ANDROID STATIC ANALYSIS REPORT

LoosidApp (3.21.3)

File Name:	Loosid Sober Recovery Network_3.21.3_APKPure.xapk
Package Name:	com.loosidapp
Scan Date:	Nov. 17, 2024, 12:50 a.m.
App Security Score:	46/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	10/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
5	29	6	2	1

FILE INFORMATION

File Name: Loosid Sober Recovery Network_3.21.3_APKPure.xapk
Size: 178.75MB
MD5: 6dee2ac918a32875912addd7d1d46112
SHA1: d6275783c2102983eae91e745a55c0405a612e23
SHA256: f59722867f140be9e8940c02bf1e262db3dc226f22695fe0cb4b12d8d730a658

APP INFORMATION

App Name: LoosidApp
Package Name: com.loosidapp
Main Activity: com.loosidapp.MainActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 3.21.3

Android Version Code: 765

APP COMPONENTS

Activities: 18
Services: 29
Receivers: 25
Providers: 13
Exported Activities: 5
Exported Services: 2
Exported Receivers: 10
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: 2018-11-08 17:50:24+00:00
Valid To: 2048-11-08 17:50:24+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x62e21a73148c594b208801653bbac9574ec1d106
Hash Algorithm: sha256
md5: 018834ae599e5d2a4dc378f2ae82d5cb
sha1: 60187a93c660f071e15ee5f530cc14153436ef68
sha256: e3311fc74ccb5d997c1668ef72f943e939d7a86a7e57a880235b7f580a644140
sha512: c9444ab2dc4978733716aab113c6decb9ed2b12628f5786ddd9a5f3cf27c36052cf65a875cafe2ca13dee748a71408d816350096a60e63224c60485afd6021fe
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: bc60394767c71a32abcf26c0de194e63df7eb97b00f2247de0eda67b0b3a6e7d
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.

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_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
com.loosidapp.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference
android.permission.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.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.loosidapp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>6dee2ac918a32875912addd7d1d46112.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.BOARD check
Build.TAGS check
SIM operator check
network operator name check
ro.kernel.qemu check
possible ro.secure check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<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
SIM operator 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>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.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.TAGS 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>
</td></tr>
<tr><td>classes4.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
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.loosidapp.MainActivity	Schemes: https://, loosidapp://, deeplink://, Hosts: loosidapp.onelink.me, loosidapp.com, posts, audio, allaudios, account, guides, dating, soberhelp, chat, dailygratitude, Path Prefixes: /vZuQ, /linking,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.loosidapp,

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: **19** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App Link assetlinks.json file not found [android:name=com.loosidapp.MainActivity] [android:host=https://loosidapp.com]	high	App Link asset verification URL (https://loosidapp.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 403). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
3	Broadcast Receiver (com.dieam.reactnativepushnotification.modules.RNPushNotificationBootEventReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Broadcast Receiver (io.invertase.firebase.messaging.ReactNativeFirebaseMessagingReceiver) 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	Activity (com.canhub.cropper.CropImageActivity) 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.
6	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
7	Broadcast Receiver (com.onesignal.notifications.receivers.FCMBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
8	Activity (com.onesignal.notifications.activities.NotificationOpenedActivityHMS) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Broadcast Receiver (com.onesignal.notifications.receivers.NotificationDismissReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Broadcast Receiver (com.onesignal.notifications.receivers.BootUpReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Broadcast Receiver (com.onesignal.notifications.receivers.UpgradeReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
12	Activity (com.onesignal.notifications.activities.NotificationOpenedActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Activity (com.onesignal.notifications.activities.NotificationOpenedActivityAndroid22AndOlder) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
14	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
15	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.
16	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.
17	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

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

CODE ANALYSIS

HIGH: **3** | WARNING: **9** | INFO: **4** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ac/c.java ai/e.java an/a.java b9/a.java bh/k0.java c7/c.java ce/k.java ch/a.java ch/c.java ch/e0.java ch/h0.java ch/h1.java ch/k1.java ch/l0.java ch/l1.java ch/m1.java ch/o1.java ch/u1.java ch/y1.java cj/i.java cm/a.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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/amazon/device/simplesignin/a/c.java com/amazon/device/simplesignin/a/c/b.java com/apphud/sdk/ApphudLog.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1qSDK.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1jSDK.java com/appsflyer/internal/AFf1kSDK.java com/appsflyer/internal/AFg1jSDK.java com/appsflyer/reactnative/RNAppsFlyerModule.java com/brentvatne/exoplayer/j.java com/bugsnag/android/h0.java com/bugsnag/android/l1.java com/bumptech/glide/GeneratedAppGlideModuleImpl.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/canhub/cropper/CropImageActivity.java com/canhub/cropper/CropOverlayView.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/henninghall/date_picker/d.java com/henninghall/date_picker/pickers/AndroidNative.java com/json/InternalLog.java com/json/b.java com/json/f1.java com/json/reactnative/SmartlookAnalyticsM

