APP SCORES

Security Score **57/100**

Trackers Detection **4/432**

FILE INFORMATION

File Name Chrono-2.18.3-20250317.2.apk

Size 56.98MB

MD5 05b7f2a83a95ea6ce9c37fd725965118

SHA1 779c2353fef3444507becc6854b8b72196b90891

SHA256 bffae3e305d155451e90573ee36ef664928938feeb35ff6df8b04114234ad997

APP INFORMATION

App Name Chrono

Package Name quebec.artm.chrono

Main Activity quebec.artm.chrono.ui.main.MainActivity

Target SDK 35 Min SDK 23 Max SDK

Android Version Name 2.18.3-20250317.2

Android Version Code 218030

PLAYSTORE INFORMATION

Title Chrono - Trips and fares

Score 3.1470587 Installs 500,000+ Price 0 Android Version Support Category Maps & Navigation Play Store URL quebec.artm.chrono

Developer ARTM, Developer ID ARTM

Developer Address None

Developer Website http://www.artm.quebec/application-mobile-chrono/

Developer Email soutien_chrono@artm.quebec

Release Date Aug 28, 2017 Privacy Policy Privacy link

Description

Chrono Mobile is the official application of the transit corporations (exo, REM, RTL, STL and STM). It has been developed to give its users a complete metropolitan experience.

Whether by bike (BIXI), metro, Communauto, river shuttle, bus or train, Chrono lets you buy your fares, find the best route for your next trip or reserve an alternative mode of transportation.

Download the application, create, and personalize your account to benefit from all the features:
-Avoid queues, reload your OPUS card, and buy fares.
-Access information on the entire metropolitan network: real-time* and planned complete schedules, bus and train positions and occupancy levels, network map, etc.
-Reserve your next BIXI, book a Communauto or Communauto Flex
-Plan all your future trips by public transit or bicycle.
-Create favorites and alerts for lines and stops you use often.
-Read the contents of all your cards (OPUS and occasional) and find a new point of sale to buy your tickets.

* When data is available.

1 / 33

EXPORTED ACTIVITIES

View All

1 / 14

EXPORTED SERVICES

View All

5 / 16

EXPORTED RECEIVERS

View All

0 / 5

EXPORTED PROVIDERS

View All

SCAN OPTIONS

DECOMPILED CODE

SIGNER CERTIFICATE

```
Binary is signed
v1 signature: True
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: 2017-08-25 17:55:52+00:00
Valid To: 2047-08-25 17:55:52+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xefd642b5fe110add50f4e4c0f88decd6591d4a07
Hash Algorithm: sha256
md5: 54abcedd5372ed43d6280ebfe0248969
sha1: d6438784876cb07fb204cd5337127d0e46fdc83d
sha256: 72493e539109b6660d660f4297796a2e08e2c6031f3758b6bfce03dfb6df5a27
sha512: 3ecb768ee09ce0296c34825f0ba0685896bc73f4da264b2163d8de8a42940178121e58723dc81e51f5d62511fb9213e356c98cac1499698849d040527c3cd4ad
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: da063d1b1162913920f55018a0cc5b3eca61ff2395dde80ad8df11f14c9f58d9
Found 1 unique certificates
```

APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
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.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
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_TOPICS	normal	allow applications to access advertising service topics	This enables the app to retrieve information related to advertising topics or interests, which can be used for targeted advertising purposes.	
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.	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference	
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.	
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.	
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	

Showing 1 to 10 of 19 entries

Previous 1 2 Next

ANDROID API

Search:

API	FILES
Android Notifications	
Base64 Decode	
Base64 Encode	

API	FILES
Certificate Handling	
Content Provider	
Crypto	
Dynamic Class and Dexloading	
Get Installed Applications	
Get Running App Processes	
Get SIM Provider Details	

Showing 1 to 10 of 28 entries

Previous 1 2 3 Next

BROWSABLE ACTIVITIES

Search:

ACTIVITY	INTENT
quebec.artm.chrono.ui.main.MainActivity	**Schemes**: @string/deeplink_base_uri_scheme_app://, **Hosts:** @string/deeplink_base_uri_host_app, **Paths:** @string/deeplink_base_communauto_auth_path,

Showing 1 to 1 of 1 entries

Previous 1 Next

NETWORK SECURITY

HIGH	WARNING	INFO	SECURE
0	0	0	2

Search:

NO	SCOPE	SEVERITY	DESCRIPTION
1	svcchronomobile.artm.quebec	secure	Domain config is securely configured to disallow clear text traffic to these domains in scope.
2	svcchronomobile.artm.quebec	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: EvXAyvo1QTp1KyaBaZNvd2bXlFnYV8OOqke4fmoR/P8= Digest: SHA-256,Pin: 2GS69UxGIZVXwfCpdsQCpr1Z65FcOIPrVUWm3+WOOqQ= Digest: SHA-256]

Showing 1 to 2 of 2 entries

Previous 1 Next

CERTIFICATE ANALYSIS

HIGH	WARNING	INFO
0	1	1

Search:

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Signed Application	info	Application is signed with a code signing certificate

Showing 1 to 2 of 2 entries

MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
1	7	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable unpatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.	
3	**Broadcast Receiver** (chrono.artm.quebec.core.receivers.ConnectivityReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
4	**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	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
			applications signed with the same certificate can obtain the permission.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
5	**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	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
			signature, only applications signed with the same certificate can obtain the permission.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
6	**Broadcast Receiver** (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. **Permission:** com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
			signature, only applications signed with the same certificate can obtain the permission.	
7	**Activity** (androidx.compose.ui.tooling.PreviewActivity) 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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
8	**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	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
			signature, only applications signed with the same certificate can obtain the permission.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
9	**Broadcast Receiver** (ccm.spirtech.calypsocardmanager.front.nfcDiscoveryWatchers.defaultImpl.NFCReceiver_NormalAndroidNFC) is Protected by a permission, but the protection level of the permission should be checked. **Permission:** android.permission.NFC [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	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
			signature, only applications signed with the same certificate can obtain the permission.	

Showing 1 to 9 of 9 entries

Previous 1 Next

</> CODE ANALYSIS

HIGH	WARNING	INFO	SECURE	SUPPRESSED
1	8	3	2	0

Search:

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
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		
2	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		
3	IP Address disclosure	warning	**CWE:** CWE-200: Information Exposure **OWASP MASVS:** MSTG-CODE-2		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
4	The App uses an insecure Random Number Generator.	warning	**CWE:** CWE-330: Use of Insufficiently Random Values **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-6		
5	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	jh/o8.java mf/t.java wb/c.java	
6	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		
7	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		
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	**OWASP MASVS:** MSTG-NETWORK-4		
9	App can write to App Directory. Sensitive Information should be encrypted.	info	**CWE:** CWE-276: Incorrect Default Permissions **OWASP MASVS:** MSTG-STORAGE-14	jx/b.java oa/a.java	
10	This App may have root detection capabilities.	secure	**OWASP MASVS:** MSTG-RESILIENCE-1	ok/g.java	

Showing 1 to 10 of 14 entries

SHARED LIBRARY BINARY ANALYSIS

Search:

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	S S
1	arm64-v8a/libandroidx.graphics.path.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.	**False** warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	**T** i S s

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	S
2	arm64-v8a/libdatastore_shared_counter.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.	**False** warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	**T** i S s

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	S S
3	arm64-v8a/libimagepipeline.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.	**False** warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	T S s

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	S S
4	arm64-v8a/libnative-filters.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.	**False** warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	T S s

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	S S
5	arm64-v8a/libnative-imagetranscoder.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: ['__vsnprintf_chk', '__strlen_chk', '__memcpy_chk', '__memmove_chk']	T info S s

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	S S
6	arm64-v8a/librealm-jni.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', '__memset_chk', '__memmove_chk', '__strlen_chk', '__strchr_chk', '__vsprintf_chk', '__read_chk', '__vsnprintf_chk', '__FD_SET_chk']	T info S s

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	S S
7	armeabi-v7a/libandroidx.graphics.path.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.	**False** warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	**T** i S s

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	S S
8	armeabi-v7a/libdatastore_shared_counter.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.	**False** warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	T S s

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	S S
9	armeabi-v7a/libimagepipeline.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.	**False** warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	T S s

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	S
10	armeabi-v7a/libnative-filters.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.	**False** warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	T S s

Showing 1 to 10 of 48 entries

NIAP ANALYSIS v1.3

Search:

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
No data available in table				

Showing 0 to 0 of 0 entries

Previous Next

FILE ANALYSIS

Search:

NO	ISSUE	FILES
1	Certificate/Key files hardcoded inside the app.	assets/ds-amex.pem assets/ds-discover.cer assets/ds-mastercard.crt assets/ds-visa.crt

