MOBSF

ANDROID STATIC ANALYSIS REPORT

Soluna (1.10.9)

File Name:	com.kooth.serenity_241217681.apk
Package Name:	com.kooth.serenity
Scan Date:	Aug. 30, 2025, 10:46 p.m.
App Security Score:	57/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	17	3	3	2

FILE INFORMATION

File Name: com.kooth.serenity_241217681.apk
Size: 24.39MB
MD5: a245df38b0e2dafd557cc5f2ef231456
SHA1: f6bda68ce92cbf1d2e092ba9d0ee910ba80973e7
SHA256: bf4ec8929338ab8e2d55733eb392e492112ae9f8452971313cbfbd89cc5c7775

APP INFORMATION

App Name: Soluna
Package Name: com.kooth.serenity
Main Activity: com.kooth.serenity.MainActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 1.10.9

Android Version Code: 241217681

APP COMPONENTS

Activities: 6
Services: 11
Receivers: 4
Providers: 6
Exported Activities: 1
Exported Services: 1
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2023-08-24 15:44:10+00:00
Valid To: 2053-08-24 15:44:10+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x89d78f4f613564860a7b7b6001cb1f8013cf061
Hash Algorithm: sha256
md5: 186aea7e003a5b96951949ba2c1d62dc
sha1: 1a2072394d0c35203ad9139e5114c31035c634df
sha256: abccb42f8b6b6a0b9f1e9e598c1d699a9438a38b53ab40d41c79db4420747f8f
sha512: c92e3e04b761629f2e60764ace1b6fb2b4f138e6a8a175a1c5f565ba6a32c088768608bf8ef2e4c858e6921c0415798f9bbe6f054eea65668a9e64c99fccb29c
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: ab5825f6040ef9df638f705ccf857c934961892fde8284f864ea58ed1729d120
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	normal	enables foreground services for media playback.	Allows a regular application to use Service.startForeground with the type "mediaPlayback".
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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.kooth.serenity.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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.

PERMISSION	STATUS	INFO	DESCRIPTION
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.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.
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.

PERMISSION	STATUS	INFO	DESCRIPTION
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
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible Build.SERIAL check SIM operator check network operator name check ro.kernel.qemu check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</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>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></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
Build.TAGS check
network operator name check
possible ro.secure check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.kooth.serenity.MainActivity	Schemes: com.kooth.serenity://, exp+kooth-costanza-mobile-app://,
com.auth0.android.provider.RedirectActivity	Schemes: com.kooth.serenity://, Hosts: us-kooth-live.us.auth0.com, Path Prefixes: /android/com.kooth.serenity/callback,

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: 0 | WARNING: 6 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Service (com.doublesymmetry.trackplayer.service.MusicService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity (com.auth0.android.provider.RedirectActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	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.
6	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ae/h0.java ag/c.java b5/c.java be/a.java be/b0.java be/c.java be/e0.java be/f1.java be/i0.java be/j1.java be/s0.java be/v0.java be/w0.java be/x0.java be/z0.java bm/c.java c0/c.java cg/g.java cg/n.java cm/b.java cm/c.java cm/d.java com/appsflyer/internal/AFa1aSDK.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1uSDK.java com/appsflyer/internal/AFc1vSDK.java com/appsflyer/internal/AFf1cSDK.java com/appsflyer/internal/AFf1dSDK.java com/appsflyer/internal/AFf1hSDK.java com/appsflyer/internal/AFf1kSDK.java com/appsflyer/internal/AFf1lSDK.java com/appsflyer/internal/AFf1tSDK.java com/appsflyer/internal/AFg1hSDK.java com/appsflyer/internal/AFg1jSDK.java com/appsflyer/internal/AFg1nSDK.java com/appsflyer/reactnative/RNAppsFlyerModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/appsflyer/share/CrossPromotionHelper.java com/appsflyer/share/LinkGenerator.java com/auth0/android/provider/a.java com/auth0/android/provider/c.java com/auth0/android/provider/e.java com/auth0/android/provider/h.java com/auth0/android/provider/l.java com/auth0/android/provider/m.java com/auth0/android/provider/q.java com/auth0/android/request/internal/k.java com/emeraldsanto/encryptedstorage/RNEncryptedStorageModule.java com/henninghall/date_picker/d.java com/henninghall/date_picker/pickers/AndroidNative.java com/reactnativecommunity/asyncstorage/c.java com/reactnativecommunity/webview/e.java com/reactnativecommunity/webview/i.java com/reactnativecommunity/webview/k.java com/shopify/reactnative/skia/PlatformContext.java com/shopify/reactnative/skia/RNSkiaModule.java com/shopify/reactnative/skia/SkiaBaseView.java com/shopify/reactnative/skia/ViewScreenshotService.java com/swmansion/gesturehandler/react/RNGestureHandlerModule.java com/swmansion/gesturehandler/react/i.java com/swmansion/gesturehandler/react/j.java com/swmansion/reanimated/NativeMetho

