MOBSF

ANDROID STATIC ANALYSIS REPORT

Paired (2.16.0)

File Name:	com.getpaired.app_9980.apk
Package Name:	com.getpaired.app
Scan Date:	Aug. 29, 2025, 10:56 p.m.
App Security Score:	**47/100 (MEDIUM RISK)**
Grade:	B
Trackers Detection:	6/432

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
4	22	5	2	1

FILE INFORMATION

File Name: com.getpaired.app_9980.apk
Size: 33.25MB
MD5: e4a2d77ad13b77736526192cc99a26c0
SHA1: a54ffe5a3b0cca1e8eb3ddb7ce93f2aa34dc6b9f
SHA256: 5a50e4f0aff4dd2feb89c5c8c0dceac5efba2a84f881ebf1f46f55b383918778

APP INFORMATION

App Name: Paired
Package Name: com.getpaired.app
Main Activity: com.getpaired.app.MainActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 2.16.0

Android Version Code: 9980

◫ APP COMPONENTS

Activities: 33
Services: 19
Receivers: 23
Providers: 13
Exported Activities: 3
Exported Services: 2
Exported Receivers: 5
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: 2020-05-12 17:11:07+00:00
Valid To: 2050-05-12 17:11:07+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x3d422902c3ef76a1c1e8dabeb44febdef79f9282
Hash Algorithm: sha256
md5: b2bc15cae5845e69e066941817052e0b
sha1: 9bdbc851cbdba4cd404e98f6b54555b747b3a603
sha256: 1c3b2f2d180d336cbcc0d0349c4d90c3c17eadb2f19e9f00cfa5e7098a98cfcf
sha512: 7884433e35e8360a75902ef9b25316c16a36b0346df28afe0fd015e660b71ac164e8ce8978ad1f09f97d250d79f6b78fec307d3eddf1257626373223a2869db8
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: e26478e11b237017b98205d32c78d9edd352f8e91e45259ea1523cec5d0221ec
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.

PERMISSION	STATUS	INFO	DESCRIPTION
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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications

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.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

PERMISSION	STATUS	INFO	DESCRIPTION
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
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.getpaired.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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

🔎 APKID ANALYSIS

FILE	DETAILS
e4a2d77ad13b77736526192cc99a26c0.apk	<table><tr><td>FINDINGS</td><td>DETAILS</td></tr><tr><td>Anti-VM Code</td><td>possible VM check</td></tr></table>

FILE	DETAILS
classes.dex	**FINDINGS** / **DETAILS** table: **Anti-VM Code**: Build.FINGERPRINT check / Build.MODEL check / Build.MANUFACTURER check / Build.PRODUCT check / Build.BOARD check / SIM operator check / network operator name check / device ID check **Compiler**: r8 without marker (suspicious)
classes2.dex	**FINDINGS** / **DETAILS** table: **Anti-VM Code**: Build.FINGERPRINT check / Build.MODEL check / Build.MANUFACTURER check / Build.PRODUCT check / Build.HARDWARE check / possible Build.SERIAL check / Build.TAGS check / possible ro.secure check **Compiler**: r8 without marker (suspicious)

FILE	DETAILS
classes3.dex	<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 possible VM check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

FILE	DETAILS
classes4.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.getpaired.app.MainActivity	Schemes: paired://, http://, https://, Hosts: paired.go.link, Mime Types: image/*,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.getpaired.app,

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: **11** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched 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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Broadcast Receiver (com.adjust.sdk.AdjustReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [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.
3	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.
4	TaskAffinity is set for activity (com.braze.push.NotificationTrampolineActivity)	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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
6	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.
7	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.
8	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
9	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.
10	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.
11	Broadcast Receiver (com.amazon.device.iap.ResponseReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.amazon.inapp.purchasing.Permission.NOTIFY [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.

