ANDROID STATIC ANALYSIS REPORT

Modivcare (1.3.33)

File Name:	com.modivcareriderapp_141.apk
Package Name:	com.modivcareriderapp
Scan Date:	Aug. 31, 2025, 6:45 a.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	13	4	1	1

FILE INFORMATION

File Name: com.modivcarerideraapp_141.apk
Size: 25.81MB
MD5: e7c003a39733f3bebd89277a1787e887
SHA1: 0224379af5f416e89e15c9f618b9f3b1fb6f9834
SHA256: 648cce4a25891e397adbca0c7bd6a1a1dd4f43c983856f86868826242d84ff3f

APP INFORMATION

App Name: Modivcare
Package Name: com.modivcareriderapp
Main Activity: com.modivcareriderapp.SplashActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 1.3.33

Android Version Code: 141

APP COMPONENTS

Activities: 11

Services: 11

Receivers: 11

Providers: 5

Exported Activities: 1

Exported Services: 2

Exported Receivers: 1

Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-03-29 18:06:42+00:00
Valid To: 2051-03-29 18:06:42+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x3800ae04d36cdbe7a08e317f9e0cf1319fcf9b5a
Hash Algorithm: sha256
md5: 5c4bffcb4123f0766e2010540e875b71
sha1: c38158f968062ad920dea6303e317b07896ee45d
sha256: b0aa58eb72c3944270501e11700b7644bfc35eaca9965d4e8b4c254b13119a1b
sha512: d55a0d349f9a3d877723099b4617f63ca32fa286fdf36642295a5558415f6dd000d8174a2fa5d05bcec6ff8c7a68bb5daba2eb70a9e0d74c03122d6f7129401b
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 72292aacfc3caf480fa19758156fe1953ec1a57cacf59e5d162be11b9e071b42
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.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
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.modivcareriderapp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>e7c003a39733f3bebd89277a1787e887.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.MANUFACTURER check
possible Build.SERIAL check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></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>Compiler</td><td>r8 without marker (suspicious)</td></tr></table></td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.modivcareriderapp.MainActivity	Schemes: memberapp://,

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: **5** | 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.
2	Activity (com.modivcareriderapp.MainActivity) 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.
3	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.
4	TaskAffinity is set for activity (com.braze.push.NotificationTrampolineActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.

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

CODE ANALYSIS

HIGH: **0** | WARNING: **6** | INFO: **4** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/agontuk/RNFusedLocation/FusedLocationProvider.java com/agontuk/RNFusedLocation/LocationManagerProvider.java

