.java j/n.java k6/b.java kf/j2.java kf/u.java lh/p.java m2/m.java n5/f.java o1/f.java qc/d.java s1/g.java s1/m.java u2/a.java u3/i.java xf/h.java xf/j.java
00091	Retrieve data from broadcast	collection	com/hiennv/flutter_callkit_incoming/CallkitIncomingActivity.java com/hiennv/flutter_callkit_incoming/CallkitIncomingBroadcastReceiver.java com/hiennv/flutter_callkit_incoming/CallkitSoundPlayerService.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 md/e.java ra/r9.java td/e.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/cloudwebrtc/webrtc/GetUserMediaImpl.java com/cloudwebrtc/webrtc/record/MediaRecorderImpl.java com/fasterxml/jackson/databind/ser/std/FileSerializer.java g4/a.java h0/v.java io/flutter/embedding/engine/deferredcomponents/PlayStoreDeferredComponentManager.java io/flutter/embedding/engine/loader/FlutterLoader.java io/flutter/plugins/camerax/ImageCaptureHostApiImpl.java io/flutter/plugins/imagepicker/ImagePickerDelegate.java io/flutter/plugins/pathprovider/PathProviderPlugin.java io/sentry/android/core/cache/b.java io/sentry/android/core/r0.java io/sentry/android/core/z.java io/sentry/android/replay/capture/f.java io/sentry/android/replay/g.java io/sentry/cache/b.java io/sentry/cache/c.java io/sentry/cache/e.java io/sentry/flutter/SentryFlutterReplayRecorder.java io/sentry/h.java io/sentry/v.java k6/a.java k6/b.java kf/j2.java kf/n.java kf/u.java m2/m.java p6/a.java qc/d.java u2/a.java wc/f0.java x0/s0.java
00029	Initialize class object dynamically	reflection	b3/f.java
00012	Read data and put it into a buffer stream	file	g4/a.java io/sentry/cache/b.java io/sentry/cache/e.java io/sentry/config/e.java io/sentry/util/e.java kf/j2.java kf/u.java qc/d.java u2/a.java
00028	Read file from assets directory	file	d9/c.java io/flutter/embedding/engine/loader/ResourceExtractor.java
00112	Get the date of the calendar event	collection calendar	com/fasterxml/jackson/databind/ser/std/StdKeySerializers.java com/fasterxml/jackson/databind/util/StdDateFormat.java
00161	Perform accessibility service action on accessibility node info	accessibility service	c2/b.java io/flutter/view/AccessibilityBridge.java io/flutter/view/AccessibilityViewEmbedder.java
00162	Create InetSocketAddress object and connecting to it	socket	gh/b.java gh/h.java