NO	ISSUE	SEVERITY	DESCRIPTION
12	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: **2** | WARNING: **9** | INFO: **4** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				Aa/C1165b.java Aa/D0.java Aa/G.java Aa/H.java Aa/L.java Aa/Q.java Aa/S.java Aa/Y.java Aa/Z.java Aa/i0.java Aa/j0.java Aa/k0.java Aa/w0.java Ba/f.java Ba/n.java C1/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				C3/a.java
				C3/d.java
				C3/j.java
				D1/a.java
				E1/C1291a.java
				E1/m.java
				E3/c.java
				F0/F.java
				G1/a.java
				G3/h.java
				I4/a.java
				I9/a.java
				J3/a.java
				J4/C1526d.java
				J4/C1529g.java
				J4/C1536n.java
				J4/N.java
				J4/s.java
				J9/a.java
				K1/n.java
				K8/l.java
				Kc/a.java
				L3/a.java
				L9/c.java
				Lc/a.java
				Lc/c.java
				Lc/f.java
				M1/s.java
				M1/x.java
				M3/b.java
				M3/h.java
				M3/k.java
				M4/l.java
				Mb/a.java
				N0/d.java
				N2/g.java
				N4/e.java
				N4/f.java
				O/AbstractC1584b.java
				O0/c.java
				O0/o.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				O1/a.java
				O2/E.java
				O7/k.java
				Oa/b.java
				P4/a.java
				Pa/c.java
				Q0/f.java
				Q1/h.java
				Q5/d.java
				Qc/b.java
				R1/d.java
				R4/f.java
				R4/i.java
				R4/j.java
				R4/m.java
				R7/a.java
				S0/a.java
				S0/c.java
				S0/d.java
				S0/f.java
				S1/a.java
				Tc/b.java
				U4/a.java
				V1/a.java
				Va/e.java
				W1/L.java
				X3/a.java
				X9/d.java
				Y0/d.java
				Y9/b.java
				Ya/c.java
				Yf/c.java
				Z1/e.java
				Zc/f.java
				a0/C1949v.java
				a1/C1951A.java
				a9/AbstractC2113x.java
				aa/C2122g.java
				ad/C2134a.java
				b6/AbstractC2457k.java
				b6/C2446A.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				b6/D.java b6/K.java b6/M.java b6/W.java b6/X.java b9/k.java c9/C2575g.java cl/json/RNShareModule.java com/adjust/nativemodule/Adjust.java com/adjust/sdk/Logger.java com/adjust/sdk/sig/NativeLibHelper.java com/adjust/sdk/sig/Signer.java com/adjust/sdk/sig/d.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java com/amazon/a/a/g/d.java com/amazon/a/a/o/c.java com/amazon/c/a/a/d.java com/amazon/device/drm/LicensingService.java com/amazon/device/drm/a/d/c.java com/amazon/device/iap/PurchasingService.java com/amazon/device/iap/internal/c/e.java com/amazon/device/simplesignin/BroadcastHandler.java com/amazon/device/simplesignin/SimpleSignInService.java com/amazon/device/simplesignin/a/a/c/b.java com/amazon/device/simplesignin/a/c.java com/amazon/device/simplesignin/a/c/b.java com/braze/support/BrazeLogger.java com/bugsnag/android/C2731y0.java com/bugsnag/android/M.java com/bumptech/glide/GeneratedAppGlide ModuleImpl.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				~~ModuleImpl.java~~ com/bumptech/glide/c.java ~~com/bumptech/glide/load/data/b.java~~ com/bumptech/glide/load/data/j.java com/bumptech/glide/load/data/l.java com/bumptech/glide/manager/e.java com/bumptech/glide/manager/p.java com/bumptech/glide/manager/q.java com/dieam/reactnativepushnotification/modules/RNPushNotification.java com/dieam/reactnativepushnotification/modules/RNPushNotificationActions.java com/dieam/reactnativepushnotification/modules/RNPushNotificationBootEventReceiver.java com/dieam/reactnativepushnotification/modules/RNPushNotificationPublisher.java com/dieam/reactnativepushnotification/modules/a.java com/dieam/reactnativepushnotification/modules/b.java com/dieam/reactnativepushnotification/modules/d.java com/dieam/reactnativepushnotification/modules/e.java com/dieam/reactnativepushnotification/modules/f.java com/getpaired/app/PairedMessagingService.java com/github/penfeizhou/animation/decode/b.java com/horcrux/svg/C3332w.java com/ibits/react_native_in_app_review/AppReviewModule.java com/intercom/reactnative/IntercomEventEmitter.java com/intercom/reactnative/IntercomModule.java com/intercom/twig/Twig.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/icarumm/RNDeviceInfo/c.java com/Iugg/RNCConfig/RNCConfigModule.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	com/microsoft/codepush/react/j.java com/reactcommunity/rndatetimepicker/d.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnative/ivpusic/imagepicker/a.java com/reactnative/ivpusic/imagepicker/f.java com/reactnativecommunity/asyncstorage/h.java com/reactnativecommunity/asyncstorage/next/a.java com/reactnativecommunity/slider/a.java com/reactnativecommunity/webview/f.java com/reactnativecommunity/webview/j.java com/reactnativecommunity/webview/l.java com/reactnativedocumentpicker/RNDocumentPickerModule.java com/reactnativegooglesignin/RNGoogleSigninModule.java com/reactnativegooglesignin/c.java com/reactnativeimageresizer/ImageResizerModule.java com/reactnativeimageresizer/a.java com/reactnativemmkv/MmkvModule.java com/reactnativereceivesharingintent/a.java com/revenuecat/purchases/common/DefaultLogHandler.java com/revenuecat/purchases/hybridcommon/CommonKt.java com/revenuecat/purchases/hybridcommon/mappers/PurchasesPeriod.java com/revenuecat/purchases/react/RNPurchasesModule.java com/rnfs/c.java com/shopify/reactnative/skia/RNSkiaModu

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/shopify/reactnative/skia/RNSkiaModule.java
				com/shopify/reactnative/skia/SkiaAHBView.java
				com/shopify/reactnative/skia/SkiaBaseView.java
				com/shopify/reactnative/skia/SkiaTextureView.java
				com/shopify/reactnative/skia/ViewScreenshotService.java
				com/sudoplz/rninappupdates/SpReactNativeInAppUpdatesModule.java
				com/swmansion/gesturehandler/react/RNGestureHandlerModule.java
				com/swmansion/gesturehandler/react/i.java
				com/swmansion/gesturehandler/react/j.java
				com/swmansion/reanimated/NativeMethodsHelper.java
				com/swmansion/reanimated/ReanimatedModule.java
				com/swmansion/reanimated/ReanimatedUIManagerFactory.java
				com/swmansion/reanimated/keyboard/WindowsInsetsManager.java
				com/swmansion/reanimated/layoutReanimation/AnimationsManager.java
				com/swmansion/reanimated/layoutReanimation/ReanimatedNativeHierarchyManager.java
				com/swmansion/reanimated/layoutReanimation/ScreensHelper.java
				com/swmansion/reanimated/layoutReanimation/SharedTransitionManager.java
				com/swmansion/reanimated/layoutReanimation/TabNavigatorObserver.java
				com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java
				com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/swmansion/rnscreens/InsetsObserverProxy.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/swmansion/rnscreens/ScreensModule.java com/swmansion/rnscreens/SearchBarManager.java com/swmansion/rnscreens/utils/ScreenDummyLayoutHelper.java com/th3rdwave/safeareacontext/k.java com/view/C3337b.java com/view/InternalLog.java com/view/d1.java com/view/reactnative/SmartlookAnalyticsModuleImpl.java com/yalantis/ucrop/UCropActivity.java com/yalantis/ucrop/task/BitmapCropTask.java com/yalantis/ucrop/view/b.java d1/e.java dd/AbstractC3391A.java dd/h.java dd/t.java e9/AbstractC3607a.java expo/modules/fetch/NativeResponse.java f6/c.java f9/o.java fa/s.java fr/greweb/reactnativeviewshot/RNViewShotModule.java fr/greweb/reactnativeviewshot/a.java gg/e.java ib/C3914a.java ib/C3916c.java id/C3921a.java io/invertase/firebase/app/ReactNativeFirebaseApp.java io/invertase/firebase/app/ReactNativeFirebaseAppModule.java io/invertase/firebase/auth/ReactNativeFire

