ANDROID STATIC ANALYSIS REPORT

VIA Rail (2.17.0)

File Name:	base.apk
Package Name:	com.viarail.reservia
Scan Date:	Nov. 27, 2025, 8:20 p.m.
App Security Score:	**52/100 (MEDIUM RISK)**
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
2	10	3	2	1

FILE INFORMATION

File Name: base.apk
Size: 39.03MB
MD5: 3dc8baf36052ff31fc11322e82bd6511
SHA1: 665b573c0200c7074840d2836cb8183149fc3dfc
SHA256: 2297c993138e00dc5eb81ef743596dc7fabc5854097369d60178412509fd09b9

APP INFORMATION

App Name: VIA Rail
Package Name: com.viarail.reservia
Main Activity: com.viarail.reservia.MainActivity
Target SDK: 35
Min SDK: 24
Max SDK:
Android Version Name: 2.17.0

Android Version Code: 251030151

APP COMPONENTS

Activities: 4
Services: 5
Receivers: 3
Providers: 6
Exported Activities: 0
Exported Services: 1
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=CA, ST=Quebec, L=Montreal, O=VIA Rail, OU=IT, CN=Via App
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-07-14 14:42:31+00:00
Valid To: 2042-11-29 14:42:31+00:00
Issuer: C=CA, ST=Quebec, L=Montreal, O=VIA Rail, OU=IT, CN=Via App
Serial Number: 0x39e88fec
Hash Algorithm: sha256
md5: 572c1d6a054fd104e93e060ddb88fe1e
sha1: 4f5f02c99c429ea677304f614ebcdfe2cb5d4f08
sha256: 628602cea4376bc21e423cd191ee656910cfe15eeedcfe2b8bf6fe9510c1d8fc
sha512: 3d70cdabcd708b9e4535ff3a7bd50af62b3c9ceb946db1df271a4abbf12599009fece92efff0e175f7465b7bad711431843b832c672ef7bba448087e332f776a
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: ce137aa919ca2c7c7e08b9403f3fe5e99a7b865136ab76af75ac0633c0819de3
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.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.viarail.reservia.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<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</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.TAGS check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
network operator name check
ro.kernel.qemu check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

