ANDROID STATIC ANALYSIS REPORT

MomiTalk (2.47.0)

File Name:	id.mmtalk.mmtalkv1_1734092433.apk
Package Name:	id.mmtalk.mmtalkv1
Scan Date:	Sept. 1, 2025, 1:46 p.m.
App Security Score:	49/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	5/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	20	4	2	1

FILE INFORMATION

File Name: id.mmtalk.mmtalkv1_1734092433.apk
Size: 49.3MB
MD5: 1c670a5ad5eda5af8150c9afdc94ce52
SHA1: 39013e83342e4a45a674536ea0c9f98081f0273d
SHA256: f9166a703cf023175cf057aae1b97176d8e60838031c48169fa1d0e848a54433

APP INFORMATION

App Name: MomiTalk
Package Name: id.mmtalk.mmtalkv1
Main Activity: com.mmt_global_app.MainActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 2.47.0

Android Version Code: 1734092433

APP COMPONENTS

Activities: 10
Services: 17
Receivers: 19
Providers: 12
Exported Activities: 2
Exported Services: 2
Exported Receivers: 5
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-09-11 10:23:19+00:00
Valid To: 2050-09-11 10:23:19+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x6f7f2facdf6346a804cfbb1d9f3b47ba0855f0bf
Hash Algorithm: sha256
md5: 6973251511099828fb398a69a548a0b3
sha1: 2f10bccb99c1ddbd6c254327eeffd0d8b96aa8ba
sha256: 3bcac0a72153ce44964be6eed9e62687b437f0810ee33745b2ca6416602625f4
sha512: 96ad129a91e2e79415b31a74d06003cddb0f1d5b3b68480ad9dcaa0b471fc64d7d5699181b60841c9d2023f4c5f1846a58c2576c4f61849f899c8c450d6f2cf1
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 7b409c88a2a43a5b7f0409e3c0d23fec4e714ede52bf68b3249174e4ce021f36
Found 1 unique certificates
```

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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_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.NEARBY_WIFI_DEVICES	dangerous	required for advertising and connecting to nearby devices via Wi-Fi.	Required to be able to advertise and connect to nearby devices via Wi-Fi.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
id.mmtalk.mmtalkv1.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BROADCAST_CLOSE_SYSTEM_DIALOGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>1c670a5ad5eda5af8150c9afdc94ce52.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>
<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.HARDWARE check
possible Build.SERIAL check
network operator name 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>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.mmt_global_app.MainActivity	Schemes: @string/url_scheme://, https://, http://, Hosts: @string/universal_domain,
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://, fbconnect://, Hosts: cct.id.mmtalk.mmtalkv1,

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: **2** | WARNING: **9** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	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.
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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	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.
6	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.
7	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.

NO	ISSUE	SEVERITY	DESCRIPTION
8	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.
9	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.
10	Activity (app.notifee.core.NotificationReceiverActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
11	Broadcast Receiver (app.notifee.core.AlarmPermissionBroadcastReceiver) 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.

