MOBSF

ANDROID STATIC ANALYSIS REPORT

RTC Nomade (2.9.2)

File Name:	base.apk
Package Name:	ca.rtcquebec.nomade
Scan Date:	Nov. 27, 2025, 6:41 p.m.
App Security Score:	**63/100 (LOW RISK)**
Grade:	
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	8	2	3	1

FILE INFORMATION

File Name: base.apk
Size: 38.39MB
MD5: a7a6bd5582ed80970882e6a291c6fbcc
SHA1: 05d2d7b7aeeab6b584129f896ecaba26d81ada70
SHA256: bedd7eb94f8294c6c9b39f77efde8458f27a4cdc507d84679eed500acaa185ba

APP INFORMATION

App Name: RTC Nomade
Package Name: ca.rtcquebec.nomade
Main Activity: ca.rtcquebec.nomade.MainActivity
Target SDK: 35
Min SDK: 24
Max SDK:
Android Version Name: 2.9.2

Android Version Code: 1753388280

APP COMPONENTS

Activities: 4
Services: 7
Receivers: 6
Providers: 3
Exported Activities: 0
Exported Services: 0
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-03-30 20:57:35+00:00
Valid To: 2043-08-16 20:57:35+00:00
Issuer: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Serial Number: 0x42f7f160
Hash Algorithm: sha256
md5: 5e5252b6759ed9ca67534a4c98ce2e40
sha1: 7f8f4951349bfdfbe01d0c39e1ba5b95f9c237d2
sha256: d6d072d46fc1ee744f2b62bcbc65f7b089d3c03c6fee7708e0844b5f3feb0537
sha512: 55b06e59e94ff03801cf12f3dbd60daa49deafb6de32cefda8edffd7bf0c58669db590b1963f989df261e16aeb050454685ca2ac0f826091ed81a68f4eeb4edb
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: b2f9f10fae010eaba1a4a1a2d8ba3ec27b8305546c23ffeb23cf6f4401c7fa46
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
ca.rtcquebec.nomade.permission.PushHandlerActivity	unknown	Unknown permission	Unknown permission from android reference
ca.rtcquebec.nomade.permission.BackgroundHandlerActivity	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
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.
ca.rtcquebec.nomade.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.

PERMISSION	STATUS	INFO	DESCRIPTION
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<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
Build.TAGS check
SIM operator 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 Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.PRODUCT check
possible Build.SERIAL check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT

ACTIVITY	INTENT
ca.rtcquebec.nomade.MainActivity	Schemes: rtcnomade://, ://, Hosts: , Path Prefixes: /,

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: 3 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION

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	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	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.
4	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: 0 | WARNING: 3 | INFO: 1 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				by/chemerisuk/cordova/firebase/FirebaseAnalyticsPlugin.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/adobe/phonegap/push/BackgroundActionButtonHandler.java com/adobe/phonegap/push/BackgroundHandlerActivity.java com/adobe/phonegap/push/FCMService.java com/adobe/phonegap/push/PushDismissedHandler.java com/adobe/phonegap/push/PushHandlerActivity.java com/adobe/phonegap/push/PushPlugin.java com/hutchind/cordova/plugins/launcher/Launcher.java com/plugin/datepicker/DatePickerPlugin.java com/silkimen/cordovahttp/CordovaClientAuth.java com/silkimen/cordovahttp/CordovaHttpBase.java com/silkimen/cordovahttp/CordovaHttpPlugin.java com/silkimen/cordovahttp/CordovaServerTrust.java cordova/plugins/Diagnostic.java cordova/plugins/Diagnostic_Bluetooth.java cordova/plugins/Diagnostic_Camera.java cordova/plugins/Diagnostic_External_Storage.java cordova/plugins/Diagnostic_Location.java cordova/plugins/Diagnostic_NFC.java cordova/plugins/Diagnostic_Notifications.java cordova/plugins/Diagnostic_Wifi.java io/sqlc/SQLiteAndroidDatabase.java io/sqlc/SQLiteConnectorDatabase.ja