Showing 1 to 1 of 1 entries

Previous 1 Next

FIREBASE DATABASE ANALYSIS

Search:

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://chronoappmobile.firebaseio.com
Firebase Remote Config enabled	warning	The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/613937898427/namespaces/firebase:fetch?key=AIzaSyD3E-Wesn3A399_hSSFDAx1qm2reRRHCWA is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'gtfs_fallback_url': 'https://firebasestorage.googleapis.com/v0/b/chronoappmobile.appspot.com/o/gtfs_v10_22.zip?alt=media&token=c60b5f65-1271-4b33-b4d5-0cdaf927f29c'}, 'state': 'UPDATE', 'templateVersion': '5'}

Showing 1 to 2 of 2 entries

Previous 1 Next

MALWARE LOOKUP

VirusTotal Report | Triage Report | MetaDefender Report | Hybrid Analysis Report

APKiD ANALYSIS

Search:

DEX	DETECTIONS
classes.dex	

Search:

FINDINGS	DETAILS
Anti Debug Code	Debug.isDebuggerConnected() check
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check SIM operator check
Compiler	r8

Showing 1 to 3 of 3 entries

Previous 1 Next

DEX	DETECTIONS
classes2.dex	Search: **FINDINGS** / **DETAILS** Anti Debug Code — Debug.isDebuggerConnected() check Anti-VM Code — Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check possible VM check Compiler — r8 Showing 1 to 3 of 3 entries Previous 1 Next
classes3.dex	Search: **FINDINGS** / **DETAILS** Anti-VM Code — Build.MANUFACTURER check Compiler — r8 Showing 1 to 2 of 2 entries Previous 1 Next

Showing 1 to 3 of 3 entries

BEHAVIOUR ANALYSIS

Search:

RULE ID	BEHAVIOUR	LABEL	FILES
00004	Get filename and put it to JSON object	file collection	bc/g.java y8/b.java
00005	Get absolute path of file and put it to JSON object	file	
00009	Put data in cursor to JSON object	file	af/s.java g8/c.java y7/n0.java
00012	Read data and put it into a buffer stream	file	cc/f.java d6/g.java
00013	Read file and put it into a stream	file	
00014	Read file into a stream and put it into a JSON object	file	
00022	Open a file from given absolute path of the file	file	
00024	Write file after Base64 decoding	reflection file	mb/p.java y8/b.java
00026	Method reflection	reflection	ns/e.java
00030	Connect to the remote server through the given URL	network	

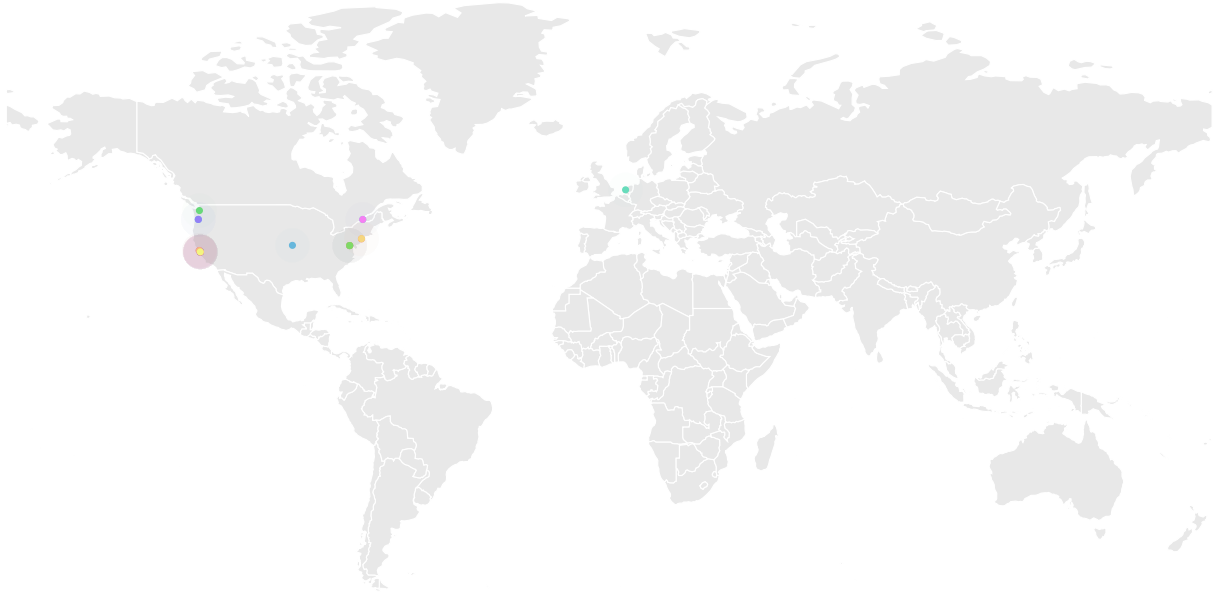
Showing 1 to 10 of 41 entries

ABUSED PERMISSIONS

Top Malware Permissions	8/25	Other Common Permissions	4/44
android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.GET_TASKS, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK		com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	