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	dsHelper.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 com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/swmansion/rnscreens/ScreensModule.java com/th3rdwave/safeareacontext/k.java com/zmxv/RNSound/RNSoundModule.java d0/b.java d0/d.java e5/b.java ei/c.java expo/modules/av/player/PlayerData.java expo/modules/av/video/e.java expo/modules/location/records/GeocodeResponse.java expo/modules/notifications/service/NotificationsService.java expo/modules/updates/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				expo/modules/updates/b.java expo/modules/updates/d.java expo/modules/updates/g.java expo/modules/updates/h.java f5/e.java f5/j.java fb/k.java fe/b.java ff/d.java g7/f.java ge/m.java gm/d.java hb/a.java hi/b.java hm/d.java hq/c.java ht/j.java i3/q.java i3/u.java im/c.java im/d.java im/h.java im/i.java io/sentry/android/core/u.java io/sentry/android/replay/s.java io/sentry/android/replay/v.java io/sentry/l6.java ir/e.java k3/a.java kf/l.java kf/m.java kl/b.java kl/c.java kl/d.java km/a.java km/b.java km/c.java km/d.java km/e.java kq/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				lm/h.java lp/d.java mh/a.java mh/d.java mh/f.java mm/g.java n/a.java n/b.java n3/h.java ng/b.java o/b.java o0/a.java o3/d.java o5/a.java og/c.java ok/a.java ol/a.java p001if/g.java p3/a.java p4/j.java ph/g.java pk/p.java pl/c.java pl/d.java pl/e.java pl/g.java pt/a.java rh/g.java ri/b.java rj/e.java s/f.java s0/q.java s3/a.java sd/x.java se/a.java sk/c.java t3/l0.java te/a.java tk/a.java tq/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				u8/a.java u8/g.java ud/g.java uh/c.java uk/b.java vf/a.java vf/b.java vf/c.java vq/b.java w1/g.java wa/a.java we/c.java wh/a.java wk/a.java wm/c.java xi/f.java xk/a.java xk/b.java y/c.java yd/b.java yd/c.java yd/d.java yd/h.java yd/i.java yd/r.java yd/t.java yd/u.java yl/a.java z7/d.java za/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	a1/r1.java c1/b.java com/appsflyer/internal/AFa1uSDK.java com/appsflyer/internal/AFb1gSDK.java expo/modules/updates/h.java lr/d.java lr/h.java o1/b1.java on/a.java qb/p1.java rd/r.java tj/b.java vc/o0.java w0/r.java wq/z.java yc/b.java
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	bm/d.java com/appsflyer/reactnative/RNAppsFlyerConstants.java expo/modules/adapters/react/NativeModulesProxy.java expo/modules/updates/d.java expo/modules/updates/g.java i4/c.java im/j.java k8/h.java rc/a.java t0/a.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/reactnativecommunity/webview/k.java h6/a.java i3/u.java ng/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	ab/b.java io/sentry/android/core/internal/util/n.java vh/b.java zi/a.java
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/reactnativecommunity/asyncstorage/f.java lb/b0.java lb/h0.java o3/c.java rd/f.java rd/k.java tb/c.java tb/d.java u0/c.java u0/d.java w0/f.java w0/k.java
7	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	as/a.java bm/a.java bs/a.java cs/a.java ds/a.java ns/e.java uk/b.java x5/a.java y9/a.java
8	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/n.java vh/a.java ya/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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/reactnativecommunity/webview/k.java h6/a.java io/sentry/android/core/a1.java r6/a.java
10	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	hr/c.java hr/d.java hr/i.java hr/j.java
11	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	li/a.java y4/g.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	ad/a.java
13	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	io/sentry/util/u.java kk/b.java ng/b.java u6/c.java
14	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	f5/k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
15	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	cj/a.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	a7/a.java com/airbnb/android/react/lottie/h.java com/appsflyer/internal/AFb1iSDK.java com/appsflyer/internal/AFg1jSDK.java com/reactnativecommunity/asyncstorage/c.java expo/modules/updates/h.java f6/b.java hn/j.java hn/l.java i3/u.java io/sentry/android/replay/g.java io/sentry/cache/b.java io/sentry/cache/c.java io/sentry/cache/e.java io/sentry/config/e.java io/sentry/p2.java io/sentry/r2.java io/sentry/util/e.java io/sentry/w.java k3/b.java li/a.java ng/c.java nr/x.java qd/i.java qd/j0.java s0/b.java sd/b.java v0/c.java v0/y.java vr/b.java xi/h.java y4/g.java y4/h.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFf1qSDK.java com/appsflyer/internal/AFi1iSDK.java com/appsflyer/internal/AFi1nSDK.java com/auth0/android/provider/q.java d6/b.java expo/modules/av/player/a.java expo/modules/notifications/service/NotificationsService.java expo/modules/updates/d.java h4/e.java ii/e.java m5/g.java me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java qd/j0.java s0/m0.java sd/v0.java v0/y.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/appsflyer/internal/AFg1jSDK.java d4/a.java expo/modules/updates/h.java gk/c0.java h6/f.java i3/u.java io/sentry/android/core/a1.java io/sentry/android/core/cache/b.java io/sentry/android/replay/capture/f.java io/sentry/android/replay/g.java io/sentry/cache/b.java io/sentry/cache/c.java io/sentry/cache/e.java io/sentry/j5.java io/sentry/p.java io/sentry/p2.java io/sentry/r2.java io/sentry/w.java l6/c.java o3/d.java p4/v.java r6/a.java y4/g.java y4/h.java
00012	Read data and put it into a buffer stream	file	io/sentry/cache/b.java io/sentry/cache/e.java io/sentry/config/e.java io/sentry/p2.java io/sentry/util/e.java io/sentry/w.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	be/m1.java com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1bSDK.java com/appsflyer/internal/AFc1vSDK.java com/appsflyer/internal/AFf1vSDK.java com/auth0/android/provider/d.java com/auth0/android/provider/q.java expo/modules/notifications/service/NotificationsService.java ii/e.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java sd/v0.java
00014	Read file into a stream and put it into a JSON object	file	com/appsflyer/internal/AFg1jSDK.java expo/modules/updates/h.java ng/c.java
00096	Connect to a URL and set request method	command network	com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java og/c.java qd/w.java v0/l.java y4/b.java
00089	Connect to a URL and receive input stream from the server	command network	com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java og/c.java qd/w.java v0/l.java
00030	Connect to the remote server through the given URL	network	qd/w.java v0/l.java y4/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/appsflyer/internal/AFd1mSDK.java com/appsflyer/internal/AFe1qSDK.java com/appsflyer/internal/AFf1jSDK.java og/c.java qd/w.java v0/l.java
00094	Connect to a URL and read data from it	command network	com/shopify/reactnative/skia/PlatformContext.java qd/w.java v0/l.java vq/a.java
00108	Read the input stream from given URL	network command	qd/w.java v0/l.java
00028	Read file from assets directory	file	qd/c.java v0/a.java
00191	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFi1bSDK.java com/appsflyer/internal/AFi1iSDK.java com/appsflyer/internal/AFi1jSDK.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	be/m1.java ii/e.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1jSDK.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/appsflyer/internal/AFb1jSDK.java com/appsflyer/internal/AFi1bSDK.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/AFi1bSDK.java d0/b.java d0/d.java
00078	Get the network operator name	collection telephony	com/appsflyer/internal/AFi1xSDK.java
00080	Save recorded audio/video to a file	record file	expo/modules/av/AVManager.java
00101	Initialize recorder	record	expo/modules/av/AVManager.java
00121	Create a directory	file command	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