NO	ISSUE	FILES	SEVERITY	STANDARDS	FILES
		baseAuthModule.java io/invertase/firebase/common/RCTConvert Firebase.java			
					io/invertase/firebase/common/ReactNative FirebaseEventEmitter.java
					io/invertase/firebase/common/SharedUtils .java
					io/invertase/firebase/perf/ScreenTrace.java
					io/invertase/firebase/utils/ReactNativeFire baseUtilsModule.java
					j1/c.java
					k6/C4052c.java
					l2/AbstractC4110b.java
					l3/C4114b.java
					l6/D.java
					l6/E.java
					l6/y.java
					la/i.java
					lb/C4152C.java
					lb/C4154E.java
					lb/C4161g.java
					lb/C4165k.java
					lb/H.java
					lb/y.java
					m2/g.java
					m3/C4211d.java
					m3/C4212e.java
					m9/g.java
					n3/C4260a.java
					nb/c.java
					nb/f.java
					o3/C4365a.java
					o9/AbstractC4378A.java
					o9/AbstractC4380b.java
					o9/C4381c.java
					o9/D.java
					o9/E.java
					o9/k.java
					o9/x.java
					o9/y.java
					p1/AbstractC4420b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				p1/C4421c.java
				p1/C4623e.java
				p9/B.java
				p9/C4469g.java
				p9/G.java
				p9/i.java
				p9/s.java
				p9/w.java
				pd/f.java
				q3/c.java
				q3/e.java
				r3/h.java
				r3/i.java
				r3/k.java
				r3/q.java
				r3/z.java
				r7/AbstractC4669a.java
				s3/i.java
				s3/j.java
				s9/C4764a.java
				sc/C4767a.java
				t3/e.java
				t3/i.java
				t7/C4877b.java
				u3/ExecutorServiceC4926a.java
				u9/b.java
				ua/g.java
				v3/c.java
				v3/d.java
				v3/g.java
				v3/s.java
				v3/t.java
				v3/u.java
				v9/g.java
				v9/q.java
				v9/r.java
				w1/C5026c.java
				x3/d.java
				x5/f.java
				y1/AbstractC5230a.java
				y3/C.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				y3/C5235c.java y3/e.java y3/f.java y3/l.java y3/q.java y3/r.java y3/u.java z4/C5373g.java z4/M2.java z9/d.java
2	[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	C8/Z.java F8/b.java V3/a.java a8/C2069p0.java b6/W.java bo/app/r20.java com/adjust/sdk/Util.java com/amazon/a/a/b/b.java com/amazon/a/a/i/b.java com/amazon/a/a/l/c.java com/braze/support/IntentUtils.java db/C3382d.java me/AbstractC4236a.java me/C4237b.java ne/C4313a.java rd/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	[App can read/write to External Storage. Any App can read data written to External Storage.](#)	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	J2/c.java Z4/b.java b6/W.java com/ReactNativeBlobUtil/c.java com/alpha0010/fs/FileAccessModule.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnative/ivpusic/imagepicker/a.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/reactnativecommunity/webview/l.java com/reactnativereceivesharingintent/a.java com/rnfs/RNFSManager.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java j5/C4005a.java
4	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	M1/x.java Oa/c.java Z4/b.java com/ReactNativeBlobUtil/a.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnativecommunity/webview/l.java fr/greweb/reactnativeviewshot/RNViewShotModule.java q2/S.java
				E0/B.java I/K.java L4/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				O/C1601j0.java Bk.java Uf/U.java
5	[Files may contain hardcoded sensitive information like usernames, passwords, keys etc.](#)	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/adjust/sdk/Constants.java com/airbnb/lottie/compose/RememberLottieCompositionKt.java com/braze/configuration/BrazeConfig.java com/bugsnag/android/C2703l1.java com/bugsnag/android/C2714p0.java com/getpaired/app/BuildConfig.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/revenuecat/purchases/amazon/AmazonBillingKt.java com/revenuecat/purchases/amazon/AmazonCacheKt.java com/revenuecat/purchases/common/BackendKt.java com/revenuecat/purchases/common/BackgroundAwareCallbackCacheKey.java com/revenuecat/purchases/common/caching/DeviceCache.java com/revenuecat/purchases/common/diagnostics/DiagnosticsEntry.java com/revenuecat/purchases/common/diagnostics/DiagnosticsHelper.java com/revenuecat/purchases/common/diagnostics/DiagnosticsTracker.java com/revenuecat/purchases/common/offlineentitlements/ProductEntitlementMapping.java com/revenuecat/purchases/common/verification/DefaultSignatureVerifier.java com/revenuecat/purchases/common/verification/Signature.java com/revenuecat/purchases/common/verification/SigningManager.java com/revenuecat/purchases/strings/ConfigureStrings.java com/revenuecat/purchases/subscriberattri