NO	ISSUE	SEVERITY	STANDARDS	FILES
				oduleImpl.java com/json/sdk/common/logger/LogPrinter.java com/json/sdk/wireframe/a3.java com/json/sdk/wireframe/b3.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/d.java com/loosidapp/PushNotificationService.java com/loosidapp/b.java com/loosidapp/c.java com/loosidapp/d.java com/masteratul/exceptionhandler/DefaultErrorScreen.java com/microsoft/appcenter/reactnative/crashes/c.java com/oblador/storereview/b.java com/onesignal/common/c.java com/onesignal/debug/internal/logging/a.java com/onesignal/rnonesignalandroid/RNOneSignal.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/reactnativeapphudsdk/ApphudSdkModule.java com/reactnativecommunity/asyncstorage/c.java com/reactnativecommunity/webview/e.java com/reactnativecommunity/webview/i.java com/reactnativecommunity/webview/k.java com/reactnativedocumentpicker/RNDocu

NO	ISSUE	SEVERITY	STANDARDS	FILES
				mentPickerModule.java com/reactnativegooglesignin/RNGoogleSigninModule.java com/reactnativegooglesignin/b.java com/reactnativeimageresizer/ImageResizerModule.java com/reactnativeimageresizer/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/rnmaps/maps/MapModule.java com/rnmaps/maps/MapTileWorker.java com/rnmaps/maps/i.java com/rnmaps/maps/p.java com/rnmaps/maps/q.java com/rt2zz/reactnativecontacts/a.java com/superwall/sdk/logger/Loggable.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/layoutReanimation/AnimationsManager.java com/swmansion/reanimated/layoutReanimation/ReanimatedNativeHierarchyManager.java com/swmansion/reanimated/layoutReani

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	mation/SharedTransitionManager.java com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/swmansion/rnscreens/ScreensModule.java com/tanguyantoine/react/MusicControlModule.java com/tanguyantoine/react/MusicControlNotification.java com/th3rdwave/safeareacontext/k.java com/vonovak/AddCalendarEventModule.java com/yalantis/ucrop/UCropActivity.java com/yalantis/ucrop/task/BitmapCropTask.java com/yalantis/ucrop/view/b.java cp/c.java d1/f.java d8/a.java d8/d.java d8/j.java d9/f.java d9/i.java d9/j.java d9/m.java dl/i.java ei/a.java es/e.java eu/c.java expo/modules/av/player/PlayerData.java expo/modules/av/player/g.java expo/modules/av/video/e.java expo/modules/location/records/GeocodeResponse.java f/d.java f2/c.java f8/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				f8/q.java f8/r.java fc/c.java fe/a.java fh/a.java fi/a.java fl/f.java fl/n.java fl/p.java fy/c.java fz/e.java g8/d.java g9/a.java gc/d0.java gc/e0.java gc/y.java gh/b.java gn/d.java gs/n.java h2/p.java h2/t.java h2/x.java h7/a.java hh/g.java hh/o.java hh/p.java i2/c.java i8/h.java ii/c.java io/invertase/firebase/app/ReactNativeFirebaseAppModule.java io/invertase/firebase/app/a.java io/invertase/firebase/crashlytics/ReactNativeFirebaseCrashlyticsInitProvider.java io/invertase/firebase/crashlytics/ReactNativeFirebaseCrashlyticsModule.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingModule.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingReceiver.java io/invertase/firebase/utils/ReactNativeFire