</> CODE ANALYSIS

HIGH: 0 | WARNING: 10 | INFO: 4 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A/Z.java B3/a.java C9/a.java E5/c.java E9/d.java G2/w0.java G6/a.java I8/c.java K2/d.java L8/c.java M/x.java N0/a.java N3/i.java N3/m.java O/d.java P6/a.java Q6/i.java R0/q.java V6/g.java V7/d.java X6/C0865c.java X6/g.java X6/q.java X6/t.java X6/w.java Y6/P.java ab/a.java app/notifee/core/AlarmPermissionBroadcastReceiver.java app/notifee/core/Logger.java app/notifee/core/RebootBroadcastReceiver.java b7/C1233j.java bb/d.java com/arthenica/ffmpegkit/AbstractC1363b.java com/arthenica/ffmpegkit/FFmpegKitC

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	com/arthenica/ffmpegkit/FFmpegKitConfig.java com/arthenica/ffmpegkit/h.java com/arthenica/ffmpegkit/reactnative/FFmpegKitReactNativeModule.java com/arthenica/ffmpegkit/reactnative/j.java com/arthenica/ffmpegkit/u.java com/dooboolab/rniap/RNIapModule.java com/dooboolab/rniap/d.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/f.java com/microsoft/codepush/react/k.java com/mrousavy/camera/core/AbstractC2268k.java com/mrousavy/camera/core/AbstractC2269l.java com/mrousavy/camera/core/AbstractC2270m.java com/mrousavy/camera/core/AbstractC2272o.java com/mrousavy/camera/core/CameraSession.java com/mrousavy/camera/core/V.java com/mrousavy/camera/core/b0.java com/mrousavy/camera/frameprocessors/FrameProcessorPluginRegistry.java com/mrousavy/camera/frameprocessors/VisionCameraProxy.java com/mrousavy/camera/react/CameraDevicesManager.java com/mrousavy/camera/react/CameraViewModule.java com/mrousavy/camera/react/o.java com/mrousavy/camera/react/r.java com/mrousavy/camera/react/u.java com/mrousavy/camera/react/v.java com/reactnativecommunity/asyncstorage/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/reactnativecommunity/cookies/CookieManagerModule.java com/reactnativemmkv/MmkvModule.java com/rnfs/c.java com/swmansion/gesturehandler/react/i.java com/swmansion/gesturehandler/react/j.java com/swmansion/reanimated/layoutReanimation/AnimationsManager.java d8/i.java e7/C2389a.java f3/C2442j.java i0/C2578b.java i7/p.java io/invertase/firebase/app/a.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingReceiver.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/sentry/U2.java io/sentry/android/core/C2704u.java io/sentry/android/core/z0.java io/sentry/android/replay/u.java io/sentry/android/replay/x.java jb/i.java k2/AbstractC2851a.java k8/C2869d.java lb/b.java m0/f.java org/wonday/orientation/a.java pb/g.java r/C3235a0.java r/C3301w1.java r2/AbstractC3327a.java r3/C3333e.java s2/AbstractC3399M.java sa/AbstractC3435m.java v/t.java v5/D.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				v5/Y.java w3/AbstractC4047a.java x2/i.java y/AbstractC4309f0.java y/U.java
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	O9/a.java Z5/a.java
3	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	C8/b.java E5/a.java io/sentry/util/w.java j4/c.java
4	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	Ma/a.java Ma/b.java Na/a.java Q8/d.java V0/r.java Z0/C0928s0.java b1/C1172b.java n1/d0.java p7/AbstractC3160c.java v5/Y.java
5	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	F5/D.java L3/j.java R3/b.java
6	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	A/A.java C8/c.java G9/h.java V3/a.java ca/d.java com/reactnativecommunity/webview/l.java i2/y.java io/sentry/react/m.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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	K6/M.java K6/U.java T0/c.java T0/d.java V0/f.java V0/k.java com/reactnativecommunity/asyncstorage/k.java n2/C3013c.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
9	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	d8/w.java io/sentry/android/core/internal/util/n.java
10	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	V3/a.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/reactnativecommunity/webview/l.java com/rnfs/RNFSManager.java g4/C2520a.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/sentry/android/core/C2680a0.java v5/Y.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	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	C2/d.java H3/g.java S0/a.java W2/c.java c5/C1320h.java com/amplitude/reactnative/AmplitudeReactNativeModule.java io/invertase/notifee/NotifeeEventSubscriber.java
12	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	F3/C0603e.java N3/m.java o3/C3079g.java
13	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	com/reactnativecommunity/clipboard/ClipboardModule.java
14	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