RULE ID	BEHAVIOUR	LABEL	FILES
00163	Create new Socket and connecting to it	socket	gh/b.java gh/h.java
00191	Get messages in the SMS inbox	sms	p/q0.java
00104	Check if the given path is directory	file	io/flutter/embedding/engine/deferredcomponents/PlayStoreDeferredComponentManager.java
00202	Make a phone call	control	c5/p.java
00203	Put a phone number into an intent	control	c5/p.java
00096	Connect to a URL and set request method	command network	com/pichillilorenzo/flutter_inappwebview_android/Util.java d9/s.java io/sentry/transport/o.java u6/d.java
00123	Save the response to JSON after connecting to the remote server	network command	com/pichillilorenzo/flutter_inappwebview_android/Util.java
00030	Connect to the remote server through the given URL	network	com/pichillilorenzo/flutter_inappwebview_android/Util.java d9/s.java h5/j.java io/sentry/transport/o.java
00094	Connect to a URL and read data from it	command network	com/pichillilorenzo/flutter_inappwebview_android/Util.java d9/s.java
00183	Get current camera parameters and change the setting.	camera	com/cloudwebrtc/webrtc/GetUserMediaImpl.java org/webrtc/Camera1Session.java
00192	Get messages in the SMS inbox	sms	pc/a.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
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	i5/c.java wc/o.java
00108	Read the input stream from given URL	network command	d9/s.java ra/k5.java ra/w9.java
00208	Capture the contents of the device screen	collection screen	com/cloudwebrtc/webrtc/OrientationAwareScreenCapturer.java org/webrtc/ScreenCapturerAndroid.java
00078	Get the network operator name	collection telephony	td/o0.java
00177	Check if permission is granted and request it	permission	o1/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	d9/s.java h5/j.java io/sentry/transport/o.java u6/d.java
00109	Connect to a URL and get the response code	network command	d9/s.java h5/j.java i9/d.java io/sentry/transport/o.java r9/f.java u6/d.java
00056	Modify voice volume	control	org/webrtc/audio/WebRtcAudioTrack.java org/webrtc/voiceengine/WebRtcAudioTrack.java rc/b.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 vd/b.java
00004	Get filename and put it to JSON object	file collection	pc/b.java
00102	Set the phone speaker on	command	rc/b.java
00121	Create a directory	file command	p1/a.java
00125	Check if the given file path exist	file	p1/a.java
00147	Get the time of current location	collection location	j/t.java
00075	Get location of the device	collection location	j/t.java
00115	Get last known location of the device	collection location	j/t.java
00114	Create a secure socket connection to the proxy address	network command	bh/f.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	c2/b.java io/flutter/view/AccessibilityViewEmbedder.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/176571152403/namespaces/firebase:fetch?key=AIzaSyCpbbXmBqw-9Rpg7f61To4pf11qbUpvpd8 is enabled. Ensure that the configurations are not sensiti ["snmunoz@gmail.com","sergio.munoz@aira.io","peter.frollo@aira.io","missourircboats@gmail.com","carla.kane@aira.io ","danielle.england@aira.io","alexandra.heatwole@aira.io","tomas.poupin@aira.io","tomas.munoz@aira.io","allie.cockrell@ 'DASH_DEFAULT_TASK_VALIDITY_DURATION': '7', 'DASH_DESKTOP_NOTIFICATIONS': '{"allUsers":true,"testers":["sergio.munoz@aira.io","peter.frollo@aira.io","missourircboats@gmail.com","carla.kane@aira.io ","danielle.england@aira.io","alexanc _klXVBhJpfSSpMGplxOZeg/viewform?usp=pp_url&entry.1288571225=","linkLabel":"Launch Survey"}]', 'DASH_FEEDBACK_EXTERNAL_TOOLS': '{\n "editing": [\n "Google Search",\n "PDF Editor",\n "Photo Editor",\n "MS Word / Google Document",\n Number, Websites Credentials)"},{"key":"ContainsFinancialPii","label":"Financial information","description":"Financial information (Bank Account Number, Credit Card Number, Financial Account Numbers, Tax Identification Number)"},{"key":"Cor 71.17869140580297,42.361116500407554],[-71.17897035554051,42.36124730689414],[-71.17852510884404,42.36192115417693],[-71.17829443886876,42.36185376977386],[-71.17737175896764,42.364105162463304],[-71.1731875129044,42 115.17696986501767,36.10872248598558],[-115.176368482383,36.10902743827762],[-115.17550479455613,36.109110137000755],[-115.17474986741902,36.10907912498958],[-115.17432762003733,36.10879484765414],[-115.173815805028 {"description":"Maps","url":"https://drive.google.com/drive/folders/1qV0o2bs2dlc6n0Fzyx7wf6Wkln_qYyGo?usp=drive_link"}]},{"name":"Disability:IN - Harry Reid International Airport","geofence":{"type":"Polygon","coordinates":[[[-115.15481000 81.65457651348606,30.3246394176737 65],[-81.65696287199981,30.325097709337513],[-81.6582473951228,30.3246295619154 44],[-81.65843008285586,30.32412198902496],[-81.65491905298542,30.32334830489779]]]},"links":[{"description" Document","url":"https://docs.google.com/document/d/1n2QBu9sMlFWkV4cPNPlc9ArH4WR9D284ZlhR9z6W2kU/edit?usp=drive_link"}]},{"name":"ACB - Jacksonville International Airport","geofence":{"type":"Polygon","coordinates":[[[-81.712433 81.47380484275321,28.420441599488356],[-81.45874313794558,28.420630295195892],[-81.46022356192265,28.425989112886384],[-81.46685328668802,28.426838196426075],[-81.46934211540265,28.428989177576838],[-81.473761931913 Maps","url":"https://drive.google.com/drive/folders/1rOT5_5B872u09duUV2ptrWIFXzhfh3Gf?usp=drive_link"},{"description":"General Information Document","url":"https://docs.google.com/document/d/16eMf3j_ubp7BOAS9xBrMvk2iVhhmSvYF\ 81.33240797831006,28.39335877117547],[-81.2786823006365,28.39335877117547],[-81.2786823006365,28.455521658724635],[-81.33240797831006,28.455521658724635]]]},"links":[{"description":"Map of MCO","url":"https://orlandoairports.r 96.83482519179853,33.08724598119832],[-96.83374282795609,33.084675154332416],[-96.8309723737168,33.08525754887941],[-96.82740752399658,33.08410939593546],[-96.8274869635448,33.0891678123823],[-96.83482519179853,33.087 ["peter.frollo@aira.io","sergio.munoz@aira.io","william.ng@aira.io","troy@aira.io","carla.kane@aira.io","joshua.flewellen@aira.io","jeff.armstrong@aira.io","peter.frollo@aira.io","noah.thompson@aira.io","belle.martinez@aira.io","allie.cockrell@a 'DASH_PRIORITY_ACCESS_OFFER_KEYS': '[]', 'DASH_PRIORITY_CLIENT_IDS': '["42324", "35698", "42302", "29752", "23236", "23271"]', 'DASH_PRIORITY_EXPLORERS_IDS': '["45578","47112","37589","35014","47219","42286","47220","47222","47223"," ["sergio.munoz@aira.io","peter.frollo@aira.io","carla.kane@aira.io","danielle.england@aira.io","alexandra.heatwole@aira.io","tomas.poupin@aira.io","tomas.munoz@aira.io","allie.cockrell@aira.io","amanda.nuckoles@aira.io","noah.thompson@ ["cydnee.hardison@aira.io","daniel.applegate@aira.io","jeremiah.mccullough@aira.io","gabi.ruderman@aira.io","zae.singleton@aira.io","madeline.genuardi@aira.io","azalya.felts@aira.io","brigett.ford@aira.io","joshua.lacerna@aira.io","rebekah. '{"buildAiProgram":{"allUsers":true,"testers":["adam.cheney@aira.io","julie.piper@aira.io","nicholas.kane@aira.io","michelle.serr@aira.io","carla.kane@aira.io","danielle.england@aira.io","alexandra.heatwole@aira.io"],"teamworkLink":"https://air the Build AI offer.","It is important that future AI works well for the Blind and Low Vision community. Sharing your recordings with our AI partner will help train future AI.","The details of this offer can be found on our website and in the app program?"],"callActions":{"actionCancelLabel":"Maybe later","actionAcceptLabel":"Sign you up","actionDeclineLabel":"Decline"}},"congratsDialog":{"title":"You successfully signed this explorer up to Build AI","body":[],"actionLabel":"Close"},"remin 'https://docs.google.com/forms/d/e/1FAIpQLScMqmne2d_ltph4w8BCTye3xXHshhQBw6u4olnyI--Zq-QIRw/viewform?usp=pp_url&entry.247094134=', 'WAITLIST_LINK_METARAYBAN': 'https://docs.google.com/forms/d/e/1FAIpQLSc-jXVJEve8OU3Ss