NO	ISSUE	SEVERITY	STANDARDS	FILES
				butes/SubscriberAttribute.java com/revenuecat/purchases/subscriberattributes/SubscriberAttributeKt.java
				com/sudoplz/rninappupdates/SpReactNativeInAppUpdatesModule.java com/view/CheckRecordingConfigRequest.java com/view/InternalLog.java com/view/RecordData.java com/view/RecordJobData.java com/view/SessionData.java com/view/SessionJobData.java com/view/sdk/storage/SessionRecordingStorage.java expo/modules/adapters/react/NativeModulesProxy.java expo/modules/image/records/SourceMap.java f2/C3675d.java fc/C3721d.java g3/k.java io/invertase/firebase/common/TaskExecutorService.java kb/C4070b.java p3/C4432g.java r3/C4664d.java r3/p.java r3/x.java x2/InterfaceC5137c.java y8/C5242a.java z2/n.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	P4/j.java V4/b.java bo/app/as.java bo/app/cx.java bo/app/d60.java bo/app/dq.java bo/app/i80.java bo/app/iu.java bo/app/kc0.java bo/app/lq.java bo/app/mq.java bo/app/mt.java bo/app/nf0.java bo/app/om.java bo/app/pc.java bo/app/q.java bo/app/se0.java bo/app/t50.java bo/app/tx.java bo/app/vd0.java bo/app/z30.java com/braze/configuration/RuntimeAppConfigurationProvider.java com/braze/managers/BrazeGeofenceManager.java l6/D.java
7	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/bugsnag/android/RootDetector.java com/view/c4.java fa/AbstractC3712c.java la/w.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/reactnativecommunity/webview/j.java
9	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	J4/C1527e.java R4/m.java com/ReactNativeBlobUtil/i.java com/airbnb/lottie/network/NetworkCache.java com/braze/support/StringUtils.java
10	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	N2/l.java R1/c.java V7/M.java V7/U.java com/reactnativecommunity/asyncstorage/l.java
11	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	Jd/b.java Oa/b.java com/amazon/a/a/o/b/a.java com/bugsnag/android/O.java com/revenuecat/purchases/common/UtilsKt.java k6/C4050a.java m5/AbstractC4221c.java
12	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	J8/b.java L6/a.java Tb/a.java com/amazon/device/drm/LicensingService.java com/amazon/device/iap/PurchasingService.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
13	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	H8/a.java Z3/d.java
14	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/amazon/a/a/o/b/a.java
15	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	G2/c.java
16	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	com/reactnativecommunity/clipboard/ClipboardModule.java
17	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/reactnativecommunity/clipboard/ClipboardModule.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	E1/C1291a.java E1/m.java Oc/c.java b6/C2448b.java b6/M.java b6/W.java b6/X.java b6/b0.java cl/json/RNShareModule.java com/ReactNativeBlobUtil/d.java com/ReactNativeBlobUtil/g.java com/adjust/sdk/ActivityHandler.java com/adjust/sdk/PreinstallUtil.java com/amazon/a/a/i/a.java com/amazon/a/a/i/g.java com/amazon/device/iap/internal/a/a.java com/braze/Braze.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/inappmessage/views/InAppMessageHtmlBaseView.java com/braze/ui/support/UriUtils.java com/dieam/reactnativepushnotification/modules/b.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnativecommunity/cameraroll/CameraRollModule.java l6/C4123c.java m2/g.java m2/n.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java
00014	Read file into a stream and put it into a JSON object	file	O6/a.java Oa/c.java S4/j.java V4/a.java d6/k.java
			J4/C1529g.java

RULE ID	BEHAVIOUR	LABEL	FILES
			Lc/e.java
			M1/x.java
			O17b.java
			O6/a.java
00013	Read file and put it into a stream	file	Oa/c.java
			R4/m.java
			S3/a.java
			S4/j.java
			V4/a.java
			X4/b.java
			Z8/C1917i.java
			Z8/J.java
			a2/AbstractC1961a.java
			b6/K.java
			bo/app/pa0.java
			bo/app/sq.java
			cg/l.java
			com/ReactNativeBlobUtil/a.java
			com/ReactNativeBlobUtil/c.java
			com/ReactNativeBlobUtil/e.java
			com/ReactNativeBlobUtil/h.java
			com/adjust/sdk/PreinstallUtil.java
			com/airbnb/android/react/lottie/h.java
			com/airbnb/lottie/compose/RememberLottieCompositionKt.java
			com/airbnb/lottie/network/NetworkCache.java
			com/airbnb/lottie/network/NetworkFetcher.java
			com/alpha0010/fs/FileAccessModule.java
			com/amazon/c/a/a/c.java
			com/braze/support/BrazeImageUtils.java
			com/braze/support/WebContentUtils.java
			com/bugsnag/android/J0.java
			com/bugsnag/android/RootDetector.java
			com/bugsnag/android/x1.java
			com/bumptech/glide/load/a.java
			com/microsoft/codepush/react/i.java
			com/microsoft/codepush/react/m.java
			com/reactnative/ivpusic/imagepicker/PickerModule.java
			com/reactnativecommunity/asyncstorage/h.java
			com/reactnativecommunity/cameraroll/CameraRollModule.java
			com/revenuecat/purchases/common/FileHelper.java

RULE ID	BEHAVIOUR	LABEL	FILES
			com/rnfs/RNFSManager.java com/rnfs/i.java d6/k.java fe/m.java
			fe/o.java g3/q.java i3/C3878b.java l1/m.java l3/C4114b.java v3/g.java
00022	Open a file from given absolute path of the file	file	Fd/K.java J2/c.java M1/x.java R1/d.java S3/a.java Z3/b.java Z4/k.java a4/C1977b.java bo/app/ea.java bo/app/fa.java bo/app/ko.java bo/app/rb0.java bo/app/ug0.java bo/app/xc.java com/ReactNativeBlobUtil/c.java com/ReactNativeBlobUtil/g.java com/airbnb/lottie/LottieCompositionFactory.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/alpha0010/fs/FileAccessModule.java com/amazon/a/a/b/b.java com/braze/d0.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java com/bugsnag/android/C0.java com/bugsnag/android/C2732z.java com/bugsnag/android/ndk/NativeBridge.java com/microsoft/codepush/react/a.java com/microsoft/codepush/react/i.java com/microsoft/codepush/react/j.java