NO	ISSUE	SEVERITY	STANDARDS	FILES
				baseUtilsModule.java iy/a.java j2/a.java j6/a.java j6/d.java j8/d.java j8/k.java js/k.java jy/d.java k1/d.java k6/g.java k6/n.java ka/f.java kh/i.java l5/n.java l8/a.java lh/d.java lj/f.java lr/a.java m/c.java m1/v.java mg/s.java mr/a.java mr/c.java mr/f.java n2/d.java n7/a.java n8/a.java nb/f.java nb/l.java o2/a.java o5/a.java o7/d.java o7/e.java o8/c.java oh/l.java oj/f.java oj/n.java org/wonday/orientation/a.java p1/c.java p2/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				p7/a.java pk/b.java q5/h.java q6/j.java qg/a.java qg/d.java qk/c.java qr/c.java qt/p.java r5/d.java r7/c.java r7/e.java r8/a.java rj/g.java rr/b.java ry/i.java s5/a.java s7/h.java s7/i.java s7/k.java s7/q.java s7/z.java sg/i.java si/a.java t1/c.java t2/q.java t7/i.java t7/j.java ta/d.java ts/e.java ty/b.java u7/e.java u7/i.java u8/a.java u8/b.java u8/c.java u8/d.java ui/d.java uj/r.java v5/a.java v7/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				v8/d.java v8/g.java v8/n.java v8/n0.java v8/s.java vi/b.java vs/h.java vt/g.java vt/m.java w3/g.java w7/c.java w7/d.java w7/g.java w7/s.java w7/t.java w7/u.java wb/a0.java wb/d0.java wb/k.java wb/k0.java wb/m0.java wb/t0.java wb/u0.java xg/g.java xi/g.java xk/c0.java xk/f0.java xk/g.java xk/i0.java xk/k.java xk/x.java y7/h.java y8/l.java yh/f.java yk/a.java yr/b.java yr/d.java z1/b.java z1/d.java z7/c.java z7/c0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				z7/e0.java z7/f.java z7/f0.java z7/n.java z7/p.java z7/q.java z7/u.java z8/e.java z8/f.java zg/a0.java zg/b.java zg/b0.java zg/c.java zg/j.java zg/t.java zg/v.java zg/x.java zh/q0.java zk/c.java zk/f.java
2	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	com/RNFetchBlob/d.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/k.java com/rnfs/RNFSManager.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java l9/a.java o8/c.java p6/a.java w9/a.java wb/t0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ay/g1.java com/apphud/sdk/ApphudUserProperty.java com/apphud/sdk/storage/SharedPreferencesStorage.java com/appsflyer/reactnative/RNAppsFlyerConstants.java com/bugsnag/android/g1.java com/bugsnag/android/v2.java com/json/CheckRecordingConfigRequest.java com/json/InternalLog.java com/json/RecordData.java com/json/RecordJobData.java com/json/SessionData.java com/json/SessionJobData.java com/json/sdk/common/job/JobIdStorage.java com/json/sdk/storage/SessionRecordingStorage.java com/onesignal/inAppMessages/internal/display/impl/i.java com/onesignal/inAppMessages/internal/prompt/impl/b.java com/onesignal/notifications/bridges/a.java com/onesignal/notifications/internal/c.java com/onesignal/notifications/receivers/FCMBroadcastReceiver.java com/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