15	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	e3/c.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00009	Put data in cursor to JSON object	file	com/amplitude/reactnative/b.java com/reactnativecommunity/asyncstorage/a.java v5/Y.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	A/A.java C8/c.java F3/C0605g.java N3/m.java O3/j.java R0/C0756b.java R3/a.java T3/b.java U0/C0846d.java U0/z.java ca/d.java com/airbnb/android/react/lottie/h.java com/microsoft/codepush/react/j.java com/microsoft/codepush/react/n.java com/reactnativecommunity/asyncstorage/h.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/rnfs/RNFSManager.java com/rnfs/i.java i2/y.java io/sentry/C2806x.java io/sentry/S0.java io/sentry/U0.java io/sentry/android/core/SentryPerformanceProvider.java io/sentry/android/replay/g.java io/sentry/cache/b.java io/sentry/cache/c.java io/sentry/cache/e.java io/sentry/config/e.java io/sentry/instrumentation/file/b.java io/sentry/instrumentation/file/h.java io/sentry/util/e.java k2/AbstractC2852b.java o3/C3079g.java o3/C3080h.java okio/Okio__JvmOkioKt.java v5/K.java

			x5/k.java
RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	F5/C0615c.java K2/a.java L2/h.java L2/o.java Y6/C0883i.java Za/n.java app/notifee/core/Notifee.java com/arthenica/ffmpegkit/reactnative/FFmpegKitReactNativeModule.java io/invertase/firebase/dynamiclinks/ReactNativeFirebaseDynamicLinksModule.java r8/C3353g.java v5/C3649b.java v5/M.java v5/Y.java v5/Z.java v5/d0.java
00004	Get filename and put it to JSON object	file collection	B5/a.java O3/f.java x5/c.java
00125	Check if the given file path exist	file	O3/f.java com/reactnativecommunity/cameraroll/CameraRollModule.java
00096	Connect to a URL and set request method	command network	D8/c.java H3/g.java U0/m.java io/sentry/transport/o.java o3/C3074b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	D8/c.java E5/c.java H3/g.java U0/m.java com/microsoft/codepush/react/h.java com/reactnativeimageresizer/a.java com/rnfs/c.java io/sentry/transport/o.java
00030	Connect to the remote server through the given URL	network	U0/m.java com/reactnativeimageresizer/a.java com/rnfs/c.java io/sentry/transport/o.java o3/C3074b.java
00109	Connect to a URL and get the response code	network command	D8/c.java H3/g.java P6/d.java U0/m.java V6/f.java com/rnfs/c.java io/sentry/transport/o.java
00094	Connect to a URL and read data from it	command network	U0/m.java ca/d.java com/reactnativeimageresizer/a.java lb/a.java
00108	Read the input stream from given URL	network command	U0/m.java com/reactnativeimageresizer/a.java
			A/A.java G9/h.java K2/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	K2/e.java K2/f.java Q2/a.java U/Q.java V3/f.java a4/c.java ca/d.java com/arthenica/ffmpegkit/FFmpegKitConfig.java com/microsoft/codepush/react/a.java com/microsoft/codepush/react/j.java com/microsoft/codepush/react/k.java com/microsoft/codepush/react/n.java com/mrousavy/camera/react/v.java com/oblador/vectoricons/VectorIconsModule.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/reactnativeimageresizer/ImageResizerModule.java com/reactnativeimageresizer/a.java com/rnfs/RNFSManager.java f3/AbstractC2454v.java g4/C2520a.java i2/y.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/sentry/AbstractC2774q.java io/sentry/C2769p2.java io/sentry/C2806x.java io/sentry/S0.java io/sentry/U0.java io/sentry/android/core/AbstractC2709z.java io/sentry/android/core/C2680a0.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/instrumentation/file/a.java io/sentry/react/m.java n2/C3014d.java o2/C3072a.java o3/C3079g.java

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	o3/C3080h.java C8/c.java O3/j.java R3/a.java x5/k.java
00012	Read data and put it into a buffer stream	file	F3/C0605g.java N3/m.java com/microsoft/codepush/react/n.java com/rnfs/i.java io/sentry/C2806x.java io/sentry/S0.java io/sentry/cache/b.java io/sentry/cache/e.java io/sentry/config/e.java io/sentry/util/e.java
00003	Put the compressed bitmap data into JSON object	camera	I3/l.java
00189	Get the content of a SMS message	sms	com/arthenica/ffmpegkit/FFmpegKitConfig.java com/imagepicker/k.java com/reactnativecommunity/cameraroll/CameraRollModule.java j4/f.java v5/M.java
00188	Get the address of a SMS message	sms	com/arthenica/ffmpegkit/FFmpegKitConfig.java com/imagepicker/k.java com/reactnativecommunity/cameraroll/CameraRollModule.java j4/f.java v5/M.java
00200	Query data from the contact list	collection contact	com/arthenica/ffmpegkit/FFmpegKitConfig.java com/imagepicker/k.java com/reactnativecommunity/cameraroll/CameraRollModule.java j4/f.java v5/M.java