RULE ID	BEHAVIOUR	LABEL	FILES
			com/microsoft/codepush/react/m.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnative/ivpusic/imagepicker/a.java com/reactnative/ivpusic/imagepicker/e.java
			com/reactnativecommunity/cameraroll/CameraRollModule.java com/reactnativedocumentpicker/RNDocumentPickerModule.java com/reactnativeimageresizer/ImageResizerModule.java com/reactnativeimageresizer/a.java com/rnfs/RNFSManager.java d5/AbstractC3370c.java dd/g.java fr/greweb/reactnativeviewshot/RNViewShotModule.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java j5/C4005a.java l1/m.java l2/AbstractC4110b.java l2/C4111c.java l2/C4112d.java r2/InterfaceC4657a.java
00089	Connect to a URL and receive input stream from the server	command network	L4/g.java N2/j.java Pa/c.java R3/a.java Z8/u.java com/bugsnag/android/N.java com/bumptech/glide/load/data/j.java com/microsoft/codepush/react/g.java com/reactnativeimageresizer/a.java com/revenuecat/purchases/common/HTTPClient.java com/rnfs/c.java com/rnfs/i.java k6/C4052c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	L4/g.java N2/j.java Pa/c.java R3/a.java Z8/u.java com/bugsnag/android/N.java com/bumptech/glide/load/data/j.java com/revenuecat/purchases/common/HTTPClient.java com/rnfs/c.java com/rnfs/i.java e9/AbstractC3607a.java m9/f.java
00078	Get the network operator name	collection telephony	N2/n.java O2/a.java b6/W.java bo/app/lq.java com/learnium/RNDeviceInfo/RNDeviceModule.java
00137	Get last known location of the device	location collection	N2/n.java
00115	Get last known location of the device	collection location	N2/n.java O2/a.java
00132	Query The ISO country code	telephony collection	N2/n.java O2/a.java a9/Z.java
00192	Get messages in the SMS inbox	sms	J2/c.java com/reactnativereceivesharingintent/a.java com/rnfs/RNFSManager.java l2/AbstractC4110b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	com/alpha0010/fs/FileAccessModule.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/rnfs/RNFSManager.java
00028	Read file from assets directory	file	Z8/C1911c.java com/rnfs/RNFSManager.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	J2/c.java b6/M.java com/adjust/sdk/DeviceInfo.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/rnfs/RNFSManager.java
00161	Perform accessibility service action on accessibility node info	accessibility service	a1/C1951A.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	a1/C1951A.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	Oc/c.java W4/a.java Z8/J.java b6/C2448b.java b6/W.java b6/X.java b6/b0.java com/adjust/sdk/ActivityHandler.java com/adjust/sdk/DeviceInfo.java com/amazon/a/a/i/g.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/support/UriUtils.java com/dieam/reactnativepushnotification/modules/b.java com/reactnative/ivpusic/imagepicker/PickerModule.java expo/modules/image/records/SourceMap.java io/invertase/firebase/common/SharedUtils.java l2/AbstractC4110b.java me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java w2/e.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	E1/C1291a.java Oc/c.java b6/W.java b6/X.java com/ReactNativeBlobUtil/g.java m2/g.java
00189	Get the content of a SMS message	sms	J2/c.java b6/M.java com/adjust/sdk/DeviceInfo.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/reactnativedocumentpicker/RNDocumentPickerModule.java com/reactnativereceivesharingintent/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00188	Get the address of a SMS message	sms	J2/c.java b6/M.java com/adjust/sdk/DeviceInfo.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/reactnativedocumentpicker/RNDocumentPickerModule.java com/reactnativereceivesharingintent/b.java
00091	Retrieve data from broadcast	collection	b6/M.java com/ReactNativeBlobUtil/g.java com/amazon/device/drm/a/d/c.java com/amazon/device/iap/internal/c/e.java com/amazon/device/simplesignin/a/c/b.java com/braze/push/BrazeNotificationUtils.java com/braze/reactbridge/BrazeReactBridgeImpl.java com/dieam/reactnativepushnotification/modules/RNPushNotification.java com/dieam/reactnativepushnotification/modules/RNPushNotificationPublisher.java l6/I.java
00191	Get messages in the SMS inbox	sms	J2/c.java b6/C2448b.java b6/M.java b6/W.java com/ReactNativeBlobUtil/g.java com/adjust/sdk/DeviceInfo.java com/reactnativecommunity/cameraroll/CameraRollModule.java
00200	Query data from the contact list	collection contact	J2/c.java b6/M.java com/adjust/sdk/DeviceInfo.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/reactnativedocumentpicker/RNDocumentPickerModule.java com/reactnativereceivesharingintent/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00187	Query a URI and check the result	collection sms calllog calendar	b6/M.java com/reactnativecommunity/cameraroll/CameraRollModule.java p1/C4423e.java
00201	Query data from the call log	collection calllog	J2/c.java b6/M.java com/adjust/sdk/DeviceInfo.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/reactnativedocumentpicker/RNDocumentPickerModule.java com/reactnativereceivesharingintent/b.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	J2/c.java b6/M.java com/adjust/sdk/DeviceInfo.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/reactnativedocumentpicker/RNDocumentPickerModule.java com/reactnativereceivesharingintent/b.java p1/AbstractC4420b.java p1/C4423e.java q3/c.java
00030	Connect to the remote server through the given URL	network	Z8/u.java com/adjust/sdk/AdjustLinkResolution.java com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/bumptech/glide/load/data/j.java com/reactnativeimageresizer/a.java com/rnfs/c.java com/rnfs/i.java

RULE ID	BEHAVIOUR	LABEL	FILES
00024	Write file after Base64 decoding	reflection file	com/ReactNativeBlobUtil/a.java com/ReactNativeBlobUtil/g.java com/airbnb/lottie/LottieCompositionFactory.java com/alpha0010/fs/FileAccessModule.java com/reactnativeimageresizer/a.java l2/C4111c.java l2/C4112d.java
00016	Get location info of the device and put it to JSON object	location collection	N2/f.java
00072	Write HTTP input stream into a file	command network file	com/microsoft/codepush/react/g.java com/reactnativeimageresizer/a.java com/rnfs/c.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/reactnativeimageresizer/a.java
00094	Connect to a URL and read data from it	command network	Z8/u.java com/reactnativeimageresizer/a.java com/shopify/reactnative/skia/PlatformContext.java
00108	Read the input stream from given URL	network command	Z8/u.java com/reactnativeimageresizer/a.java
00012	Read data and put it into a buffer stream	file	J4/C1529g.java R4/m.java com/amazon/c/a/a/c.java com/microsoft/codepush/react/m.java com/rnfs/i.java