Malware Permissions are the top permissions that are widely abused by known malware.
Other Common Permissions are permissions that are commonly abused by known malware.

SERVER LOCATIONS



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

Search:

DOMAIN	COUNTRY/REGION
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

DOMAIN MALWARE CHECK

Search:

DOMAIN	STATUS	GEOLOCATION
api.keen.io	ok	**IP:** 35.162.17.146 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
api.stripe.com	ok	**IP:** 34.202.153.183 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
app-measurement.com	ok	**IP:** 142.250.137.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
chronoappmobile.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

DOMAIN	STATUS	GEOLOCATION
console.firebase.google.com	ok	**IP:** 142.250.137.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developer.android.com	ok	**IP:** 192.178.192.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
docs.mongodb.com	ok	**IP:** 3.33.186.135 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
errors.stripe.com	ok	**IP:** 198.202.176.161 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.797550 **Longitude:** -73.946190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
files.stripe.com	ok	**IP:** 3.94.14.82 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.139.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

Showing 1 to 10 of 36 entries

Previous 1 2 3 4 Next

URLS

Search:

URL	FILE
data:image	be/j.java
data:image	hc/d.java
http://%s https://github.com/realm/realm-core/issues/new/choose	apktool_out/lib/arm64-v8a/librealm-jni.so

URL	FILE
http://%s https://github.com/realm/realm-core/issues/new/choose	apktool_out/lib/armeabi-v7a/librealm-jni.so
http://%s https://github.com/realm/realm-core/issues/new/choose	apktool_out/lib/x86/librealm-jni.so
http://%s https://github.com/realm/realm-core/issues/new/choose	apktool_out/lib/x86_64/librealm-jni.so
http://%s https://github.com/realm/realm-core/issues/new/choose	lib/arm64-v8a/librealm-jni.so
http://%s https://github.com/realm/realm-core/issues/new/choose	lib/armeabi-v7a/librealm-jni.so
http://%s https://github.com/realm/realm-core/issues/new/choose	lib/x86/librealm-jni.so
http://%s https://github.com/realm/realm-core/issues/new/choose	lib/x86_64/librealm-jni.so

Showing 1 to 10 of 62 entries

Previous 1 2 3 4 5 6 7 Next

EMAILS

Search:

EMAIL	FILE
support@stripe.com	com/stripe/android/exception/APIConnectionException.java

EMAIL	FILE
support@stripe.com	com/stripe/android/networking/StripeRequest.java

Showing 1 to 2 of 2 entries

Previous 1 Next

TRACKERS

Search:

TRACKER NAME	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Keen	Analytics	https://reports.exodus-privacy.eu.org/trackers/262