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/sqlc/SQLiteConnectorDatabase.java io/sqlc/SQLitePlugin.java me/leolin/shortcutbadger/ShortcutBadger.java
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	com/adobe/phonegap/push/FCMService.java com/adobe/phonegap/push/PushConstants.java
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/silkimen/cordovahttp/CordovaHttpPlugin.java com/silkimen/cordovahttp/CordovaServerTrust.java com/silkimen/http/HttpRequest.java
4	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	io/sqlc/SQLiteAndroidDatabase.java
5	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/plugin/datepicker/DatePickerPlugin.java cordova/plugins/Diagnostic.java
6	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	cordova/plugins/Diagnostic.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libsqlc-ndk-native-driver.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__memset_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	armeabi-v7a/libsqlc-ndk-native-driver.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__memset_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	x86/libsqlc-ndk-native-driver.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__memset_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86_64/libsqlc-ndk-native-driver.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__memset_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64-v8a/libsqlc-ndk-native-driver.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__memset_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	armeabi-v7a/libsqlc-ndk-native-driver.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__memset_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	x86/libsqlc-ndk-native-driver.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__memset_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86_64/libsqlc-ndk-native-driver.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk', '__strlen_chk', '__memset_chk']	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	io/sqlc/SQLiteConnectorDatabase.java io/sqlc/SQLitePlugin.java
00005	Get absolute path of file and put it to JSON object	file	io/sqlc/SQLiteConnectorDatabase.java io/sqlc/SQLitePlugin.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/adobe/phonegap/push/FCMService.java com/hutchind/cordova/plugins/launcher/Launcher.java cordova/plugins/Diagnostic_Notifications.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java
00123	Save the response to JSON after connecting to the remote server	network command	com/adobe/phonegap/push/FCMService.java
00089	Connect to a URL and receive input stream from the server	command network	com/adobe/phonegap/push/FCMService.java com/silkimen/http/HttpRequest.java
00030	Connect to the remote server through the given URL	network	com/adobe/phonegap/push/FCMService.java
00036	Get resource file from res/raw directory	reflection	com/adobe/phonegap/push/FCMService.java com/adobe/phonegap/push/PushPlugin.java cordova/plugins/Diagnostic_Notifications.java me/leolin/shortcutbadger/impl/EverythingMeHomeBadger.java me/leolin/shortcutbadger/impl/HuaweiHomeBadger.java me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	com/silkimen/cordovahttp/CordovaHttpUpload.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00091	Retrieve data from broadcast	collection	com/adobe/phonegap/push/BackgroundActionButtonHandler.java com/adobe/phonegap/push/BackgroundHandlerActivity.java com/adobe/phonegap/push/PushHandlerActivity.java com/hutchind/cordova/plugins/launcher/Launcher.java
00189	Get the content of a SMS message	sms	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00188	Get the address of a SMS message	sms	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00200	Query data from the contact list	collection contact	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00187	Query a URI and check the result	collection sms calllog calendar	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00201	Query data from the call log	collection calllog	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00096	Connect to a URL and set request method	command network	com/silkimen/http/HttpRequest.java
00013	Read file and put it into a stream	file	com/silkimen/http/HttpRequest.java
00072	Write HTTP input stream into a file	command network file	com/silkimen/http/HttpRequest.java

RULE ID	BEHAVIOUR	LABEL	FILES
00012	Read data and put it into a buffer stream	file	com/silkimen/http/HttpRequest.java
00109	Connect to a URL and get the response code	network command	com/silkimen/http/HttpRequest.java
00094	Connect to a URL and read data from it	command network	com/silkimen/http/HttpRequest.java
00108	Read the input stream from given URL	network command	com/silkimen/http/HttpRequest.java
00175	Get notification manager and cancel notifications	notification	com/adobe/phonegap/push/PushPlugin.java
00009	Put data in cursor to JSON object	file	io/sqlc/SQLiteAndroidDatabase.java
00004	Get filename and put it to JSON object	file collection	cordova/plugins/Diagnostic.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/hutchind/cordova/plugins/launcher/Launcher.java cordova/plugins/Diagnostic_Notifications.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://rtc-nomade-1243.firebaseio.com

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/862435004659/namespaces/firebase:fetch?key=AIzaSyB3QSsxJjXv_vnrU1xETmC22sQyAuRaatg. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.WAKE_LOCK, android.permission.VIBRATE
Other Common Permissions	4/44	android.permission.BLUETOOTH, com.google.android.c2dm.permission.RECEIVE, 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
rtc-nomade-1243.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyB3QSsxJjXv_vnrU1xETmC22sQyAuRaatg"
"google_api_key" : "AIzaSyB3QSsxJjXv_vnrU1xETmC22sQyAuRaatg"

POSSIBLE SECRETS
"firebase_database_url" : "https://rtc-nomade-1243.firebaseio.com"
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a

PLAYSTORE INFORMATION

Title: RTC's real-time Nomade

Score: 4.5 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Maps & Navigation **Play Store URL:** ca.rtcquebec.nomade