RULE ID	BEHAVIOUR	LABEL	FILES
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00130	Get the current WIFI information	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00134	Get the current WiFi IP address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00082	Get the current WiFi MAC address	collection wifi	com/learnium/RNDeviceInfo/RNDeviceModule.java
00004	Get filename and put it to JSON object	file collection	S4/f.java com/airbnb/lottie/LottieCompositionFactory.java d6/c.java h6/C3833a.java
00125	Check if the given file path exist	file	S4/f.java com/ReactNativeBlobUtil/g.java com/reactnativecommunity/cameraroll/CameraRollModule.java
00026	Method reflection	reflection	Ee/C1300a.java Ee/C1301b.java
00043	Calculate WiFi signal strength	collection wifi	ic/e.java
00079	Hide the current app's icon	evasion	g2/p.java
00005	Get absolute path of file and put it to JSON object	file	com/airbnb/lottie/LottieCompositionFactory.java com/microsoft/codepush/react/j.java
00015	Put buffer stream (data) to JSON object	file	b6/W.java

RULE ID	BEHAVIOUR	LABEL	FILES
00009	Put data in cursor to JSON object	file	N2/l.java b6/W.java com/reactnativecommunity/asyncstorage/a.java
00003	Put the compressed bitmap data into JSON object	camera	M4/l.java
00096	Connect to a URL and set request method	command network	L4/g.java Pa/c.java R3/a.java Z8/u.java com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/revenuecat/purchases/common/HTTPClient.java com/rnfs/i.java
00175	Get notification manager and cancel notifications	notification	com/dieam/reactnativepushnotification/modules/b.java
00163	Create new Socket and connecting to it	socket	com/adjust/sdk/network/ActivityPackageSender.java
00121	Create a directory	file command	com/reactnativecommunity/cameraroll/CameraRollModule.java
00104	Check if the given path is directory	file	com/reactnativecommunity/cameraroll/CameraRollModule.java

🛢 FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://betterhalf-e4a77.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/3304116375/namespaces/firebase:fetch?key=AIzaSyBZquDIQKaYFDSQb7BAT8n7fL2tDl49pwI is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'hasCommunity': '1', 'hasIosConsent': 'true'}, 'state': 'UPDATE', 'templateVersion': '16'}

⦂⦙⦙ ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.CAMERA, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.READ_PHONE_STATE, android.permission.ACCESS_WIFI_STATE
Other Common Permissions	4/44	android.permission.FOREGROUND_SERVICE, 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
pinterest.com	ok	**IP:** 151.101.0.84 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** [Google Map](#)
subscription.adjust.io	ok	**IP:** 185.151.204.44 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
appleid.apple.com	ok	**IP:** 17.111.105.242 **Country:** United States of America **Region:** California **City:** Cupertino **Latitude:** 37.316605 **Longitude:** -122.046486 **View:** Google Map
graph-video.s	ok	No Geolocation information available.
codepush.appcenter.ms	ok	No Geolocation information available.
api.revenuecat.com	ok	**IP:** 52.203.57.188 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
goo.gle	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
app.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
app.adjust.com	ok	**IP:** 185.151.204.12 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
sdk.iad-01.braze.com	ok	**IP:** 104.18.39.68 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
xml.org	ok	**IP:** 104.239.142.8 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
api.eu.amplitude.com	ok	**IP:** 3.122.30.79 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
plus.google.com	ok	**IP:** 64.233.185.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)
gdpr.adjust.com	ok	**IP:** 185.151.204.50 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** [Google Map](#)
issuetracker.google.com	ok	**IP:** 64.233.177.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)
notify.bugsnag.com	ok	**IP:** 35.186.205.6 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 172.253.124.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)
.facebook.com	ok	No Geolocation information available.
graph.s	ok	No Geolocation information available.
default.url	ok	No Geolocation information available.
facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **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](#)

DOMAIN	STATUS	GEOLOCATION
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](#)
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** [Google Map](#)
twitter.com	ok	**IP:** 162.159.140.229 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** [Google Map](#)
sessions.bugsnag.com	ok	**IP:** 35.190.88.7 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 64.233.176.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.paired.run	ok	**IP:** 34.8.91.133 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
ssrv.adjust.com	ok	**IP:** 185.151.204.2 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
docs.swmansion.com	ok	**IP:** 104.21.27.136 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.braze.com	ok	**IP:** 104.17.227.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
bugsnag.com	ok	**IP:** 18.238.96.92 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
developers.facebook.com	ok	**IP:** 31.13.70.1 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
subscription.s	ok	No Geolocation information available.
rev.cat	ok	**IP:** 52.72.49.79 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sondheim.braze.com	ok	**IP:** 172.64.144.252 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** [Google Map](#)
app.adjust.io	ok	**IP:** 185.151.204.1 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** [Google Map](#)
accounts.google.com	ok	**IP:** 142.251.2.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)
betterhalf-e4a77.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** [Google Map](#)
filesystem.local	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
api-diagnostics.revenuecat.com	ok	**IP:** 54.158.163.245 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** [Google Map](#)
api2.amplitude.com	ok	**IP:** 44.238.64.219 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** [Google Map](#)
gdpr.s	ok	No Geolocation information available.
iamcache.braze	ok	No Geolocation information available.
developer.apple.com	ok	**IP:** 17.253.83.137 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
api-paywalls.revenuecat.com	ok	**IP:** 54.88.247.37 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
dust.k8s.test-001.d-usw-2.braze.com	ok	No Geolocation information available.
schemas.microsoft.com	ok	**IP:** 13.107.253.71 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
docs.bugsnag.com	ok	**IP:** 18.155.173.77 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
errors.rev.cat	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** [Google Map](#)
docs.revenuecat.com	ok	**IP:** 18.238.109.116 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** [Google Map](#)
subscription.adjust.com	ok	**IP:** 185.151.204.52 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** [Google Map](#)
ssrv.adjust.io	ok	**IP:** 185.151.204.1 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
regionconfig.eu.amplitude.com	ok	**IP:** 18.238.96.4 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** [Google Map](#)
xmlpull.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](#)
dashif.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** [Google Map](#)
www.amazon.com	ok	**IP:** 18.155.172.176 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
shopify.github.io	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
regionconfig.amplitude.com	ok	**IP:** 18.155.173.79 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
ssrv.s	ok	No Geolocation information available.
aomedia.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
console.firebase.google.com	ok	**IP:** 64.233.176.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
gdpr.adjust.io	ok	**IP:** 185.151.204.1 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