Showing 1 to 4 of 4 entries

Previous 1 Next

POSSIBLE HARDCODED SECRETS

▶ Show all **450** secrets

STRINGS

From APK Resource

▶ Show all **3607** strings

From Code

▶ Show all **41542** strings

From Shared Objects

apktool_out/lib/arm64-v8a/libandroidx.graphics.path.so

▶ Show all **19** strings

apktool_out/lib/arm64-v8a/libdatastore_shared_counter.so

▼ Showing all **3** strings
ro.arch
exynos9810
java/io/IOException

apktool_out/lib/arm64-v8a/libimagepipeline.so

▶ Show all **25** strings

apktool_out/lib/arm64-v8a/libnative-filters.so

▶ Show all **45** strings

apktool_out/lib/arm64-v8a/libnative-imagetranscoder.so

▶ Show all **477** strings

apktool_out/lib/arm64-v8a/librealm-jni.so

▶ Show all **9656** strings

apktool_out/lib/armeabi-v7a/libandroidx.graphics.path.so

▶ Show all **19** strings

apktool_out/lib/armeabi-v7a/libdatastore_shared_counter.so

▼ Showing all **1** strings
java/io/IOException

apktool_out/lib/armeabi-v7a/libimagepipeline.so

▶ Show all **25** strings

apktool_out/lib/armeabi-v7a/libnative-filters.so

▶ Show all **45** strings

apktool_out/lib/armeabi-v7a/libnative-imagetranscoder.so

▶ Show all **466** strings

apktool_out/lib/armeabi-v7a/librealm-jni.so

▶ Show all **9581** strings

apktool_out/lib/x86/libandroidx.graphics.path.so

▶ Show all **19** strings

apktool_out/lib/x86/libdatastore_shared_counter.so

▼ Showing all **1** strings
java/io/IOException

apktool_out/lib/x86/libimagepipeline.so

▶ Show all **25** strings

apktool_out/lib/x86/libnative-filters.so

▶ Show all **45** strings

apktool_out/lib/x86/libnative-imagetranscoder.so

▶ Show all **441** strings

apktool_out/lib/x86/librealm-jni.so

▶ Show all **9541** strings

apktool_out/lib/x86_64/libandroidx.graphics.path.so

▶ Show all **19** strings

apktool_out/lib/x86_64/libdatastore_shared_counter.so

▼ Showing all **1** strings
java/io/IOException

apktool_out/lib/x86_64/libimagepipeline.so

▶ Show all **25** strings

apktool_out/lib/x86_64/libnative-filters.so

▶ Show all **45** strings

apktool_out/lib/x86_64/libnative-imagetranscoder.so

▶ Show all **447** strings

apktool_out/lib/x86_64/librealm-jni.so

▶ Show all **9573** strings

lib/arm64-v8a/libandroidx.graphics.path.so

▶ Show all **19** strings

lib/arm64-v8a/libdatastore_shared_counter.so

▼ Showing all **3** strings
ro.arch
exynos9810
java/io/IOException

lib/arm64-v8a/libimagepipeline.so

▶ Show all **25** strings

lib/arm64-v8a/libnative-filters.so

▶ Show all **45** strings

lib/arm64-v8a/libnative-imagetranscoder.so

▶ Show all **477** strings

lib/arm64-v8a/librealm-jni.so

▶ Show all **9656** strings

lib/armeabi-v7a/libandroidx.graphics.path.so

▶ Show all **19** strings

lib/armeabi-v7a/libdatastore_shared_counter.so

▼ Showing all **1** strings
java/io/IOException

lib/armeabi-v7a/libimagepipeline.so

▶ Show all **25** strings

lib/armeabi-v7a/libnative-filters.so

▶ Show all **45** strings

lib/armeabi-v7a/libnative-imagetranscoder.so

▶ Show all **466** strings

lib/armeabi-v7a/librealm-jni.so

▶ Show all **9581** strings

lib/x86/libandroidx.graphics.path.so

▶ Show all **19** strings

lib/x86/libdatastore_shared_counter.so

▼ Showing all **1** strings
java/io/IOException

lib/x86/libimagepipeline.so

▶ Show all **25** strings

lib/x86/libnative-filters.so

▶ Show all **45** strings

lib/x86/libnative-imagetranscoder.so

▶ Show all **441** strings

lib/x86/librealm-jni.so

▶ Show all **9541** strings

lib/x86_64/libandroidx.graphics.path.so

▶ Show all **19** strings

lib/x86_64/libdatastore_shared_counter.so

▼ Showing all **1** strings
java/io/IOException

lib/x86_64/libimagepipeline.so

▶ Show all **25** strings

lib/x86_64/libnative-filters.so

▶ Show all **45** strings

lib/x86_64/libnative-imagetranscoder.so

▶ Show all **447** strings

lib/x86_64/librealm-jni.so

▶ Show all **9573** strings

ACTIVITIES

▼ Showing all **33** activities

quebec.artm.chrono.ui.main.MainActivity
quebec.artm.chrono.ui.account.AccountActivity
quebec.artm.chrono.ui.feed.FeedActivity
quebec.artm.chrono.ui.bookmark.create.BookmarkActivity