RULE ID	BEHAVIOUR	LABEL	FILES
00201	Query data from the call log	collection calllog	com/arthenica/ffmpegkit/FFmpegKitConfig.java com/imagepicker/k.java com/reactnativecommunity/cameraroll/CameraRollModule.java j4/f.java v5/M.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/arthenica/ffmpegkit/FFmpegKitConfig.java com/imagepicker/k.java com/reactnativecommunity/cameraroll/CameraRollModule.java v5/M.java
00078	Get the network operator name	collection telephony	com/amplitude/reactnative/a.java com/learnium/RNDeviceInfo/RNDeviceModule.java v5/Y.java
00132	Query The ISO country code	telephony collection	R0/N.java com/amplitude/reactnative/a.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	L2/h.java Y6/C0883i.java Za/n.java app/notifee/core/Notifee.java v5/Y.java v5/Z.java
00115	Get last known location of the device	collection location	com/mrousavy/camera/core/V.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	K2/d.java R0/N.java S3/a.java U0/z.java V2/e.java Y6/C0883i.java Za/o.java app/notifee/core/Notifee.java q6/C3185a.java v5/C3649b.java v5/Y.java v5/Z.java v5/d0.java z3/C4384h.java
00043	Calculate WiFi signal strength	collection wifi	da/e.java
00079	Hide the current app's icon	evasion	D2/p.java
00192	Get messages in the SMS inbox	sms	K2/d.java com/reactnativecommunity/cameraroll/CameraRollModule.java com/rnfs/RNFSManager.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	com/reactnativecommunity/cameraroll/CameraRollModule.java com/rnfs/RNFSManager.java
00028	Read file from assets directory	file	U0/C0843a.java com/rnfs/RNFSManager.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/reactnativecommunity/cameraroll/CameraRollModule.java com/rnfs/RNFSManager.java v5/M.java

RULE ID	BEHAVIOUR	LABEL	FILES
00072	Write HTTP input stream into a file	command network file	com/microsoft/codepush/react/h.java com/reactnativeimageresizer/a.java com/rnfs/c.java
00024	Write file after Base64 decoding	reflection file	K2/e.java K2/f.java com/reactnativeimageresizer/a.java f3/AbstractC2454v.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	Q0/a.java com/reactnativeimageresizer/a.java
00015	Put buffer stream (data) to JSON object	file	v5/Y.java
00191	Get messages in the SMS inbox	sms	com/reactnativecommunity/cameraroll/CameraRollModule.java v5/C3649b.java v5/M.java v5/Y.java
00161	Perform accessibility service action on accessibility node info	accessibility service	v0/C3614A.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	v0/C3614A.java
00121	Create a directory	file command	com/reactnativecommunity/cameraroll/CameraRollModule.java
00187	Query a URI and check the result	collection sms calllog calendar	com/reactnativecommunity/cameraroll/CameraRollModule.java v5/M.java

RULE ID	BEHAVIOUR	LABEL	FILES
00104	Check if the given path is directory	file	com/reactnativecommunity/cameraroll/CameraRollModule.java
00147	Get the time of current location	collection location	com/reactnativecommunity/geolocation/a.java com/reactnativecommunity/geolocation/q.java
00075	Get location of the device	collection location	com/reactnativecommunity/geolocation/a.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00130	Get the current WIFI information	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00134	Get the current WiFi IP address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00082	Get the current WiFi MAC address	collection wifi	com/learnium/RNDeviceInfo/RNDeviceModule.java
00091	Retrieve data from broadcast	collection	F5/I.java v5/M.java
00005	Get absolute path of file and put it to JSON object	file	com/microsoft/codepush/react/k.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/382315722129/namespaces/firebase:fetch?key=AIzaSyDCmIH_KywZHBfQ5GWHtNvw1nfcu1oUee0. This is indicated by the response: The response code is 403

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/25	android.permission.INTERNET, android.permission.CAMERA, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.RECORD_AUDIO, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.VIBRATE
Other Common Permissions	5/44	com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_SERVICE, android.permission.ACCESS_NOTIFICATION_POLICY

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
pinterest.com	ok	**IP:** 151.101.64.84 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
appleid.apple.com	ok	**IP:** 17.111.105.242 **Country:** United States of America **Region:** California **City:** Cupertino **Latitude:** 37.316605 **Longitude:** -122.046486 **View:** Google Map
graph-video.s	ok	No Geolocation information available.