✉ EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	p9/r.java

🕵 TRACKERS

TRACKER	CATEGORIES	URL
Adjust	Analytics	https://reports.exodus-privacy.eu.org/trackers/52
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125
Bugsnag	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/207
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67

TRACKER	CATEGORIES	URL
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"ADJUST_TOKEN" : "6ss12u389zls"
"AMPLITUDE_EXPERIMENT_ANDROID_KEY" : "client-0zttntx6qo33HjElrZ3IBNljg0LduqIc"
"AMPLITUDE_EXPERIMENT_IOS_KEY" : "client-nUMbaoSKPd5otkBrjfJ3iPwPbAGHi3So"
"AMPLITUDE_KEY" : "5d9282abadbe9fddd628ffe989b3d762"
"ANDROID_BRAZE_KEY" : "f9843dbd-5911-451e-b184-b8b7eeae2c66"
"ANDROID_INTERCOM_KEY" : "android_sdk-6735e9aff97c97a3c26c7eee92348a79f271c4c2"
"AND_REVENUE_CAT_API_KEY" : "goog_ztfPRGvpWJmnsDhznDdrsUXUKdl"
"CodePushDeploymentKey" : "SaG2msE45XsQlL0BRCruudaV7AvOTOsvj5MjP"
"IOS_BRAZE_KEY" : "d8fabf23-91ef-460e-8919-6f1b734f53ce"
"IOS_INTERCOM_KEY" : "ios_sdk-bd5e1858658133c53613a0ab764fa08eb0306419"

POSSIBLE SECRETS

"IOS_REVENUE_CAT_API_KEY" : "appl_LWorsRipMRSsHUzfWjRQiqiMlpT"

"SMARTLOOK_KEY" : "7626e75f37bbf9afc8931f7fbe3b6ff096c09aa4"

"STREAM_API_KEY" : "j9h2chgqqh7e"

"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"

"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"

"com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key"

"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"

"com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key"

"facebook_client_token" : "31192547bcde0138945af2f7d00dc644"

"firebase_database_url" : "https://betterhalf-e4a77.firebaseio.com"

"google_api_key" : "AIzaSyBZquDIQKaYFDSQb7BAT8n7fL2tDl49pwl"

"google_crash_reporting_api_key" : "AIzaSyBZquDIQKaYFDSQb7BAT8n7fL2tDl49pwl"

11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a

11579208923731619542357098500868790785326998466564056403945758400790883467 1663

POSSIBLE SECRETS

686479766013060971498190079908139321726943530014330540939446345918554318339765605212255964066145455497729631139148085803712198799971664381257402829111505715

2758019355995970587784901184038904809305690585636156852142870730198868924130986086513626076488374510776543976123057

410583637251521421293261297800472684091144410159937255548352563140394674012915

49350489625a8460cc7142

258EAFA5-E914-47DA-95CA-C5AB0DC85B11

4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

d8fabf23-91ef-460e-8919-6f1b734f53ce

a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc

af60eb711bd85bc1e4d3e0a462e074eea428a8

b956059a88e9dfb420dc5fb101fd3156

3267051002075881697808308513050704318447127338065924327593890433575733748242

ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n

-bd5e1858658133c53613a0ab764fa08eb0306419

ccb64c8fceffe7d2c654e6ef2101a275207613ba

ae2044fb577e65ee8bb576ca48a2f06e

POSSIBLE SECRETS

c56fb7d591ba6704df047fd98f535372fea00211

6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148

edef8ba9-79d6-4ace-a3c8-27dcd51d21ed

1093849038073734274511112390766805569936207598951683748994586394495953116150735016013708737573759623248592132296706313309438452531591012912142327488478985984

UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMlM=

f9843dbd-5911-451e-b184-b8b7eeae2c66

8a3c4b262d721acd49a4bf97d5213199c86fa2b9

3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394 2643

37a6259cc0c1dae299a7866489dff0bd

36864200e0eaf5284d884a0e77d31646

9a04f079-9840-4286-ab92-e65be0885f95

POSSIBLE SECRETS

30820268308201d102044a9c4610300d06092a864886f70d0101040500307a310b30090603550406130255533310b3009060355040813024341311230100603550407130950616c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b130846616365626f6f6b311d301b060355040313144661636f6f6b20436f72706f726174696f6e3020170d3039303833313231353231365a180f32303530303039323353231353231365a307a310b30090603550406130255533310b3009060355040813024341311230100603550407130950616c6f20416c746f31183016060355040a130f46616365626f6f6b204d6f62696c653111300f060355040b130846616365626f6f6b311d301b060355040313144661636f6f6b20436f72706f726174696f6e30819f300d06092a864886f70d010101050003818d0030818902818100c207d51df8eb8c97d93ba0c8c1002c928fab00dc1b42fca5e66e99cc3023ed2d214d822bc59e8e35ddcf5f44c7ae8ade50d7e0c434f500e6c131f4a2834f987fc46406115de2018ebbb0d5a3c261bd97581ccfef76afc7135a6d59e8855ecd7eacc8f8737e794c60a761c536b72b11fac8e603f5da1a2d54aa103b8a13c0dbc10203010001300d06092a864886f70d0101040500038181005ee9be8bcbb250648d3b741290a82a1c9dc2e76a0af2f2228f1d9f9c4007529c446a70175c5a900d5141812866db46be6559e2141616483998211f4a673149fb2232a10d247663b26a9031e15f84bc1c74d141ff98a02d76f85b2c8ab2571b6469b232d8e768a7f7ca04f7abe4a775615916c07940656b58717457b42bd928a2

128-c20968b22ed168a498a4bf28ebadc7e883bd4b8c2dba719cb4c661a2c15147f5

5506626302227734366957871889516853432625060345377759417550018736038911 6729240

4843956129390645175905258525279791420276294952604174799584408071708240 4635286

5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

9b8f518b086098de3d77736f9458a3d2f6f95a37

5d9282abadbe9fddd628ffe989b3d762

e2719d58-a985-b3c9-781a-b030af78d30e

3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

375718002577002046354550722449118360359445513476976248669456777961554447744055631669123440501294553956214444453728942852258566672919658081012 4344277578376784