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/25	android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.INTERNET, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.RECORD_AUDIO, android.permission.SYSTEM_ALERT_WINDOW, android.permission.VIBRATE, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	9/44	android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.CHANGE_NETWORK_STATE, android.permission.FOREGROUND_SERVICE, android.permission.MODIFY_AUDIO_SETTINGS, com.google.android.gms.permission.AD_ID, android.permission.ACCESS_NOTIFICATION_POLICY, 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
schemas.microsoft.com	ok	**IP:** 13.107.246.36 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
google.com	ok	**IP:** 142.250.69.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
dashif.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
pagead2.googlesyndication.com	ok	**IP:** 142.250.69.98 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developer.apple.com	ok	**IP:** 17.253.24.198 **Country:** United States of America **Region:** Illinois **City:** Chicago **Latitude:** 41.850029 **Longitude:** -87.650047 **View:** Google Map
api3-eu.branch.io	ok	**IP:** 13.225.195.123 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map
branch.app.link	ok	**IP:** 13.225.195.123 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
github.com	ok	**IP:** 140.82.114.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
app-measurement.com	ok	**IP:** 142.250.69.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.branch.io	ok	**IP:** 13.225.195.28 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map
help.branch.io	ok	**IP:** 104.16.242.118 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.google.com	ok	**IP:** 142.250.69.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developer.android.com	ok	**IP:** 142.251.33.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.69.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.googleadservices.com	ok	**IP:** 142.250.69.34 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gl	ok	**IP:** 142.250.69.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
docs.flutter.dev	ok	**IP:** 199.36.158.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
default.url	ok	No Geolocation information available.
www.example.com	ok	**IP:** 93.184.215.14 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
cdn.branch.io	ok	**IP:** 3.161.213.119 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
accounts.google.com	ok	**IP:** 142.250.31.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.
issuetracker.google.com	ok	**IP:** 142.250.69.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
aomedia.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
bnc.lt	ok	**IP:** 3.162.3.56 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
api2.branch.io	ok	**IP:** 3.161.213.105 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
manage.auth0.com	ok	**IP:** 172.64.148.184 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
auth0.com	ok	**IP:** 104.17.255.182 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com u0013android@android.com0	u9/w.java