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: 2 | 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	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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	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: **6** | INFO: **3** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/caverock/androidsvg/CSSParser.java com/caverock/androidsvg/SVG.java com/caverock/androidsvg/SVGAndroidRenderer.java com/caverock/androidsvg/SVGImageView.java com/caverock/androidsvg/SVGParser.java com/caverock/androidsvg/SimpleAssetResolver.java com/henninghall/date_picker/DerivedData.java com/henninghall/date_picker/pickers/AndroidNative.java com/horcrux/svg/Brush.java com/horcrux/svg/ClipPathView.java com/horcrux/svg/FilterView.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/horcrux/svg/ImageView.java com/horcrux/svg/LinearGradientView.java com/horcrux/svg/PatternView.java com/horcrux/svg/RadialGradientView.java com/horcrux/svg/SvgViewManager.java com/horcrux/svg/UseView.java com/horcrux/svg/VirtualView.java com/ibits/react_native_in_app_review/AppReviewModule.java com/lugg/RNCConfig/RNCConfigModule.java com/mapbox/android/gestures/MultiFingerGesture.java com/mapbox/common/AccessTokenInitializer.java com/mapbox/common/BaseMapboxInitializer.java com/mapbox/common/CoreInitializer.java com/mapbox/common/LifecycleMonitorAndroid.java com/mapbox/common/LifecycleService.java com/mapbox/common/LifecycleUtils.java com/mapbox/common/MapboxCommonLogger.java com/mapbox/common/MapboxMapsAndroidLogger.java com/mapbox/common/Reachability.java com/mapbox/common/RunloopErrorHandler.java com/mapbox/common/SettingsServiceHelper.java com/mapbox/common/TelemetrySystemUtils.java com/mapbox/common/ValueUtilsKt.java com/mapbox/common/location/LocationUpdatesReceiver.java com/mapbox/common/logger/MapboxLogger.java com/mapbox/common/module/okhttp/NetworkUsageListener.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/mapbox/common/module/provider/MapboxModuleProvider.java com/mapbox/maps/FontUtils.java com/mapbox/maps/extension/style/atmosphere/generated/Atmosphere.java com/mapbox/maps/extension/style/layers/Layer.java com/mapbox/maps/extension/style/layers/properties/PropertyValue.java com/mapbox/maps/extension/style/precipitations/generated/Rain.java com/mapbox/maps/extension/style/precipitations/generated/Snow.java com/mapbox/maps/extension/style/sources/CustomGeometrySource.java com/mapbox/maps/extension/style/sources/CustomRasterSource.java com/mapbox/maps/extension/style/sources/Source.java com/mapbox/maps/extension/style/sources/generated/GeoJsonSource.java com/mapbox/maps/extension/style/sources/generated/ImageSource.java com/mapbox/maps/extension/style/sources/generated/RasterArraySource.java com/mapbox/maps/extension/style/sources/generated/RasterDemSource.java com/mapbox/maps/extension/style/sources/generated/RasterSource.java com/mapbox/maps/extension/style/sources/generated/VectorSource.java com/mapbox/maps/extension/style/terrain/generated/Terrain.java com/mapbox/maps/extension/style/utils/ColorUtils.java com/mapbox/maps/plugin/locationcomponent/ModelSourceWrapper.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.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	com/reactnativecommunity/asyncstorage/AsyncStorageModule.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/reactnativecommunity/cookies/CookieManagerModule.java com/reactnativecommunity/webview/RNCWebView.java com/reactnativecommunity/webview/RNCWebViewClient.java com/reactnativecommunity/webview/RNCWebViewManagerImpl.java com/rnmapbox/rnmbx/components/mapview/RNMBXLifeCycle.java com/rnmapbox/rnmbx/components/styles/layers/RNMBXLayer.java com/rnmapbox/rnmbx/components/styles/sources/RNMBXImageSource.java com/rnmapbox/rnmbx/events/EventEmitter.java com/rnmapbox/rnmbx/location/LocationManager.java com/rnmapbox/rnmbx/modules/RNMBXLogging.java com/rnmapbox/rnmbx/modules/RNMBXOfflineModule.java com/rnmapbox/rnmbx/modules/RNMBXOfflineModuleLegacy.java com/rnmapbox/rnmbx/modules/RNMBXSnapshotModule.java com/rnmapbox/rnmbx/shapeAnimators/ShapeAnimatorCommon.java com/rnmapbox/rnmbx/utils/BitmapUtils.java com/rnmapbox/rnmbx/utils/ConvertUtils.java com/rnmapbox/rnmbx/utils/DownloadMapImageTask$downloadImage$1$1.java com/rnmapbox/rnmbx/utils/DownloadMapImageTask.java com/rnmapbox/rnmbx/utils/Logger.