POSSIBLE SECRETS

394020061963944479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316

808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f

e973d14c97f1c647a41b0aff5c0c1a26

115792089237316195423570985008687907852837564279074904382605163141518161494337

b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3

-6735e9aff97c97a3c26c7eee92348a79f271c4c2

aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7

115792089210356248762697446949407573530086143415290314195533631308867097853951

051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00

394020061963944479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319

2661740802050217063228768716723360960729859168756973147706671368418802944996427808491545080627771902352094241225065558662157113545570916814161637315895999846

cc2751449a350f668590264ed76692694a80308a

5181942b9ebc31ce68dacb56c16fd79f

6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449

POSSIBLE SECRETS

a0784d7a4716f3feb4f64e7f4b39bf04
834895984c9262844b67d1998e4aa1af
115792089210356248762697446949407573530086143415290314195533631308867097853948
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
8325710961489029985546751289520108179287853048861315594709205902480503199884419224438643760392947333078086511627871
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087
36134250956749795798585127919587881956611106672985015071877198253568414405109
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
bae8e37fc83441b16034566b
115792089210356248762697446949407573529996955224135760342422259061068512044369
7626e75f37bbf9afc8931f7fbe3b6ff096c09aa4

⯈ PLAYSTORE INFORMATION

Title: Paired: Couples & Relationship

Score: 4.6143026 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support: Category:** Health & Fitness **Play Store URL:** com.getpaired.app

Developer Details: Paired - Relationship Advice & Quiz for Couples, 5958832408214147601, None, http://www.paired.com, support@paired.com,

Release Date: Sep 17, 2020 **Privacy Policy:** [Privacy link](#)

Description:

Welcome to Paired: the app that brings couples closer. Life can be messy, but your relationship doesn't have to be. Paired helps you build better communication, manage conflict, and deepen your connection in just 5 minutes a day. ❤ 8 million downloads ⬜ Google Play Awards, 2020 Winner in Personal Growth ⬜ Scientifically proven to increase relationship satisfaction ⬜ Featured in BBC News, The Times, Bustle, and more MAKE CONNECTION A DAILY HABIT With Paired's Daily Conversations, you can effortlessly dedicate time each day to build strong communication, encourage intimacy, and strengthen your relationship. JOIN PAIRED WITH YOUR PARTNER Add your answers to our questions for couples, and then unlock your partners responses to start a discussion, discover more about them and build a deep connection. REACH YOUR RELATIONSHIP GOALS Paired's guided journeys support you in developing the skills you need to help your relationship to thrive, with activities and conversations each day to build habits. DEEPEN YOUR CONNECTION Paired is the relationship app that helps couples to dive into subjects they don't often discuss, from household finances to love language, with guidance from experts to ensure sure it's always healthy and productive. FOCUS ON THE TOPICS THAT MATTER Paired has thousands of relationship games, quizzes, and questions, suitable for all stages of your couple, whether you're married, newly dating, or in a long-distance relationship. CELEBRATE EVERY EVENT, BIG AND SMALL Use Paired to keep track of the important dates in your relationship, from the big ones like anniversaries and birthdays, to the small, significant moments, like your first kiss or your favorite date night. Join millions around the world using the Paired, the app for couples, to build happier, lasting relationships. Questions? Suggestions? Let us know at support@paired.com. ***** Please note that Paired and the materials and information contained herein are not intended to, and do not constitute medical, psychological, or mental health advice, or diagnosis, and may not be used for such purposes. You should always consult with a qualified physician or mental health professional about your specific circumstances. Our Privacy Policy: https://www.paired.com/privacy_policy.html Our Terms and Conditions: https://www.paired.com/terms_and_conditions.html

☰ SCAN LOGS

Timestamp	Event	Error
2025-08-29 22:56:28	Generating Hashes	OK
2025-08-29 22:56:29	Extracting APK	OK
2025-08-29 22:56:29	Unzipping	OK

2025-08-29 22:56:36	Parsing APK with androguard	OK
2025-08-29 22:56:36	Extracting APK features using aapt/aapt2	OK
2025-08-29 22:56:36	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 22:56:38	Parsing AndroidManifest.xml	OK
2025-08-29 22:56:38	Extracting Manifest Data	OK
2025-08-29 22:56:38	Manifest Analysis Started	OK
2025-08-29 22:56:39	Performing Static Analysis on: Paired (com.getpaired.app)	OK
2025-08-29 22:56:39	Fetching Details from Play Store: com.getpaired.app	OK
2025-08-29 22:56:40	Checking for Malware Permissions	OK
2025-08-29 22:56:40	Fetching icon path	OK

2025-08-29 22:56:40	Library Binary Analysis Started	OK
2025-08-29 22:56:40	Reading Code Signing Certificate	OK
2025-08-29 22:56:40	Running APKiD 2.1.5	OK
2025-08-29 22:56:47	Detecting Trackers	OK
2025-08-29 22:56:51	Decompiling APK to Java with JADX	OK
2025-08-29 22:57:11	Converting DEX to Smali	OK
2025-08-29 22:57:11	Code Analysis Started on - java_source	OK
2025-08-29 22:57:18	Android SBOM Analysis Completed	OK
2025-08-29 22:57:30	Android SAST Completed	OK
2025-08-29 22:57:30	Android API Analysis Started	OK
2025-08-29 22:57:43	Android API Analysis Completed	OK

2025-08-29 22:57:43	Android Permission Mapping Started	OK
2025-08-29 22:57:53	Android Permission Mapping Completed	OK
2025-08-29 22:57:54	Android Behaviour Analysis Started	OK
2025-08-29 22:58:11	Android Behaviour Analysis Completed	OK
2025-08-29 22:58:11	Extracting Emails and URLs from Source Code	OK
2025-08-29 22:58:17	Email and URL Extraction Completed	OK
2025-08-29 22:58:17	Extracting String data from APK	OK
2025-08-29 22:58:17	Extracting String data from Code	OK
2025-08-29 22:58:17	Extracting String values and entropies from Code	OK
2025-08-29 22:58:22	Performing Malware check on extracted domains	OK
2025-08-29 22:58:29	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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