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	anagerProvider.java com/agontuk/RNFusedLocation/RNFusedLocationModule.java com/braze/support/BrazeLogger.java com/horcrux/svg/Brush.java com/horcrux/svg/ClipPathView.java com/horcrux/svg/ImageView.java com/horcrux/svg/LinearGradientView.java com/horcrux/svg/PatternView.java com/horcrux/svg/RadialGradientView.java com/horcrux/svg/UseView.java com/horcrux/svg/VirtualView.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/RNInstallReferrerClient.java com/learnium/RNDeviceInfo/resolver/DeviceIdResolver.java com/lugg/RNCConfig/RNCConfigModule.java com/masteratul/exceptionhandler/DefaultErrorScreen.java com/reactcommunity/rndatetimepicker/MinuteIntervalSnappableTimePickerDialog.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/reactnativecommunity/webview/RNCWebViewManager.java com/rnmaps/maps/FileUtil.java com/rnmaps/maps/MapGradientPolyline.java com/rnmaps/maps/MapModule.java com/rnmaps/maps/MapTileProvider.java com/rnmaps/maps/MapTileWorker.java com/rnmaps/maps/MapUrlTile.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/rnmaps/maps/MapUrlTile.java com/swmansion/gesturehandler/react/RNGestureHandlerModule.java com/swmansion/gesturehandler/react/RNGestureHandlerRootHelper.java com/swmansion/gesturehandler/react/RNGestureHandlerRootView.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/swmansion/rnscreens/ScreensModule.java com/swmansion/rnscreens/SearchBarManager.java com/th3rdwave/safeareacontext/SafeAreaView.java io/invertase/firebase/app/ReactNativeFirebaseApp.java io/invertase/firebase/common/RCTConvertFirebase.java io/invertase/firebase/common/ReactNativeFirebaseEventEmitter.java io/invertase/firebase/common/SharedUtils.java io/invertase/firebase/crashlytics/ReactNativeFirebaseCrashlyticsInitProvider.java io/invertase/firebase/crashlytics/ReactNativeFirebaseCrashlyticsModule.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java org/wonday/orientation/OrientationActivityLifecycle.java org/wonday/orientation/OrientationModule.java
2	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	bo/app/r20.java com/agontuk/RNFusedLocation/FusedLocationProvider.java com/braze/support/IntentUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	bo/app/as.java bo/app/cx.java bo/app/d60.java bo/app/dq.java bo/app/i80.java bo/app/iu.java bo/app/kc0.java bo/app/lq.java bo/app/mq.java bo/app/mt.java bo/app/nf0.java bo/app/om.java bo/app/pc.java bo/app/q.java bo/app/se0.java bo/app/t50.java bo/app/tx.java bo/app/vd0.java bo/app/z30.java com/braze/configuration/RuntimeAppConfigurationProvider.java com/braze/managers/BrazeGeofenceManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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	bo/app/f80.java com/braze/Constants.java com/braze/configuration/BrazeConfig.java com/braze/enums/CardKey.java com/braze/images/DefaultBrazeImageLoader.java com/braze/models/inappmessage/InAppMessageHtml.java com/braze/models/outgoing/AttributionData.java com/braze/push/BrazeNotificationUtils.java com/braze/push/BrazePushReceiver.java com/braze/support/StringUtils.java com/braze/ui/contentcards/ContentCardsFragment.java com/braze/ui/inappmessage/listeners/DefaultInAppMessageWebViewClientListener.java io/invertase/firebase/common/TaskExecutorService.java
5	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java
6	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnativecommunity/webview/RNCWebViewModule.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/reactnativecommunity/webview/RNCWebViewModule.java com/rnmaps/maps/FileUtil.java com/rnmaps/maps/MapModule.java
8	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	com/reactnativecommunity/clipboard/ClipboardModule.java
9	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
10	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/braze/support/StringUtils.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/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00078	Get the network operator name	collection telephony	bo/app/lq.java com/learnium/RNDeviceInfo/RNDeviceModule.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
00043	Calculate WiFi signal strength	collection wifi	com/reactnativecommunity/netinfo/ConnectivityReceiver.java
00016	Get location info of the device and put it to JSON object	location collection	com/braze/models/outgoing/BrazeLocation.java
00022	Open a file from given absolute path of the file	file	bo/app/ea.java bo/app/fa.java bo/app/ko.java bo/app/rb0.java bo/app/ug0.java bo/app/xc.java com/braze/d0.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java com/oblador/vectoricons/VectorIconsModuleImpl.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	bo/app/pa0.java bo/app/sq.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/rnmaps/maps/FileUtil.java com/rnmaps/maps/MapLocalTile.java com/rnmaps/maps/MapTileProvider.java okio/Okio__JvmOkioKt.java
00147	Get the time of current location	collection location	com/agontuk/RNFusedLocation/LocationUtils.java
00036	Get resource file from res/raw directory	reflection	com/braze/push/BrazeNotificationUtils.java com/braze/ui/support/UriUtils.java com/rnmaps/maps/ImageReader.java com/rnmaps/maps/MapMarker.java io/invertase/firebase/common/SharedUtils.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/braze/Braze.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/inappmessage/views/InAppMessageHtmlBaseView.java com/braze/ui/support/UriUtils.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/rnmaps/maps/ImageUtil.java com/rnmaps/maps/MapTileProvider.java
00091	Retrieve data from broadcast	collection	com/braze/push/BrazeNotificationUtils.java com/braze/reactbridge/BrazeReactBridgeImpl.java com/masteratul/exceptionhandler/DefaultErrorScreen.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/260487953805/namespaces/firebase:fetch?key=AIzaSyDwmDss_oA98Q-S2923eNBRdTzBFwqFH8Q. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	android.permission.INTERNET, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	4/44	com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
dust.k8s.test-001.d-usw-2.braze.com	ok	No Geolocation information available.
www.braze.com	ok	**IP:** 104.17.228.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **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
sdk.iad-01.braze.com	ok	**IP:** 172.64.148.188 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sondheim.braze.com	ok	**IP:** 172.64.144.252 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
iamcache.braze	ok	No Geolocation information available.
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