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/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/subscriberattributes/SubscriberAttribute.java com/revenuecat/purchases/subscriberattributes/SubscriberAttributeKt.java com/superwall/sdk/config/models/Survey.java com/superwall/sdk/debug/DebugViewActivity.java com/superwall/sdk/models/config/RawFeatureFlag.java com/superwall/sdk/models/paywall/Paywall.java com/superwall/sdk/models/triggers/TriggerRuleOccurrence.java com/superwall/sdk/paywall/presentation/PaywallInfo.java com/superwall/sdk/paywall/vc/SuperwallPaywallActivity.java com/superwall/sdk/paywall/vc/web_view/templating/models/DeviceTemplate.java com/superwall/sdk/storage/core_data/entities/ManagedTriggerRuleOccurrence.java db/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				e6/d.java expo/modules/adapters/react/NativeModulesProxy.java expo/modules/webbrowser/OpenBrowserOptions.java fp/a.java ip/e.java jm/c.java k7/f.java q7/g.java s7/d.java s7/p.java s7/x.java u2/a.java vj/b.java wj/e.java wj/w.java x/v.java x8/g.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	com/RNFetchBlob/a.java com/canhub/cropper/CropImageActivity.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnativecommunity/webview/k.java com/rnmaps/maps/MapModule.java com/rnmaps/maps/a.java l9/a.java o8/c.java pk/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	b3/r1.java com/amazon/a/a/b/b.java com/amazon/a/a/i/b.java com/amazon/a/a/l/c.java com/appsflyer/internal/AFa1zSDK.java com/appsflyer/internal/AFb1hSDK.java com/json/o1.java com/loosidapp/PushNotificationService.java com/onesignal/common/AndroidUtils.java d3/b.java fl/o.java iz/d.java iz/h.java o3/c1.java oe/o1.java pm/h.java qf/o0.java tf/b.java uy/z.java vs/h.java vu/a.java wb/t0.java x2/r.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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/onesignal/session/internal/outcomes/impl/m.java com/reactnativecommunity/asyncstorage/f.java en/a.java fn/e.java je/m0.java je/t0.java r5/c.java sn/c.java v2/c.java v2/d.java vm/a.java x2/f.java x2/k.java
7	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/onesignal/inAppMessages/internal/display/impl/i.java com/superwall/sdk/paywall/vc/web_view/SWWebView.java com/superwall/sdk/view/SWWebViewOld.java n6/c.java
8	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 ez/c.java ez/d.java ez/i.java ez/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/amazon/a/a/o/b/a.java com/bugsnag/android/l0.java com/revenuecat/purchases/common/UtilsKt.java fc/a.java nt/b.java pk/b.java z9/c.java
10	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	cj/w.java com/bugsnag/android/RootDetector.java com/json/e4.java uj/i.java
11	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/appsflyer/internal/AFb1vSDK.java
12	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/json/sdk/common/storage/b.java vf/a.java
13	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	bd/a.java com/amazon/device/drm/LicensingService.java com/amazon/device/iap/PurchasingService.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
14	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	com/RNFetchBlob/h.java com/superwall/sdk/storage/CacheKeysKt.java d9/m.java v8/e.java z6/g.java
15	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/onesignal/inAppMessages/internal/display/impl/i.java com/superwall/sdk/view/SWWebViewOld.java
16	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	b9/j.java com/apphud/sdk/storage/SharedPreferencesStorage.java gc/d0.java h9/b.java sr/e.java vs/i.java yr/d.java
17	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	com/reactnativecommunity/clipboard/ClipboardModule.java
18	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
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00078	Get the network operator name	collection telephony	an/c.java com/appsflyer/internal/AFh1cSDK.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/onesignal/common/e.java fn/l.java wb/t0.java
00038	Query the phone number	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
			com/amazon/a/a/i/g.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFi1mSDK.java com/appsflyer/internal/AFi1sSDK.java com/dylanvann/fastimage/f.java com/loosidapp/d.java com/onesignal/common/AndroidUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/onesignal/location/internal/permissions/c.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/EverythingMeHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/HuaweiHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/NovaHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/OPPOHomeBader.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SonyHomeBadger.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/rnmaps/maps/d.java com/rnmaps/maps/l.java expo/modules/av/player/a.java f7/i.java gs/n.java i9/a.java ip/e.java j6/d.java lg/e0.java me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java mg/m0.java r8/a.java rd/a.java sr/e.java t2/n0.java u8/c.java w2/z.java wb/b.java wb/t0.java wb/u0.java wb/y0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/appsflyer/internal/AFb1uSDK.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java com/json/android/common/http/HttpClient.java com/revenuecat/purchases/common/HTTPClient.java com/superwall/sdk/network/RequestExecutor.java gn/b.java lg/t.java qk/c.java w2/m.java x8/g.java z6/b.java
00089	Connect to a URL and receive input stream from the server	command network	com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java com/bugsnag/android/i0.java com/bumptech/glide/load/data/j.java com/json/android/common/http/HttpClient.java com/reactnativeimageresizer/a.java com/revenuecat/purchases/common/HTTPClient.java com/rnfs/c.java com/superwall/sdk/network/RequestExecutor.java fc/c.java fl/n.java gn/b.java lg/t.java qk/c.java w2/m.java x8/g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/appsflyer/internal/AFb1uSDK.java com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1sSDK.java com/appsflyer/internal/AFf1oSDK.java com/bugsnag/android/i0.java com/bumptech/glide/load/data/j.java com/json/android/common/http/HttpClient.java com/revenuecat/purchases/common/HTTPClient.java com/rnfs/c.java com/superwall/sdk/network/RequestExecutor.java fl/n.java gn/b.java lg/t.java qg/d.java qk/c.java w2/m.java x8/g.java xg/f.java
00014	Read file into a stream and put it into a JSON object	file	bk/a.java com/appsflyer/internal/AFg1nSDK.java e9/j.java h9/a.java pk/c.java vj/f.java yb/k.java
			bk/a.java com/RNFetchBlob/a.java com/RNFetchBlob/d.java com/airbnb/android/react/lottie/h.java com/amazon/c/a/a/c.java com/appsflyer/internal/AFb1iSDK.java com/appsflyer/internal/AFg1nSDK.java com/bugsnag/android/RootDetector.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/bugsnag/android/h3.java com/bugsnag/android/v1.java com/bumptech/glide/load/a.java com/json/android/common/http/b.java com/json/android/common/http/extension/OutputStreamExtKt.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/reactnativecommunity/asyncstorage/c.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/revenuecat/purchases/common/FileHelper.java com/rnfs/RNFSManager.java com/rnfs/i.java com/rnmaps/maps/a.java com/rnmaps/maps/k.java com/rnmaps/maps/p.java d9/m.java e9/j.java en/b.java es/g.java gs/n.java h9/a.java i2/c.java j9/b.java jz/q.java k7/k.java lg/e0.java lg/g.java mr/e.java n7/a.java o5/b.java oz/b.java pk/c.java pu/k.java r8/a.java t2/b.java uj/a0.java v1/m.java v8/g.java vj/f.java w2/d.java w2/z.java

RULE ID	BEHAVIOUR	LABEL	FILES
			w7/g.java wb/k0.java yb/k.java z6/g.java z6/h.java zj/e.java
00091	Retrieve data from broadcast	collection	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/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1jSDK.java com/dieam/reactnativepushnotification/modules/RNPushNotification.java com/dieam/reactnativepushnotification/modules/RNPushNotificationPublisher.java com/masteratul/exceptionhandler/DefaultErrorScreen.java com/onesignal/core/activities/PermissionsActivity.java com/onesignal/notifications/receivers/FCMBroadcastReceiver.java expo/modules/location/services/LocationTaskService.java gc/i0.java ip/c.java wb/m0.java
			com/RNFetchBlob/d.java com/RNFetchBlob/g.java com/amazon/a/a/b/b.java com/appsflyer/internal/AFg1nSDK.java com/bugsnag/android/ndk/NativeBridge.java com/bugsnag/android/p1.java com/bugsnag/android/u.java com/json/android/common/http/extension/OutputStreamExtKt.java com/json/sdk/common/storage/Storage.java com/json/sdk/common/storage/cache/FileSimplePermanentCache.java com/oblador/vectoricons/a.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