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/rnmapbox/rnmbx/utils/Logger.java com/swmansion/gesturehandler/react/RNGestureHandlerModule.java com/swmansion/gesturehandler/react/RNGestureHandlerRootHelper.java com/swmansion/gesturehandler/react/RNGestureHandlerRootView.java com/swmansion/reanimated/NativeMethodsHelper.java com/swmansion/reanimated/ReanimatedModule.java com/swmansion/reanimated/ReanimatedUIManagerFactory.java com/swmansion/reanimated/keyboard/WindowsInsetsManager.java com/swmansion/reanimated/layoutReanimation/AnimationsManager.java com/swmansion/reanimated/layoutReanimation/ReanimatedNativeHierarchyManager.java com/swmansion/reanimated/layoutReanimation/ScreensHelper.java com/swmansion/reanimated/layoutReanimation/SharedTransitionManager.java com/swmansion/reanimated/layoutReanimation/TabNavigatorObserver.java com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java com/swmansion/rnscreens/InsetsObserverProxy.java com/swmansion/rnscreens/NativeProxy.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/swmansion/rnscreens/ScreensModule.java com/swmansion/rnscreens/SearchBarManager.java com/swmansion/rnscreens/gamma/helpers/SystemDrawableKt.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				s/SystemDrawableKt.java com/swmansion/rnscreens/gamma/tabs/TabScreenViewManager.java com/swmansion/rnscreens/utils/ScreenDummyLayoutHelper.java com/th3rdwave/safeareacontext/SafeAreaView.java com/zoontek/rnedgetoedge/EdgeToEdgeModuleImpl.java io/invertase/firebase/app/ReactNativeFirebaseApp.java io/invertase/firebase/app/ReactNativeFirebaseAppModule.java io/invertase/firebase/common/RCTConvertFirebase.java io/invertase/firebase/common/ReactNativeFirebaseEventEmitter.java io/invertase/firebase/common/SharedUtils.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/sentry/SystemOutLogger.java io/sentry/android/core/AndroidLogger.java io/sentry/android/core/SentryLogcatAdapter.java io/sentry/android/replay/WindowManagerSpy.java io/sentry/android/replay/WindowSpy.java io/sentry/transport/StdoutTransport.java net/time4j/android/ApplicationStarter.java net/time4j/base/ResourceLoader.java net/time4j/format/expert/ChronoFormatter.java net/time4j/format/expert/CustomizedProcessor.java net/time4j/format/expert/DecimalProcessor.java net/time4j/format/expert/FormatStep.java net/time4j/format/expert/FractionProcessor.java net/time4j/format/expert/IgnorableWhitespaceProcessor.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				aceProcessor.java net/time4j/format/expert/Iso8601Format.java net/time4j/format/expert/LiteralProcessor.java net/time4j/format/expert/LocalizedGMTProcessor.java net/time4j/format/expert/LookupProcessor.java net/time4j/format/expert/MultiFormatParser.java net/time4j/format/expert/NumberProcessor.java net/time4j/format/expert/OrdinalProcessor.java net/time4j/format/expert/SkipProcessor.java net/time4j/format/expert/StyleProcessor.java net/time4j/format/expert/TextProcessor.java net/time4j/format/expert/TimezoneGenericProcessor.java net/time4j/format/expert/TimezoneIDProcessor.java net/time4j/format/expert/TimezoneNameProcessor.java net/time4j/format/expert/TimezoneOffsetProcessor.java net/time4j/format/expert/TwoDigitYearProcessor.java net/time4j/i18n/WeekdataProviderSPI.java net/time4j/tz/spi/ZoneNameProviderSPI.java
				coil3/intercept/EngineInterceptor.java coil3/memory/MemoryCache.java coil3/memory/MemoryCacheService.java coil3/request/ImageRequest.java coil3/request/Options.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	coil3/request/SuccessResult.java coil3/transform/Transformation.java com/mapbox/common/PlatformHttpService.java com/mapbox/common/geofencing/GeofencingPropertiesKeys.java com/mapbox/common/location/LocationUpdatesReceiver.java com/mapbox/maps/ThreadChecker.java com/mapbox/maps/plugin/animation/MapAnimationOwnerRegistry.java com/mapbox/maps/plugin/annotation/generated/CircleAnnotation.java com/mapbox/maps/plugin/annotation/generated/CircleAnnotationOptions.java com/mapbox/maps/plugin/annotation/generated/PointAnnotation.java com/mapbox/maps/plugin/annotation/generated/PointAnnotationOptions.java com/mapbox/maps/plugin/annotation/generated/PolygonAnnotation.java com/mapbox/maps/plugin/annotation/generated/PolygonAnnotationOptions.java com/mapbox/maps/plugin/annotation/generated/PolylineAnnotation.java com/mapbox/maps/plugin/annotation/generated/PolylineAnnotationOptions.java com/mapbox/maps/plugin/locationcomponent/model/AnimatableModel.java com/mapbox/turf/TurfMisc.java com/rnmapbox/rnmbx/components/styles/RNMBXStyleFactory.java com/rnmapbox/rnmbx/modules/RNMBXOfflineModuleKt.java com/swmansion/rnscreens/gamma/tabs/event/TabsHostNativeFocusChangeEvent.java com/viarail/reservia/BuildConfig.java io/invertase/firebase/common/TaskExecutorService.java io/sentry/Baggage.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/sentry/RequestDetailsResolver.java io/sentry/SpanDataConvention.java io/sentry/TraceContext.java io/sentry/protocol/User.java net/time4j/tz/spi/WinZoneProviderSPI.java
3	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	coil3/decode/SourceImageSource.java com/reactnativecommunity/webview/RNCWebViewModuleImpl.java com/rnmapbox/rnmbx/components/mapview/RNMBXMapView.java com/rnmapbox/rnmbx/utils/BitmapUtils.java io/sentry/react/RNSentryModuleImpl.java