RULE ID	BEHAVIOUR	LABEL	FILES
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
00104	Check if the given path is directory	file	expo/modules/av/AVManager.java
00041	Save recorded audio/video to file	record	expo/modules/av/AVManager.java
00056	Modify voice volume	control	com/zmxv/RNSound/RNSoundModule.java
00005	Get absolute path of file and put it to JSON object	file	com/appsflyer/internal/AFg1jSDK.java expo/modules/updates/h.java
00091	Retrieve data from broadcast	collection	com/appsflyer/internal/AFb1vSDK.java com/appsflyer/internal/AFc1vSDK.java expo/modules/location/services/LocationTaskService.java expo/modules/notifications/service/NotificationsService.java
00162	Create InetSocketAddress object and connecting to it	socket	hr/b.java hr/j.java
00163	Create new Socket and connecting to it	socket	hr/b.java hr/j.java
00026	Method reflection	reflection	eo/a.java eo/b.java
00132	Query The ISO country code	telephony collection	s0/m0.java sd/v0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00189	Get the content of a SMS message	sms	com/appsflyer/internal/AFi1bSDK.java u6/f.java
00188	Get the address of a SMS message	sms	com/appsflyer/internal/AFi1bSDK.java u6/f.java
00200	Query data from the contact list	collection contact	com/appsflyer/internal/AFi1bSDK.java u6/f.java
00201	Query data from the call log	collection calllog	com/appsflyer/internal/AFi1bSDK.java u6/f.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/a.java
00114	Create a secure socket connection to the proxy address	network command	cr/f.java
00130	Get the current WIFI information	wifi collection	uk/b.java
00134	Get the current WiFi IP address	wifi collection	uk/b.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	r0/a.java
00187	Query a URI and check the result	collection sms calllog calendar	d0/d.java
00043	Calculate WiFi signal strength	collection wifi	hh/e.java
00147	Get the time of current location	collection location	pk/l.java
00024	Write file after Base64 decoding	reflection file	p4/v.java