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/superwall/sdk/storage/Storable.java en/b.java gs/n.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java j6/d.java j6/e.java j6/f.java jt/c0.java l9/f.java ls/d.java om/a.java p6/a.java q6/v.java q9/c.java r5/d.java r8/a.java v1/m.java vj/f.java w9/a.java z6/g.java z6/h.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/RNFetchBlob/g.java com/amazon/a/a/i/a.java com/amazon/a/a/i/g.java com/amazon/device/iap/internal/a/a.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1cSDK.java com/appsflyer/internal/AFc1jSDK.java com/appsflyer/internal/AFf1sSDK.java com/canhub/cropper/CropImageActivity.java com/loosidapp/d.java com/onesignal/common/AndroidUtils.java com/onesignal/location/internal/permissions/c.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/OPPOHomeBader.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SonyHomeBadger.java com/reactnative/ivpusic/imagepicker/PickerModule.java com/superwall/sdk/paywall/vc/PaywallView.java gc/c.java gs/n.java j6/a.java k6/g.java k6/n.java ks/a.java ks/c.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java sr/e.java u8/c.java ut/b.java ut/k.java wb/b.java wb/m0.java wb/t0.java wb/u0.java wb/y0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/a.java fn/e.java wb/t0.java
00072	Write HTTP input stream into a file	command network file	com/reactnativeimageresizer/a.java com/rnfs/c.java
00030	Connect to the remote server through the given URL	network	com/appsflyer/internal/AFb1uSDK.java com/bumptech/glide/load/data/j.java com/reactnativeimageresizer/a.java com/rnfs/c.java lg/t.java w2/m.java z6/b.java
00012	Read data and put it into a buffer stream	file	com/amazon/c/a/a/c.java com/json/android/common/http/b.java com/rnfs/i.java d9/m.java gs/n.java v8/g.java
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFi1oSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/reactnativedocumentpicker/RNDocumentPickerModule.java com/rt2zz/reactnativecontacts/a.java com/vonovak/a.java js/l.java p6/a.java wb/m0.java z9/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFi1oSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/reactnativedocumentpicker/RNDocumentPickerModule.java com/rt2zz/reactnativecontacts/a.java com/vonovak/a.java js/l.java p6/a.java wb/m0.java z9/f.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1sSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java com/reactnativecommunity/cameraroll/CameraRollModule.java p6/a.java wb/m0.java
00191	Get messages in the SMS inbox	sms	com/RNFetchBlob/g.java com/appsflyer/internal/AFi1mSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1qSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java com/reactnativecommunity/cameraroll/CameraRollModule.java p6/a.java wb/b.java wb/m0.java wb/t0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFi1oSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/reactnativedocumentpicker/RNDocumentPickerModule.java com/rt2zz/reactnativecontacts/a.java com/vonovak/a.java js/l.java p6/a.java wb/m0.java z9/f.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFi1oSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/reactnativedocumentpicker/RNDocumentPickerModule.java com/rt2zz/reactnativecontacts/a.java com/vonovak/a.java js/l.java p6/a.java wb/m0.java z9/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1oSDK.java com/appsflyer/internal/AFi1sSDK.java com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/reactnativedocumentpicker/RNDocumentPickerModule.java js/l.java p6/a.java r7/c.java wb/m0.java z1/b.java z1/d.java
00028	Read file from assets directory	file	com/rnfs/RNFSManager.java lg/c.java w2/a.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1jSDK.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/rnfs/RNFSManager.java j6/d.java p6/a.java
00187	Query a URI and check the result	collection sms calllog calendar	com/onesignal/notifications/internal/badges/impl/shortcutbadger/impl/SamsungHomeBadger.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/rt2zz/reactnativecontacts/a.java wb/m0.java z1/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00132	Query The ISO country code	telephony collection	an/c.java mg/m0.java t2/n0.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/onesignal/common/AndroidUtils.java com/onesignal/location/internal/permissions/c.java k6/g.java sr/e.java ut/b.java ut/k.java wb/t0.java wb/u0.java
00094	Connect to a URL and read data from it	command network	ai/i0.java com/reactnativeimageresizer/a.java gn/b.java lg/t.java ty/a.java w2/m.java yj/a.java
00043	Calculate WiFi signal strength	collection wifi	kq/e.java
00147	Get the time of current location	collection location	qt/l.java
00004	Get filename and put it to JSON object	file collection	cc/a.java e9/f.java om/a.java yb/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00125	Check if the given file path exist	file	com/reactnativecommunity/cameraroll/CameraRollModule.java e9/f.java gs/n.java
00121	Create a directory	file command	com/reactnativecommunity/cameraroll/CameraRollModule.java expo/modules/av/AVManager.java gs/n.java
00024	Write file after Base64 decoding	reflection file	com/RNFetchBlob/a.java com/RNFetchBlob/d.java com/reactnativeimageresizer/a.java gs/n.java j6/e.java j6/f.java q6/v.java
00104	Check if the given path is directory	file	com/reactnativecommunity/cameraroll/CameraRollModule.java expo/modules/av/AVManager.java gs/n.java
00114	Create a secure socket connection to the proxy address	network command	zy/f.java
00162	Create InetSocketAddress object and connecting to it	socket	ez/b.java ez/j.java
00163	Create new Socket and connecting to it	socket	ez/b.java ez/j.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/reactnativeimageresizer/a.java com/rnmaps/maps/p.java s2/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	com/reactnativecommunity/cameraroll/CameraRollModule.java
00161	Perform accessibility service action on accessibility node info	accessibility service	m1/v.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	m1/v.java
00005	Get absolute path of file and put it to JSON object	file	com/appsflyer/internal/AFg1nSDK.java om/a.java vj/f.java
00108	Read the input stream from given URL	network command	com/reactnativeimageresizer/a.java gn/b.java lg/t.java w2/m.java
00026	Method reflection	reflection	lv/a.java lv/b.java
00175	Get notification manager and cancel notifications	notification	u8/c.java
00015	Put buffer stream (data) to JSON object	file	wb/t0.java
00003	Put the compressed bitmap data into JSON object	camera	y8/l.java