4	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/RNCWebViewModuleImpl.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/sentry/android/core/DeviceInfoUtil.java
5	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/DeviceInfoUtil.java io/sentry/android/core/internal/util/RootChecker.java
6	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/reactnativecommunity/webview/RNCWebViewManagerImpl.java
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	com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	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/StringUtils.java
9	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/RootChecker.java
10	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	com/reactnativecommunity/clipboard/ClipboardModule.java
11	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/reactnativecommunity/clipboard/ClipboardModule.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	com/mapbox/maps/plugin/MapAttributionDelegateImpl.java com/rnmapbox/rnmbx/utils/DownloadMapImageTask.java io/invertase/firebase/common/SharedUtils.java io/sentry/react/RNSentryModuleImpl.java
00013	Read file and put it into a stream	file	com/mapbox/common/PlatformStreamFactoryKt.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/PreviousSessionFinalizer.java io/sentry/android/core/SentryPerformanceProvider.java io/sentry/android/replay/ReplayCache.java io/sentry/cache/CacheStrategy.java io/sentry/cache/CacheUtils.java io/sentry/cache/EnvelopeCache.java io/sentry/config/FilesystemPropertiesLoader.java io/sentry/instrumentation/file/FileInputStreamInitData.java io/sentry/instrumentation/file/SentryFileInputStream.java io/sentry/util/FileUtils.java okio/Okio__JvmOkioKt.java
00012	Read data and put it into a buffer stream	file	io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/cache/CacheStrategy.java io/sentry/cache/EnvelopeCache.java io/sentry/config/FilesystemPropertiesLoader.java io/sentry/util/FileUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	coil3/util/FileSystems_androidKt.java com/mapbox/common/CoreInitializer.java com/oblador/vectoricons/VectorIconsModuleImpl.java com/rnmapbox/rnmbx/modules/RNMBXOfflineModule.java com/rnmapbox/rnmbx/modules/RNMBXOfflineModuleLegacy.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/sentry/DirectoryProcessor.java io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/PreviousSessionFinalizer.java io/sentry/SentryOptions.java io/sentry/android/core/AndroidOptionsInitializer.java io/sentry/android/core/DeviceInfoUtil.java io/sentry/android/core/cache/AndroidEnvelopeCache.java io/sentry/android/replay/ReplayCache.java io/sentry/android/replay/capture/BufferCaptureStrategy.java io/sentry/cache/CacheStrategy.java io/sentry/cache/CacheUtils.java io/sentry/cache/EnvelopeCache.java io/sentry/instrumentation/file/FileIOSpanManager.java io/sentry/react/RNSentryModuleImpl.java
00031	Check the list of currently running applications	reflection collection	com/mapbox/common/LifecycleUtils.java
00028	Read file from assets directory	file	com/caverock/androidsvg/SimpleAssetResolver.java
00159	Use accessibility service to perform action getting node info by text	accessibility service	com/henninghall/date_picker/generated/NumberPicker.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/mapbox/maps/plugin/attribution/AttributionDialogManagerImpl.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/mapbox/maps/plugin/attribution/AttributionDialogManagerImpl.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java
00096	Connect to a URL and set request method	command network	io/sentry/transport/HttpConnection.java
00089	Connect to a URL and receive input stream from the server	command network	io/sentry/transport/HttpConnection.java
00030	Connect to the remote server through the given URL	network	io/sentry/transport/HttpConnection.java
00109	Connect to a URL and get the response code	network command	io/sentry/transport/HttpConnection.java
00029	Initialize class object dynamically	reflection	com/mapbox/common/module/provider/MapboxModuleProvider.java
00157	Instantiate new object using reflection, possibly used for dexClassLoader	reflection dexClassLoader	com/mapbox/common/module/provider/MapboxModuleProvider.java
00046	Method reflection	reflection	com/mapbox/common/module/provider/MapboxModuleProvider.java
00026	Method reflection	reflection	com/mapbox/common/module/provider/MapboxModuleProvider.java
00043	Calculate WiFi signal strength	collection wifi	com/reactnativecommunity/netinfo/ConnectivityReceiver.java
00094	Connect to a URL and read data from it	command network	net/time4j/tz/spi/TimezoneRepositoryProviderSPI.java