RULE ID	BEHAVIOUR	LABEL	FILES
00175	Get notification manager and cancel notifications	notification	wk/a.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/804787746683/namespaces/firebase:fetch?key=AIzaSyDfAwDQ4mpB4z66zmcm_JNMXiBAo0Uqxvg. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/25	android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.RECORD_AUDIO, android.permission.SYSTEM_ALERT_WINDOW, android.permission.VIBRATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	6/44	android.permission.MODIFY_AUDIO_SETTINGS, android.permission.FOREGROUND_SERVICE, android.permission.ACTIVITY_RECOGNITION, 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
www.risktabsprev10pxrise25pxblueding300ballfordearnwildbox.fairlackverspairjunetechifpickevil	ok	No Geolocation information available.
www.wencodeuricomponent	ok	No Geolocation information available.
www.css	ok	No Geolocation information available.
www.interpretation	ok	No Geolocation information available.
sinapps.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
plus.google.com	ok	**IP:** 172.217.12.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.251.40.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
default.url	ok	No Geolocation information available.
www.world	ok	**IP:** 75.2.38.108 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
sdlsdk.s	ok	No Geolocation information available.
www.years	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
.css	ok	No Geolocation information available.
sconversions.s	ok	No Geolocation information available.
simpression.s	ok	No Geolocation information available.
developer.android.com	ok	**IP:** 142.250.217.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
smonitorsdk.s	ok	No Geolocation information available.
sgcdsdk.s	ok	No Geolocation information available.
sattr.s	ok	No Geolocation information available.
docs.swmansion.com	ok	**IP:** 172.67.142.188 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
www.hortcut	ok	No Geolocation information available.
www.a	ok	No Geolocation information available.
sars.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.manifestations	ok	No Geolocation information available.
sregister.s	ok	No Geolocation information available.
g.co	ok	**IP:** 142.250.72.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
scdn-ssettings.s	ok	No Geolocation information available.
www.example.com	ok	**IP:** 23.220.73.43 **Country:** Colombia **Region:** Antioquia **City:** Medellin **Latitude:** 6.251840 **Longitude:** -75.563591 **View:** Google Map
www.googleorganizationautocompleterequirementsconservative	ok	No Geolocation information available.
www.in	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
manage.auth0.com	ok	**IP:** 104.18.39.72 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.language	ok	No Geolocation information available.
scdn-stestsettings.s	ok	No Geolocation information available.
www.recent	ok	No Geolocation information available.
aps-webhandler.appsflyer.com	ok	**IP:** 18.238.109.114 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
developer.apple.com	ok	**IP:** 17.253.83.137 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
sonelink.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
slaunches.s	ok	No Geolocation information available.
ns.adobe.com	ok	No Geolocation information available.
schemas.microsoft.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
svalidate-and-log.s	ok	No Geolocation information available.
sapp.s	ok	No Geolocation information available.
www.icon	ok	No Geolocation information available.
www.c	ok	No Geolocation information available.
sviap.s	ok	No Geolocation information available.
www.style	ok	**IP:** 75.2.38.108 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
.jpg	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
dashif.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
shopify.github.io	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
svalidate.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
www.text-decoration	ok	No Geolocation information available.