TRACKERS

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

HARDCODED SECRETS

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"google_api_key" : "AIzaSyCpbbXmBqw-9Rpg7f61To4pf11qbUpvpd8"
"google_crash_reporting_api_key" : "AIzaSyCpbbXmBqw-9Rpg7f61To4pf11qbUpvpd8"
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
50b64369864aab4a2931d9c5812795ae8699a47b
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
af60eb711bd85bc1e4d3e0a462e074eea428a8
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
115792089210356248762697446949407573529996955224135760342422259061068512044369
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
e2719d58-a985-b3c9-781a-b030af78d30e
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
8081828384858687888 98a8b8c8d8e8f90919293949596979899 9a9b9c9d9e9f
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
23456789abcdefghjkmnpqrstvwxyz
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

POSSIBLE SECRETS
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
a0784d7a4716f3feb4f64e7f4b39bf04
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
9a04f079-9840-4286-ab92-e65be0885f95
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
36864200e0eaf5284d884a0e77d31646
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
bae8e37fc83441b16034566b

PLAYSTORE INFORMATION

Title: Aira Explorer

Score: 3.6666667 **Installs:** 5,000+ **Price:** 0 **Android Version Support:** **Category:** Lifestyle **Play Store URL:** io.aira.explorer

Developer Details: Aira Tech Corp, Aira+Tech+Corp, 3451 Via Montebello, STE 192 PMB 214 Carlsbad, CA 92009, https://aira.io, support@aira.io,

Release Date: Feb 6, 2023 **Privacy Policy:** Privacy link

Description:

What is Aira? Aira is an app that provides on-demand, remote visual interpreting for the blind and low vision community to enhance independence and efficiency. With one tap, connect with a professional Visual Interpreter and work together to accomplish a wide range of tasks. Anytime you encounter an obstacle related to visual information, Aira can assist. It is a trusted and secure tool that can support every realm of your life—on your own terms. How Does Aira Work? Download the free Aira app on your smartphone, create an account, and with one tap connect with a professional Visual Interpreter. Aira streams live video, including your GPS location, and through an integrated dashboard, a Visual Interpreter can immerse themselves in your surroundings. They will use your phone's camera to assist you to better understand your surroundings by navigating, describing, narrating, and reading. They have access to web-based data, including maps, location tracking, search engines, text-based messaging, and even rideshare integration. This is all carefully calibrated to provide our blind and low vision users, who we call Explorers, with a seamless experience. How Does Access AI Work? Access AI is Aira's image chat feature that is free for all Explorers, whether they have a subscription or not. Simply tap the Access AI button on the home screen menu, and then take or upload an image. Send it through the chat, and an AI description will be generated. Ask questions, get refined answers, or for added confidence, use Aira Verify to confirm the description with a Visual Interpreter. Some popular uses of this free tool include getting info about labels, signs, and printed menus, choosing outfits, and getting readings from digital displays like thermostats. How Can I Get Free Aira Minutes?? Aira has individual subscriptions available, but there are many ways to get free minutes without one! Our Access Partners are leading organizations that provide free access to Aira's services to their customers, visitors, students, and employees. When you call Aira from an Access Partner location, the offer will automatically be applied, and you can connect with a Visual Interpreter at no cost to you. To manually search for Access Partner offers, open the app, and click "Browse Access Offers." You can scroll through recently used offers, and even see ones available near you. Some examples of popular locations include Starbucks, Target, and Wegmans. Aira also has many promotional offers, like a daily Five Minute Free Call, free minutes for those seeking employment, and a limited time offer for those who opt into our Build AI data collection program. Learn more about accessing free Aira minutes here: https://aira.io/explorer-tips-how-to-get-free-aira-minutes/ Highlights - Create a free account and start experiencing visual interpreting without commitment - Browse Access Offers and promotional offers to get free minutes - Use Access AI to take or upload a photo, get an instant description, and choose to verify with a human - Need more minutes? A variety of paid plans support a wide range of needs - Easily connect to a Visual Interpreter 24/7/365, no reservations required - Integrate your Lyft account with your Aira - Join a supportive and inspiring community - Increase your everyday efficiency and independence Learn More Listen to Airacast, our podcast for help getting started, and for news and updates. Subscribe at https://pinecast.com/feed/airacast. Follow us on Twitter (@airaio), Facebook and YouTube, or learn more at aira.io. Questions? Contact Customer Care daily from 6:00 AM to 6:00 PM Pacific time. Phone: 1-800-835-1934 Email: support@aira.io

SCAN LOGS

Timestamp	Event	Error

2024-11-17 23:37:54	Generating Hashes	OK
2024-11-17 23:37:54	Extracting APK	OK
2024-11-17 23:37:54	Unzipping	OK
2024-11-17 23:37:54	Getting Hardcoded Certificates/Keystores	OK
2024-11-17 23:37:54	Parsing APK with androguard	OK
2024-11-17 23:37:57	Parsing AndroidManifest.xml	OK
2024-11-17 23:37:57	Extracting Manifest Data	OK
2024-11-17 23:37:57	Performing Static Analysis on: Aira Explorer (io.aira.explorer)	OK
2024-11-17 23:37:57	Fetching Details from Play Store: io.aira.explorer	OK
2024-11-17 23:37:57	Manifest Analysis Started	OK
2024-11-17 23:37:57	Checking for Malware Permissions	OK
2024-11-17 23:37:57	Fetching icon path	OK
2024-11-17 23:37:57	Library Binary Analysis Started	OK
2024-11-17 23:37:57	Reading Code Signing Certificate	OK
2024-11-17 23:37:58	Running APKiD 2.1.5	OK
2024-11-17 23:38:02	Detecting Trackers	OK
2024-11-17 23:38:05	Decompiling APK to Java with JADX	OK

2024-11-17 23:38:22	Converting DEX to Smali	OK
2024-11-17 23:38:22	Code Analysis Started on - java_source	OK
2024-11-17 23:38:30	Android SAST Completed	OK
2024-11-17 23:38:30	Android API Analysis Started	OK
2024-11-17 23:38:33	Android API Analysis Completed	OK
2024-11-17 23:38:33	Android Permission Mapping Started	OK
2024-11-17 23:38:40	Android Permission Mapping Completed	OK
2024-11-17 23:38:42	Email and URL Extraction Completed	OK
2024-11-17 23:38:42	Android Behaviour Analysis Started	OK
2024-11-17 23:38:47	Android Behaviour Analysis Completed	OK
2024-11-17 23:38:47	Extracting String data from APK	OK
2024-11-17 23:38:47	Extracting String data from Code	OK
2024-11-17 23:38:47	Extracting String values and entropies from Code	OK
2024-11-17 23:38:49	Performing Malware check on extracted domains	OK
2024-11-17 23:38:51	Saving to Database	OK