codepush.appcenter.ms	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
plus.google.com	ok	**IP:** 216.58.211.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
.facebook.com	ok	No Geolocation information available.
play.google.com	ok	**IP:** 142.250.74.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
graph.s	ok	No Geolocation information available.
default.url	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
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
twitter.com	ok	**IP:** 172.66.0.227 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
notifee.app	ok	**IP:** 13.52.188.95 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
developers.facebook.com	ok	**IP:** 31.13.70.1 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.250.74.2 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
g.co	ok	**IP:** 172.217.21.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
accounts.google.com	ok	**IP:** 209.85.233.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.apple.com	ok	**IP:** 17.253.83.141 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
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
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
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
aomedia.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
console.firebase.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
shopify.github.io	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	Y6/A.java

TRACKERS

TRACKER	CATEGORIES	URL
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

HARDCODED SECRETS

POSSIBLE SECRETS
"facebook_client_token" : "57f8724e7b5aa48e99f725cb52ae7a2f"
"firebase_pagelink_domain" : "momitalk.page.link"
"google_api_key" : "AIzaSyDCmIH_KywZHBfQ5GWHtNvw1nfcu1oUee0"
"google_crash_reporting_api_key" : "AIzaSyDCmIH_KywZHBfQ5GWHtNvw1nfcu1oUee0"
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a

POSSIBLE SECRETS
115792089237316195423570985008687907853269984665640564039457584007908834671663
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
41058363725152142129326129780047268409114441015993725554835256314039467401291
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
32670510020758816978083085130507043184471273380659243275938904335757337482424
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
ae2044fb577e65ee8bb576ca48a2f06e
c56fb7d591ba6704df047fd98f535372fea00211
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
1093849038073734274511112390766805569936207598951683748994586394495953116150735016013708737573759623248592132296706313309438452531591012912142327488478985984
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643

POSSIBLE SECRETS
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
9a04f079-9840-4286-ab92-e65be0885f95
55066263022277343669578718895168534326250603453777594175500187360389116729240
48439561293906451759052585252797914202762949526041747995844080717082404635286
9b8f518b086098de3d77736f9458a3d2f6f95a37
e2719d58-a985-b3c9-781a-b030af78d30e
3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316
115792089237316195423570985008687907852837564279074904382605163141518161494337
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
115792089210356248762697446949407573530086143415290314195533631308867097853951
2661740802050217063228768716723360960729859168756973147706671368418802944996427808491545080627771902352094241225065558662157113545570916814161637315895999846
cc2751449a350f668590264ed76692694a80308a
5181942b9ebc31ce68dacb56c16fd79f

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
1ddaa4b892e61b0f7010597ddc582ed3
115792089210356248762697446949407573530086143415290314195533631308867097853948
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
83257109614890299855467512895201081792878530488613155947092059024805031998844192244386437603929473330780865116278 71