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"google_api_key" : "AIzaSyDfAwDQ4mpB4z66zmcm_JNMXiBAo0Uqxvg"
"google_crash_reporting_api_key" : "AIzaSyDfAwDQ4mpB4z66zmcm_JNMXiBAo0Uqxvg"
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
472340246d291854f67ce4b51e48fb0b
44e91f336617a878939030a5de33f923
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed

POSSIBLE SECRETS
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
9a04f079-9840-4286-ab92-e65be0885f95
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
e2719d58-a985-b3c9-781a-b030af78d30e

PLAYSTORE INFORMATION

Title: Soluna: Mental Health Care

Score: 4.5940595 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.kooth.serenity

Developer Details: Kooth, Kooth, None, https://solunaapp.com/, appsupport@kooth.com,

Release Date: Aug 24, 2023 **Privacy Policy:** Privacy link

Description:

Soluna is a free, confidential, mental health app designed to help young people navigate life's challenges. With interactive tools, community features, and access to professional support, Soluna is a space to check in with yourself daily and improve your mental wellness at your own pace. WHO IS THIS FOR? Soluna is available for young people in California, New Jersey, and Illinois thanks to partnerships with your state or insurance provider. Eligibility for services vary by state. • California (ages 13-25): Coaching & Care Navigation • Aetna of Illinois members (ages 13-17): Coaching & Counseling • New Jersey (ages 13-18): Coaching & Counseling WHAT DOES SOLUNA OFFER? In the Soluna universe, some of our most popular tools include: • Mood Log: Record and explore your emotional patterns • Goals: Set and track meaningful goals to map your future • Free Write: Destress and process feelings in your digital journal • Starboard: Draw peacefully when you can't find the words • Breathwork: Steady yourself with easy-to-follow animations Download the app to access the entire Solunaverse, including quizzes, videos, articles, and more! 1:1 PROFESSIONAL SUPPORT & ACCESS TO LOCAL RESOURCES • Gain instant access to a team of mental health professionals • Schedule a chat with a mental health professional or drop in when you need it — you choose • Explore your goals, problems, feelings, and ideas to live your best life • Learn about mental health services and other resources local to your area Check us out on social! Instagram: https://www.instagram.com/soluna.app/ TikTok: https://www.tiktok.com/@soluna.app

SCAN LOGS

Timestamp	Event	Error
2025-08-30 22:46:15	Generating Hashes	OK
2025-08-30 22:46:19	Extracting APK	OK
2025-08-30 22:46:19	Unzipping	OK
2025-08-30 22:46:23	Parsing APK with androguard	OK
2025-08-30 22:46:23	Extracting APK features using aapt/aapt2	OK
2025-08-30 22:46:23	Getting Hardcoded Certificates/Keystores	OK
2025-08-30 22:46:25	Parsing AndroidManifest.xml	OK
2025-08-30 22:46:25	Extracting Manifest Data	OK
2025-08-30 22:46:25	Manifest Analysis Started	OK

2025-08-30 22:46:25	Performing Static Analysis on: Soluna (com.kooth.serenity)	OK
2025-08-30 22:46:28	Fetching Details from Play Store: com.kooth.serenity	OK
2025-08-30 22:46:29	Checking for Malware Permissions	OK
2025-08-30 22:46:29	Fetching icon path	OK
2025-08-30 22:46:29	Library Binary Analysis Started	OK
2025-08-30 22:46:30	Reading Code Signing Certificate	OK
2025-08-30 22:46:31	Running APKiD 2.1.5	OK
2025-08-30 22:46:42	Detecting Trackers	OK
2025-08-30 22:46:46	Decompiling APK to Java with JADX	OK

2025-08-30 23:15:08	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/a245df38b0e2dafd557cc5f2ef231456/java_source', '-q', '-r', '--show-bad-code', '/home/mobsf/.MobSF/uploads/a245df38b0e2dafd557cc5f2ef231456/a245df38b0e2dafd557cc5f2ef231456.apk'], 999.9999705553055)
2025-08-30 23:15:08	Converting DEX to Smali	OK
2025-08-30 23:15:08	Code Analysis Started on - java_source	OK
2025-08-30 23:15:13	Android SBOM Analysis Completed	OK
2025-08-30 23:15:12	Android SAST Completed	OK
2025-08-30 23:15:12	Android API Analysis Started	OK
2025-08-30 23:15:23	Android API Analysis Completed	OK
2025-08-30 23:15:24	Android Permission Mapping Started	OK
2025-08-30 23:15:32	Android Permission Mapping Completed	OK
2025-08-30 23:15:33	Android Behaviour Analysis Started	OK

2025-08-30 23:15:45	Android Behaviour Analysis Completed	OK
2025-08-30 23:15:45	Extracting Emails and URLs from Source Code	OK
2025-08-30 23:15:48	Email and URL Extraction Completed	OK
2025-08-30 23:15:48	Extracting String data from APK	OK
2025-08-30 23:15:48	Extracting String data from Code	OK
2025-08-30 23:15:48	Extracting String values and entropies from Code	OK
2025-08-30 23:15:51	Performing Malware check on extracted domains	OK
2025-08-30 23:15:53	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.