Developer Details: RTC : Réseau de transport de la Capitale, RTC+:+R%C3%A9seau+de+transport+de+la+Capitale, None, http://www.rtcquebec.ca, nomadecommentaires@rtcquebec.ca,

Release Date: Apr 6, 2016 **Privacy Policy:** Privacy link

Description:

RTC's real-time Nomade lets you plan trips and check real-time or published schedules for all RTC routes. RTC (Réseau de transport de la Capitale) provides public bus transportation for Quebec City and STLévis. • With real-time updates, you'll know exactly how much time is left before your bus arrives at a given stop. • Use your location to see nearby stops and routes. • Find out where buses are and track them in real time. • Set an alert for yourself and know when to leave to catch your bus. • Select trips as your favorites and save your starting or arrival destinations. • Locate our point of sales and Parc-O-Bus on the map. • Be informed of all disruptions in real time. • Locate àVélo stations. • Locate where Flexibus is available.

SCAN LOGS

Timestamp	Event	Error
2025-11-27 18:41:40	Generating Hashes	OK

2025-11-27 18:41:41	Extracting APK	OK
2025-11-27 18:41:41	Unzipping	OK
2025-11-27 18:41:44	Parsing APK with androguard	OK
2025-11-27 18:41:45	Extracting APK features using aapt/aapt2	OK
2025-11-27 18:41:45	Getting Hardcoded Certificates/Keystores	OK
2025-11-27 18:41:54	Parsing AndroidManifest.xml	OK
2025-11-27 18:41:54	Extracting Manifest Data	OK
2025-11-27 18:41:54	Manifest Analysis Started	OK
2025-11-27 18:41:54	Performing Static Analysis on: RTC Nomade (ca.rtcquebec.nomade)	OK
2025-11-27 18:41:56	Fetching Details from Play Store: ca.rtcquebec.nomade	OK

2025-11-27 18:41:56	Checking for Malware Permissions	OK
2025-11-27 18:41:56	Fetching icon path	OK
2025-11-27 18:41:56	Library Binary Analysis Started	OK
2025-11-27 18:41:56	Analyzing apktool_out/lib/arm64-v8a/libsqlc-ndk-native-driver.so	OK
2025-11-27 18:41:56	Analyzing apktool_out/lib/armeabi-v7a/libsqlc-ndk-native-driver.so	OK
2025-11-27 18:41:56	Analyzing apktool_out/lib/x86/libsqlc-ndk-native-driver.so	OK
2025-11-27 18:41:56	Analyzing apktool_out/lib/x86_64/libsqlc-ndk-native-driver.so	OK
2025-11-27 18:41:56	Analyzing lib/arm64-v8a/libsqlc-ndk-native-driver.so	OK
2025-11-27 18:41:56	Analyzing lib/armeabi-v7a/libsqlc-ndk-native-driver.so	OK
2025-11-27 18:41:57	Analyzing lib/x86/libsqlc-ndk-native-driver.so	OK
2025-11-27 18:41:57	Analyzing lib/x86_64/libsqlc-ndk-native-driver.so	OK

2025-11-27 18:41:57	Reading Code Signing Certificate	OK
2025-11-27 18:41:58	Running APKiD 3.0.0	OK
2025-11-27 18:42:03	Detecting Trackers	OK
2025-11-27 18:42:06	Decompiling APK to Java with JADX	OK
2025-11-27 18:43:43	Converting DEX to Smali	OK
2025-11-27 18:43:43	Code Analysis Started on - java_source	OK
2025-11-27 18:44:07	Android SBOM Analysis Completed	OK
2025-11-27 18:44:12	Android SAST Completed	OK
2025-11-27 18:44:12	Android API Analysis Started	OK
2025-11-27 18:44:19	Android API Analysis Completed	OK
2025-11-27 18:44:19	Android Permission Mapping Started	OK

2025-11-27 18:44:26	Android Permission Mapping Completed	OK
2025-11-27 18:44:29	Android Behaviour Analysis Started	OK
2025-11-27 18:44:33	Android Behaviour Analysis Completed	OK
2025-11-27 18:44:33	Extracting Emails and URLs from Source Code	OK
2025-11-27 18:44:34	Email and URL Extraction Completed	OK
2025-11-27 18:44:34	Extracting String data from APK	OK
2025-11-27 18:44:34	Extracting String data from SO	OK
2025-11-27 18:44:34	Extracting String data from Code	OK
2025-11-27 18:44:34	Extracting String values and entropies from Code	OK
2025-11-27 18:46:19	Performing Malware check on extracted domains	OK
2025-11-27 18:46:21	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.