24b2477514809255df232947ce7928c4
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087
3613425095674979579858512791958788195661110667298501507187719825356841440510 9
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: Momitalk: Pregnancy Ultrasound

Score: 4.93 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** id.mmtalk.mmtalkv1

Developer Details: Humanscape, Inc., Humanscape,+Inc., None, https://humanscape.io/en/index.html, help@humanscape.co.id,

Release Date: Sep 11, 2020 **Privacy Policy:** Privacy link

Description:

Embrace the wonders of motherhood with ease using Momitalk. Share your baby’s first dance and heartbeats with the World (your loved ones), Celebrate your milestones, Find comfort, and Have all your questions answered. AI-empowered all-in-one pregnancy solution (partner) is just at your fingertips. [Peek Inside: Instant Baby Glimpses] Save and Share Baby’s first movement with every heartbeat With Momitalk, access ultrasound videos from your studio or OB clinic anytime, anywhere. No more waiting for appointments—share or relive your baby's first moments with just a click! [From Bump to Birth: Be Informed, Be Empowered] Navigate Pregnancy effortlessly (with ease) With Momitalk, effortlessly traverse your pregnancy journey week-by-week. Uncover your baby's growth, your body's changes, vital prenatal tests, and ways your loved ones can support you. Knowledge is power—Momitalk brings it all to your fingertips! [Always Here: Your 24/7 Pregnancy Pro, Powered by Chat GPT] Late-night worry or daytime curiosity? With Momitalk's AI chat, expert advice is always a tap away. No more waiting for expert advice—get accurate, caring answers to all your queries, big or small, anytime. Your round-the-clock support for every wonder and concern is here!

SCAN LOGS

Timestamp	Event	Error
2025-09-01 13:46:34	Generating Hashes	OK
2025-09-01 13:46:34	Extracting APK	OK
2025-09-01 13:46:34	Unzipping	OK
2025-09-01 13:46:35	Parsing APK with androguard	OK
2025-09-01 13:46:35	Extracting APK features using aapt/aapt2	OK
2025-09-01 13:46:35	Getting Hardcoded Certificates/Keystores	OK

2025-09-01 13:46:38	Parsing AndroidManifest.xml	OK
2025-09-01 13:46:38	Extracting Manifest Data	OK
2025-09-01 13:46:38	Manifest Analysis Started	OK
2025-09-01 13:46:38	Performing Static Analysis on: MomiTalk (id.mmtalk.mmtalkv1)	OK
2025-09-01 13:46:39	Fetching Details from Play Store: id.mmtalk.mmtalkv1	OK
2025-09-01 13:46:41	Checking for Malware Permissions	OK
2025-09-01 13:46:41	Fetching icon path	OK
2025-09-01 13:46:41	Library Binary Analysis Started	OK
2025-09-01 13:46:41	Reading Code Signing Certificate	OK
2025-09-01 13:46:41	Running APKiD 2.1.5	OK

2025-09-01 13:46:46	Detecting Trackers	OK
2025-09-01 13:46:48	Decompiling APK to Java with JADX	OK
2025-09-01 13:47:01	Converting DEX to Smali	OK
2025-09-01 13:47:01	Code Analysis Started on - java_source	OK
2025-09-01 13:47:04	Android SBOM Analysis Completed	OK
2025-09-01 13:47:11	Android SAST Completed	OK
2025-09-01 13:47:11	Android API Analysis Started	OK
2025-09-01 13:47:18	Android API Analysis Completed	OK
2025-09-01 13:47:18	Android Permission Mapping Started	OK
2025-09-01 13:47:23	Android Permission Mapping Completed	OK
2025-09-01 13:47:24	Android Behaviour Analysis Started	OK

2025-09-01 13:47:32	Android Behaviour Analysis Completed	OK
2025-09-01 13:47:32	Extracting Emails and URLs from Source Code	OK
2025-09-01 13:47:35	Email and URL Extraction Completed	OK
2025-09-01 13:47:35	Extracting String data from APK	OK
2025-09-01 13:47:35	Extracting String data from Code	OK
2025-09-01 13:47:35	Extracting String values and entropies from Code	OK
2025-09-01 13:47:38	Performing Malware check on extracted domains	OK
2025-09-01 13:47:40	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.