RULE ID	BEHAVIOUR	LABEL	FILES
00005	Get absolute path of file and put it to JSON object	file	com/rnmapbox/rnmbx/modules/RNMBXOfflineModule.java
00004	Get filename and put it to JSON object	file collection	com/rnmapbox/rnmbx/modules/RNMBXOfflineModule.java
00078	Get the network operator name	collection telephony	com/mapbox/maps/module/telemetry/PhoneState.java
00034	Query the current data network type	collection network	com/mapbox/common/TelemetrySystemUtils.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/108692095942/namespaces/firebase:fetch?key=AIzaSyAGozKNA3_OnNZJyRn-n_2UTs67cGYyS3E. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	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

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	2/44	com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID

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
cloudfront-staging.tilestream.net	ok	**IP:** 13.225.196.126 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.113.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
play.google.com	ok	**IP:** 142.250.69.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.viarail.ca	ok	**IP:** 108.163.144.101 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map
xml.org	ok	**IP:** 104.239.142.8 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api-events-config-staging.tilestream.net	ok	**IP:** 98.89.195.93 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **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
apps.apple.com	ok	**IP:** 23.214.73.104 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **View:** Google Map
apps.mapbox.com	ok	**IP:** 54.192.51.58 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.714272 **Longitude:** -74.005966 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
docs.mapbox.com	ok	**IP:** 13.225.196.78 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map
events.mapbox.com	ok	**IP:** 52.73.46.18 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **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
api-events-staging.tilestream.net	ok	**IP:** 3.229.90.147 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
config.mapbox.com	ok	**IP:** 18.208.47.156 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
o4509479970603008.ingest.de.sentry.io	ok	**IP:** 34.120.62.213 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
api.reservia.viarail.ca	ok	**IP:** 3.162.3.17 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
reservia.viarail.ca	ok	**IP:** 3.161.213.126 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.mapbox.com	ok	**IP:** 199.232.196.143 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
docs.swmansion.com	ok	**IP:** 172.64.80.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
xmlpull.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
api.mapbox.com	ok	**IP:** 3.161.213.58 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

EMAILS

EMAIL	FILE
dd1fecb06b33169509b6@o4509479970603008.ingest	com/viarail/reservia/BuildConfig.java
dd1fecb06b33169509b6@o4509479970603008.ingest	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
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
"API_LOGS_ENABLED" : "false"
"FB_IOS_API_KEY" : "AIzaSyDzMpmai_Joqy2pd2hzjpJYwyKnc-EfeBU"
"google_api_key" : "AIzaSyAGozKNA3_OnNZJyRn-n_2UTs67cGYyS3E"

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyAGozKNA3_OnNZJyRn-n_2UTs67cGYyS3E"
"mapbox_access_token" : "pk.eyJ1IjoidmlhcmFpbCIsImEiOiJjbTAzc2Y0enQwMHk1Mmpvand1ZThpaGtlIn0.RwxNB8FVKOjL0BLZA1ylIg"
eyJ1IjoidmlhcmFpbCIsImEiOiJjbTAzc2Y0enQwMHk1Mmpvand1ZThpaGtlIn0
02d9061db66eed0ef528c7
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
c76b9b6a188d43a09957c13e835bc6a2fe7ac772-
337faf174783e7f0f528c7
108e1963be92dd1fecb06b33169509b6
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A93AD2CAFFFFFFFFFFFFFFFF
23456789abcdefghjkmnpqrstvwxyz

PLAYSTORE INFORMATION

Title: VIA Rail Canada

Score: 2.7741935 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Travel & Local **Play Store URL:** com.viarail.reservia

Developer Details: VIA Rail Canada inc., VIA+Rail+Canada+inc., None, https://www.viarail.ca, application@viarail.ca,

Release Date: Aug 27, 2015 **Privacy Policy:** Privacy link

Description:

Discover the advantages of our newly designed app for a seamless travel journey. Book, travel, and manage your VIA Préférence account—all just a tap away. DAY OF TRAVEL Enjoy a stress-free travel day with all your essential info right on the home screen. ARRIVALS AND DEPARTURES Get real-time status updates on your train and SMS notifications. MANAGE TRIPS Easily adjust your seat selection, add travel options, or modify your itinerary. UPCOMING TRIPS Access everything you need to know about your upcoming journeys in one place. NEW BOOKING Search and book your next adventure effortlessly. TRAIN TRACKER Follow your train’s progress along the route in real time. VIA PRÉFÉRENCE Quickly view your VIA Préférence account and points balance at a glance. DARK MODE Enjoy a visually comfortable experience that reduces eye strain during nighttime use. Happy travels! TERMS, CONDITIONS AND PRIVACY POLICY By downloading the VIA Rail mobile app, you consent to the installation of the application and updates, which can be automatically installed depending on the default settings of your device or operating system, or the settings you selected. You may withdraw your consent at any time by uninstalling this application. By downloading and accessing the app, you confirm that you have read and agree to the terms and conditions of use of the VIA Rail application (https://www.viarail.ca/en/terms-and-conditions-mobile). When you use it, any personal information you provide to VIA Rail will be used and protected in accordance with the requirements of the Privacy Act and VIA Rail's Privacy Policy (https://www.viarail.ca/en/our-privacy-policy). Please contact us with any questions or suggestions you may have concerning our Policy policy: ATIP@viarail.ca Finally, by downloading and accessing the app, you are also accepting the use of cookies. These are designed to improve your user experience on our site and other media by providing you with targeted advertising based on your interests, collecting traffic statistics, information on your behaviour, and facilitating the sharing of information on social networks. See our Cookie Policy (https://www.viarail.ca/en/cookie-policy) to learn more.

SCAN LOGS

Timestamp	Event	Error
2025-11-27 20:20:40	Generating Hashes	OK

2025-11-27 20:20:40	Extracting APK	OK
2025-11-27 20:20:40	Unzipping	OK
2025-11-27 20:20:43	Parsing APK with androguard	OK
2025-11-27 20:20:43	Extracting APK features using aapt/aapt2	OK
2025-11-27 20:20:43	Getting Hardcoded Certificates/Keystores	OK
2025-11-27 20:20:51	Parsing AndroidManifest.xml	OK
2025-11-27 20:20:51	Extracting Manifest Data	OK
2025-11-27 20:20:51	Manifest Analysis Started	OK
2025-11-27 20:20:51	Performing Static Analysis on: VIA Rail (com.viarail.reservia)	OK
2025-11-27 20:20:52	Fetching Details from Play Store: com.viarail.reservia	OK
2025-11-27 20:20:52	Checking for Malware Permissions	OK

2025-11-27 20:20:52	Fetching icon path	OK
2025-11-27 20:20:52	Library Binary Analysis Started	OK
2025-11-27 20:20:52	Reading Code Signing Certificate	OK
2025-11-27 20:20:53	Running APKiD 3.0.0	OK
2025-11-27 20:21:01	Detecting Trackers	OK
2025-11-27 20:21:06	Decompiling APK to Java with JADX	OK
2025-11-27 20:23:00	Converting DEX to Smali	OK
2025-11-27 20:23:00	Code Analysis Started on - java_source	OK
2025-11-27 20:24:37	Android SBOM Analysis Completed	OK
2025-11-27 20:24:47	Android SAST Completed	OK
2025-11-27 20:24:47	Android API Analysis Started	OK

2025-11-27 20:24:57	Android API Analysis Completed	OK
2025-11-27 20:24:58	Android Permission Mapping Started	OK
2025-11-27 20:25:10	Android Permission Mapping Completed	OK
2025-11-27 20:25:13	Android Behaviour Analysis Started	OK
2025-11-27 20:25:24	Android Behaviour Analysis Completed	OK
2025-11-27 20:25:24	Extracting Emails and URLs from Source Code	OK
2025-11-27 20:25:32	Email and URL Extraction Completed	OK
2025-11-27 20:25:32	Extracting String data from APK	OK
2025-11-27 20:25:32	Extracting String data from Code	OK
2025-11-27 20:25:32	Extracting String values and entropies from Code	OK
2025-11-27 20:28:26	Performing Malware check on extracted domains	OK

2025-11-27 20:28:29	Saving to Database	OK

Report Generated by - MobSF v4.4.3

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.