RULE ID	BEHAVIOUR	LABEL	FILES
00080	Save recorded audio/video to a file	record file	expo/modules/av/AVManager.java
00101	Initialize recorder	record	expo/modules/av/AVManager.java
00199	Stop recording and release recording resources	record	expo/modules/av/AVManager.java
00198	Initialize the recorder and start recording	record	expo/modules/av/AVManager.java
00136	Stop recording	record command	expo/modules/av/AVManager.java
00194	Set the audio source (MIC) and recorded file format	record	expo/modules/av/AVManager.java
00090	Set recroded audio/video file format	record	expo/modules/av/AVManager.java
00197	Set the audio encoder and initialize the recorder	record	expo/modules/av/AVManager.java
00102	Set the phone speaker on	command	expo/modules/av/AVManager.java
00138	Set the audio source (MIC)	record	expo/modules/av/AVManager.java
00196	Set the recorded file format and output path	record file	expo/modules/av/AVManager.java
00133	Start recording	record command	expo/modules/av/AVManager.java
00041	Save recorded audio/video to file	record	expo/modules/av/AVManager.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://loosid-1541174860307.firebaseio.com
Firebase Remote Config check failed	info	Failed to check for Firebase Remote Config. Please verify this manually. Error: ConnectionError(MaxRetryError('HTTPSConnectionPool(host=\'firebaseremoteconfig.googleapis.com\', port=443): Max retries exceeded with url: /v1/projects/628723516426/namespaces/firebase:fetch?key=AIzaSyB5xYuZfnHWKzY5RvuS4ZrSyFIzsaz52jI (Caused by NameResolutionError("<urllib3.connection.HTTPSConnection object at 0x7f99c1639ee0>: Failed to resolve \'firebaseremoteconfig.googleapis.com\' ([Errno -3] Temporary failure in name resolution)"))'))

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/25	android.permission.READ_EXTERNAL_STORAGE, android.permission.INTERNET, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.CAMERA, android.permission.READ_CONTACTS, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_PHONE_STATE, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE
Other Common Permissions	6/44	android.permission.FOREGROUND_SERVICE, android.permission.READ_CALENDAR, com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.ACTIVITY_RECOGNITION

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
sdlsdk.s	ok	No Geolocation information available.
bugsnag.com	ok	No Geolocation information available.
api-paywalls.revenuecat.com	ok	No Geolocation information available.
scdn-stestsettings.s	ok	No Geolocation information available.
graph-video.s	ok	No Geolocation information available.
firebase-settings.crashlytics.com	ok	No Geolocation information available.
pinterest.com	ok	No Geolocation information available.
sars.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
rev.cat	ok	No Geolocation information available.
mobile.events.data.microsoft.com	ok	No Geolocation information available.
docs.revenuecat.com	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.
api.revenuecat.com	ok	No Geolocation information available.
developer.android.com	ok	No Geolocation information available.
pagead2.googlesyndication.com	ok	No Geolocation information available.
notify.bugsnag.com	ok	No Geolocation information available.
api.onesignal.com	ok	No Geolocation information available.
plus.google.com	ok	No Geolocation information available.
www.amazon.com	ok	No Geolocation information available.
superwall.com	ok	No Geolocation information available.
sregister.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.
errors.rev.cat	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
twitter.com	ok	No Geolocation information available.
dashif.org	ok	No Geolocation information available.
docs.bugsnag.com	ok	No Geolocation information available.
appleid.a	ok	No Geolocation information available.
api.mixpanel.com	ok	No Geolocation information available.
schemas.microsoft.com	ok	No Geolocation information available.
ns.adobe.com	ok	No Geolocation information available.
sviap.s	ok	No Geolocation information available.
facebook.com	ok	No Geolocation information available.
google.com	ok	No Geolocation information available.
sapp.s	ok	No Geolocation information available.
docs.apphud.com	ok	No Geolocation information available.
www.facebook.com	ok	No Geolocation information available.
in.appcenter.ms	ok	No Geolocation information available.
api-diagnostics.revenuecat.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
simpression.s	ok	No Geolocation information available.
issuetracker.google.com	ok	No Geolocation information available.
default.url	ok	No Geolocation information available.
docs.swmansion.com	ok	No Geolocation information available.
appleid.apple.com	ok	No Geolocation information available.
svalidate.s	ok	No Geolocation information available.
g.co	ok	No Geolocation information available.
scdn-ssettings.s	ok	No Geolocation information available.
api.apphud.com	ok	No Geolocation information available.
firebase.google.com	ok	No Geolocation information available.
developer.apple.com	ok	No Geolocation information available.
developers.facebook.com	ok	No Geolocation information available.
aomedia.org	ok	No Geolocation information available.
sconversions.s	ok	No Geolocation information available.
graph.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
accounts.google.com	ok	No Geolocation information available.
github.com	ok	No Geolocation information available.
expo.dev	ok	No Geolocation information available.
play.google.com	ok	No Geolocation information available.
.facebook.com	ok	No Geolocation information available.
loosid-1541174860307.firebaseio.com	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
slaunches.s	ok	No Geolocation information available.
www.w3.org	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.
sessions.bugsnag.com	ok	No Geolocation information available.
sinapps.s	ok	No Geolocation information available.
sattr.s	ok	No Geolocation information available.
exoplayer.dev	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Bugsnag	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/207
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Microsoft Visual Studio App Center Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/243
Microsoft Visual Studio App Center Crashes	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/238
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118
OneSignal		https://reports.exodus-privacy.eu.org/trackers/193