quebec.artm.chrono.ui.bookmark.create.CreateBookmarkActivity
quebec.artm.chrono.ui.webview.WebViewActivity
quebec.artm.chrono.ui.webview.CustomUrlWebViewActivity
quebec.artm.chrono.ui.webview.contactus.ContactUsWebViewActivity
quebec.artm.chrono.ui.webview.aboutus.AboutUsWebViewActivity
quebec.artm.chrono.ui.help.HelpActivity
quebec.artm.chrono.ui.settings.SettingActivity
quebec.artm.chrono.ui.salepoints.detail.SalePointDetailActivity
quebec.artm.chrono.ui.communauto.station.accessories.CarAccessoriesActivity
quebec.artm.chrono.ui.communauto.station.characteristics.CommunautoVehicleCharacteristicsActivity
quebec.artm.chrono.ui.search.GenericSearchBarActivity
quebec.artm.chrono.ui.addressonmap.AddressOnMapActivity
quebec.artm.chrono.ticketing.ui.opus.main.OpusActivity
quebec.artm.chrono.ticketing.ui.transitfare.main.TransitFareActivity
com.stripe.android.view.AddPaymentMethodActivity
com.stripe.android.view.PaymentMethodsActivity
com.stripe.android.view.PaymentFlowActivity
com.stripe.android.view.PaymentAuthWebViewActivity
com.stripe.android.view.PaymentRelayActivity
com.stripe.android.view.Stripe3ds2CompletionActivity
com.stripe.android.paymentsheet.PaymentSheetActivity
com.stripe.android.paymentsheet.PaymentOptionsActivity
com.stripe.android.stripe3ds2.views.ChallengeActivity
com.stripe.android.stripe3ds2.views.ChallengeProgressActivity

com.google.android.gms.ads.AdActivity
com.google.android.gms.ads.OutOfContextTestingActivity
com.google.android.gms.ads.NotificationHandlerActivity
com.google.android.gms.common.api.GoogleApiActivity
androidx.compose.ui.tooling.PreviewActivity

SERVICES

▼ Showing all **14** services
quebec.artm.chrono.firebase.ChronoMessagingService
quebec.artm.chrono.widget.WidgetService
com.google.firebase.components.ComponentDiscoveryService
com.google.android.gms.ads.AdService
androidx.work.impl.background.systemalarm.SystemAlarmService
androidx.work.impl.background.systemjob.SystemJobService
androidx.work.impl.foreground.SystemForegroundService
androidx.room.MultiInstanceInvalidationService
com.google.firebase.messaging.FirebaseMessagingService
com.google.firebase.sessions.SessionLifecycleService
com.google.android.datatransport.runtime.backends.TransportBackendDiscovery
com.google.android.gms.measurement.AppMeasurementService
com.google.android.gms.measurement.AppMeasurementJobService
com.google.android.datatransport.runtime.scheduling.jobscheduling.JobInfoSchedulerService

RECEIVERS

▼ Showing all **16** receivers
quebec.artm.chrono.receiver.NotificationReceiver
quebec.artm.chrono.widget.ChronoWidgetProvider
chrono.artm.quebec.core.receivers.ConnectivityReceiver
androidx.work.impl.utils.ForceStopRunnable$BroadcastReceiver
androidx.work.impl.background.systemalarm.ConstraintProxy$BatteryChargingProxy
androidx.work.impl.background.systemalarm.ConstraintProxy$BatteryNotLowProxy

androidx.work.impl.background.systemalarm.ConstraintProxy$StorageNotLowProxy
androidx.work.impl.background.systemalarm.ConstraintProxy$NetworkStateProxy
androidx.work.impl.background.systemalarm.RescheduleReceiver
androidx.work.impl.background.systemalarm.ConstraintProxyUpdateReceiver
androidx.work.impl.diagnostics.DiagnosticsReceiver
com.google.firebase.iid.FirebaseInstanceIdReceiver
com.google.android.gms.measurement.AppMeasurementReceiver
androidx.profileinstaller.ProfileInstallReceiver
com.google.android.datatransport.runtime.scheduling.jobscheduling.AlarmManagerSchedulerBroadcastReceiver
ccm.spirtech.calypsocardmanager.front.nfcDiscoveryWatchers.defaultImpl.NFCReceiver_NormalAndroidNFC

PROVIDERS

▼ Showing all **5** providers
androidx.startup.InitializationProvider
androidx.core.content.FileProvider
com.google.android.gms.ads.MobileAdsInitProvider
com.squareup.picasso.PicassoProvider
com.google.firebase.provider.FirebaseInitProvider

LIBRARIES

▼ Showing all **4** libraries
org.apache.http.legacy
androidx.window.extensions
androidx.window.sidecar
android.ext.adservices

SBOM

▶ Show all **124** Versioned Packages
▶ Show all **1102** Packages

FILES

▶ Show all **2813** files