TRACKERS

TRACKER	CATEGORIES	URL
Facebook Flipper	Analytics	https://reports.exodus-privacy.eu.org/trackers/392
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"com_braze_api_key" : "8e52fb75-56e7-4397-9650-d8dbe0a8b3f4"
"com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key"
"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"
"com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key"
"google_api_key" : "AIzaSyDwmDss_oA98Q-S2923eNBRdTzBFwqFH8Q"
"google_crash_reporting_api_key" : "AIzaSyDwmDss_oA98Q-S2923eNBRdTzBFwqFH8Q"
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
c103703e120ae8cc73c9248622f3cd1e
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa
37a6259cc0c1dae299a7866489dff0bd
49f946663a8deb7054212b8adda248c6

PLAYSTORE INFORMATION

Title: Modivcare

Score: 4.5039506 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.modivcareriderapp

Developer Details: Modivcare, Modivcare, None, https://modivcare.com/, ITApplicationSupport@modivcare.com,

Release Date: Aug 4, 2021 **Privacy Policy:** Privacy link

Description:

This app is available to members with participating benefit plans. The Modivcare app is an easy, convenient and accessible way to schedule and manage all of your Modivcare non-emergency transportation needs. No need to call a care center. For eligible members who drive themselves to appointments, they can submit their claims for Mileage Reimbursement. Existing Member Services Website accounts will not work logging in.

SCAN LOGS

Timestamp	Event	Error
2025-08-31 06:45:19	Generating Hashes	OK
2025-08-31 06:45:19	Extracting APK	OK
2025-08-31 06:45:19	Unzipping	OK
2025-08-31 06:45:19	Parsing APK with androguard	OK

2025-08-31 06:45:24	Extracting APK features using aapt/aapt2	OK
2025-08-31 06:46:02	Getting Hardcoded Certificates/Keystores	OK
2025-08-31 06:46:03	Parsing AndroidManifest.xml	OK
2025-08-31 06:46:03	Extracting Manifest Data	OK
2025-08-31 06:46:03	Manifest Analysis Started	OK
2025-08-31 06:46:03	Performing Static Analysis on: Modivcare (com.modivcareriderapp)	OK
2025-08-31 06:46:05	Fetching Details from Play Store: com.modivcareriderapp	OK
2025-08-31 06:46:05	Checking for Malware Permissions	OK
2025-08-31 06:46:05	Fetching icon path	OK
2025-08-31 06:46:05	Library Binary Analysis Started	OK
2025-08-31 06:46:05	Reading Code Signing Certificate	OK

2025-08-31 06:46:06	Running APKiD 2.1.5	OK
2025-08-31 06:46:11	Detecting Trackers	OK
2025-08-31 06:46:14	Decompiling APK to Java with JADX	OK
2025-08-31 07:00:07	Decompiling with JADX failed, attempting on all DEX files	OK
2025-08-31 07:00:07	Decompiling classes2.dex with JADX	OK
2025-08-31 07:00:18	Decompiling classes.dex with JADX	OK
2025-08-31 07:00:23	Decompiling classes3.dex with JADX	OK
2025-08-31 07:00:32	Decompiling classes2.dex with JADX	OK
2025-08-31 07:00:43	Decompiling classes.dex with JADX	OK
2025-08-31 07:00:53	Decompiling classes3.dex with JADX	OK

2025-08-31 07:01:03	Converting DEX to Smali	OK
2025-08-31 07:01:03	Code Analysis Started on - java_source	OK
2025-08-31 07:01:06	Android SBOM Analysis Completed	OK
2025-08-31 07:01:14	Android SAST Completed	OK
2025-08-31 07:01:14	Android API Analysis Started	OK
2025-08-31 07:01:20	Android API Analysis Completed	OK
2025-08-31 07:01:21	Android Permission Mapping Started	OK
2025-08-31 07:01:27	Android Permission Mapping Completed	OK
2025-08-31 07:01:28	Android Behaviour Analysis Started	OK
2025-08-31 07:01:36	Android Behaviour Analysis Completed	OK
2025-08-31 07:01:36	Extracting Emails and URLs from Source Code	OK

2025-08-31 07:01:38	Email and URL Extraction Completed	OK
2025-08-31 07:01:38	Extracting String data from APK	OK
2025-08-31 07:01:38	Extracting String data from Code	OK
2025-08-31 07:01:38	Extracting String values and entropies from Code	OK
2025-08-31 07:01:42	Performing Malware check on extracted domains	OK
2025-08-31 07:01:45	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.