HARDCODED SECRETS

POSSIBLE SECRETS
"CodePushDeploymentKey" : "LCnYbIMTj46B1_qR3Zb9tNemfl0zHkYmCvryB"
"bugsnag_api_key" : "6191a2dca5c02d4a61b126616a8e8fa8"
"com.google.firebase.crashlytics.mapping_file_id" : "6c9f7d2b4a38485e80c20b0cc190e5ab"
"facebook_client_token" : "209611e215d87889f907983f59fe33c3"
"firebase_database_url" : "https://loosid-1541174860307.firebaseio.com"
"google_api_key" : "AIzaSyB5xYuZfnHWKzY5RvuS4ZrSyFIzsaz52jI"
"google_crash_reporting_api_key" : "AIzaSyB5xYuZfnHWKzY5RvuS4ZrSyFIzsaz52jI"
e2719d58-a985-b3c9-781a-b030af78d30e
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
3071c8717539de5d5353f4c8cd59a032
c682b8144a8dd52bc1ad63
9b8f518b086098de3d77736f9458a3d2f6f95a37
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
c56fb7d591ba6704df047fd98f535372fea00211

POSSIBLE SECRETS
470fa2b4ae81cd56ecbcda9735803434cec591fa
cc2751449a350f668590264ed76692694a80308a
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
ee4655b3ec0d2ace448aa481008538b7
85053bf24bba75239b16a601d9387e17
7d73d21f1bd82c9e5268b6dcf9fde2cb
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
UC1upXWg5QVmyOSwozp755xLqquBKjjU+di6U8QhMlM=
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
11f00dc53be30cfe213781d453297cf1

POSSIBLE SECRETS
9a04f079-9840-4286-ab92-e65be0885f95
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901

PLAYSTORE INFORMATION

Title: Loosid: Sober Recovery Network

Score: 4.33 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Social **Play Store URL:** com.loosidapp

Developer Details: Loosid App LLC, Loosid+App+LLC, None, http://loosidapp.com, support@loosidapp.com,

Release Date: Nov 15, 2018 **Privacy Policy:** Privacy link

Description:

Sober shouldn’t be somber! Discover Loosid, the ultimate sobriety companion app for anyone looking to join a clean, sober community. Loosid is a revolutionary app designed to help people in recovery or those who choose to get sober, connect and chat with like-minded individuals, access resources, milestones, and counters, and find sober events and activities in their area. Featured on Forbes, Today, NY Times, People, Good Morning America, and more! At the core of the Loosid app is its robust community feature, which is designed to provide users with support where they can connect and chat with others who are on a similar journey. One of the key features of the Loosid community is its inclusivity. The app is not limited to people who are in recovery from alcohol or drug addiction, but also caters to those who have chosen to live a sober lifestyle for personal or health reasons. This creates a vibrant and diverse environment where users can celebrate milestones together, build relationships and friendships, and find inspiration to stay sober. Loosid is the guide to living sober and alcohol clean: whether you want to set a clean time counter, connect with other sober members, listen to audio episodes of how people have overcome alcohol or addiction, live sober in the rooms and out, or date other clean singles, Loosid is for you! The Loosid app is an essential tool for anyone who is committed to living a sober lifestyle. Its focus on community, inclusivity, safety, and support makes it an ideal platform for individuals who are in recovery from addiction, as well as those who have chosen to live a sober lifestyle for other reasons. With its user-friendly interface and wealth of chat features, the Loosid app is a must-have for anyone who wants to connect with others, find inspiration, and stay on track with their sobriety journey. One of the most exciting features of Loosid is its social component. With Loosid, you'll be able to forge connections with sober individuals in your area and around the world. Whether you're looking for a sober buddy to hit up a meeting with, try out sober dating, or just to chat with someone who understands the challenges of sobriety, Loosid has you covered. In addition to its social features, Loosid also offers a range of helpful tools and resources to help you stay sober. You'll have access to a clean time counter and tips, aa hotlines, rehab & treatment centers, and motivational quotes and voices from those that have overcome addiction to keep you focused and inspired. You can also use the app to track your progress, set goals, and monitor your sober time. Looking for ways to stay engaged and active in our social network? Loosid has a range of community events to widen your sober grid. With Loosid, online dating has never been easier, helping sober singles connect and mingle. Loosid also offers boozeless restaurant guides, so you and your friends can celebrate milestones while also discovering no alcohol options. HIGHLIGHTS If you're looking for ways to stay engaged and active in your sobriety, Loosid has a range of community events and help. Meet and socialize with sober friends! Loosid also offers boozeless guides, so you and your friends can discover new and exciting places to explore or attend a function without the peer pressure of drinking alcohol to stay social. Take time to set your sobriety goals. Celebrate addiction recovery milestones featuring our customizable trackers and counters. Then celebrate your milestone by taking advantage of our dating system or non-alcoholic guides! Need help? Use our crisis hotline for immediate help and support, and get access to aa (alcoholics anonymous) and local treatment center lists. Discover safety on the clean road to alcohol or addiction recovery. Loosid is the perfect companion app to help you stay on track and live your best life. Celebrate recovery and sobriety today! https://loosidapp.com/contact-us/

SCAN LOGS

Timestamp	Event	Error
2024-11-17 00:50:46	Generating Hashes	OK
2024-11-17 00:50:47	Extracting APK	OK
2024-11-17 00:50:47	Unzipping	OK
2024-11-17 00:50:58	Getting Hardcoded Certificates/Keystores	OK
2024-11-17 00:50:58	Parsing APK with androguard	OK
2024-11-17 00:51:24	Parsing AndroidManifest.xml	OK
2024-11-17 00:51:24	Extracting Manifest Data	OK

2024-11-17 00:51:24	Performing Static Analysis on: LoosidApp (com.loosidapp)	OK
2024-11-17 00:51:24	Fetching Details from Play Store: com.loosidapp	OK
2024-11-17 00:51:25	Manifest Analysis Started	OK
2024-11-17 00:51:25	Checking for Malware Permissions	OK
2024-11-17 00:51:25	Fetching icon path	OK
2024-11-17 00:51:25	Library Binary Analysis Started	OK
2024-11-17 00:51:25	Reading Code Signing Certificate	OK
2024-11-17 00:51:28	Running APKiD 2.1.5	OK
2024-11-17 00:51:43	Updating Trackers Database....	OK
2024-11-17 00:51:43	Detecting Trackers	OK

2024-11-17 00:51:52	Decompiling APK to Java with JADX	OK
2024-11-17 00:57:13	Converting DEX to Smali	OK
2024-11-17 00:57:13	Code Analysis Started on - java_source	OK
2024-11-17 01:03:09	Android SAST Completed	OK
2024-11-17 01:03:09	Android API Analysis Started	OK
2024-11-17 01:03:48	Android API Analysis Completed	OK
2024-11-17 01:03:49	Android Permission Mapping Started	OK
2024-11-17 01:05:14	Android Permission Mapping Completed	OK
2024-11-17 01:05:30	Email and URL Extraction Completed	OK
2024-11-17 01:05:30	Android Behaviour Analysis Started	OK
2024-11-17 01:06:25	Android Behaviour Analysis Completed	OK

2024-11-17 01:06:25	Extracting String data from APK	OK
2024-11-17 01:06:25	Extracting String data from Code	OK
2024-11-17 01:06:25	Extracting String values and entropies from Code	OK
2024-11-17 01:06:53	Failed to check for Firebase Remote Config	ConnectionError(MaxRetryError('HTTPSConnectionPool(host=\'firebaseremoteconfig.googleapis.com\', port=443): Max retries exceeded with url: /v1/projects/628723516426/namespaces/firebase:fetch?key=AIzaSyB5xYuZfnHWKzY5RvuS4ZrSyFIzsaz52jI (Caused by NameResolutionError("<urllib3.connection.HTTPSConnection object at 0x7f99c1639ee0>: Failed to resolve \'firebaseremoteconfig.googleapis.com\' ([Errno -3] Temporary failure in name resolution)"))'))
2024-11-17 01:06:53	Performing Malware check on extracted domains	OK
2024-11-17 01:15:33	Saving to Database	OK
2024-11-17 02:22:25	Unzipping	OK
2024-11-17 02:22:34	Unzipping	OK

Report Generated by - MobSF v4.1.9

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.