ANDROID STATIC ANALYSIS REPORT

Chrono (2.18.8-10)

File Name:	base.apk
Package Name:	quebec.artm.chrono
Scan Date:	Nov. 27, 2025, 6:51 p.m.
App Security Score:	**57/100 (MEDIUM RISK)**
Grade:	B
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
2	19	4	4	2

FILE INFORMATION

File Name: base.apk
Size: 25.84MB
MD5: f04a5a66d9fd792edec197b44b0b9e68
SHA1: 24310a4730c118986450eb88ce1f893adf46d5e8
SHA256: 38f2c4be0d107af7c1d2ed5ba6de22ca873ba5d58f5a5db935e9fbbb04a53cd3

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: 2.18.8-10

Android Version Code: 218080

APP COMPONENTS

Activities: 36

Services: 14

Receivers: 16

Providers: 6

Exported Activities: 2

Exported Services: 1

Exported Receivers: 5

Exported Providers: 0

CERTIFICATE INFORMATION

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

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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_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.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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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_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
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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
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.
quebec.artm.chrono.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<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.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
SIM operator check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() 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>Compiler</td><td>dexlib 2.x</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 Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>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</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
net.openid.appauth.RedirectUriReceiverActivity	Schemes: chronoartmquebec://, quebec.artm.chrono://, Hosts: quebec.artm.chrono, Paths: /auth/activation, /auth/logout,
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,

NETWORK SECURITY

HIGH: **0** | WARNING: **0** | INFO: **0** | SECURE: **2**

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]

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **1** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
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.

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **8** | INFO: **0** | SUPPRESSED: **0**

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

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

NO	ISSUE	SEVERITY	DESCRIPTION
7	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.
8	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
9	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

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

CODE ANALYSIS

HIGH: 1 | WARNING: 7 | INFO: 3 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a0/o.java a3/j1.java a6/f.java a8/a0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a8/d0.java a8/n.java a8/u0.java ae/e.java ae/f.java ae/m.java ae/q.java ae/r.java ae/s.java al/e.java am/c1.java am/i0.java am/r.java am/v0.java ax/c.java b3/g1.java b8/s.java b9/b.java bd/c.java bd/d.java bd/g.java bd/l.java bd/o.java be/q.java c8/d.java cm/f.java cm/g.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/c.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/m.java com/bumptech/glide/n.java com/bumptech/glide/p.java com/pairip/licensecheck/LicenseActivity.java com/pairip/licensecheck/LicenseClient.java com/stripe/android/IssuingCardPinService.java com/stripe/android/Logger.java d4/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				d5/b.java d5/d1.java d5/h2.java d5/w.java d6/c.java d6/g.java d8/e.java dd/x.java dd/y.java el/e0.java el/f.java el/f0.java el/g0.java el/h.java el/i.java el/i0.java el/k.java el/k0.java el/l.java el/q.java el/r.java el/s.java el/z.java f6/d.java fg/i.java g7/g.java gd/k.java go/n.java h4/j.java hc/b.java hc/g.java hc/l.java hd/g.java hd/h.java hf/b.java hf/c.java hf/g.java hf/i.java hf/m.java hf/n.java hf/o.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	hf/p.java hf/q.java ho/a.java hr/c.java i7/e0.java i7/v.java ic/e.java ic/g.java j5/u.java j8/e.java j8/i.java jc/c.java jf/e.java jf/f.java jf/w.java jo/u3.java k/a0.java k/j.java k4/l.java k4/p.java kc/c.java kc/d.java kf/a0.java kf/f.java kf/j0.java kf/q0.java kf/x.java kg/a6.java kg/b5.java kg/h8.java kk/a.java kk/d.java kv/j.java lg/a.java lj/a.java lj/b.java lj/c.java m5/h.java mj/d.java mk/q.java ml/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				mi/a.java nc/b.java ng/a.java nj/c.java nj/d.java nq/c.java o1/u2.java o4/c1.java o4/g0.java o4/k.java o4/u0.java o4/w.java o7/k.java of/c.java of/l.java og/a.java oj/b.java on/a.java pc/d.java pe/k.java pj/f.java pj/g.java pj/k.java pj/n.java pj/p.java pj/q.java pj/r.java pj/t.java pj/w.java pj/z.java q3/a.java q3/c.java qc/o.java qc/p.java qc/s0.java qc/w.java qj/i.java qj/n.java quebec/artm/chrono/ui/communauto/flex/detail/FlexCarFragment.java r4/r.java r4/s.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				r4/s.java rc/k.java rc/m.java re/f.java re/i.java rr/s.java s10/i.java s30/j.java s4/k.java s4/l.java s4/m.java s4/p.java s4/q.java s6/g0.java sf/d.java sj/a.java sk/b.java sk/b0.java sk/l.java sm/c.java so/c.java sr/f.java t4/d.java t7/e.java tc/d.java u/h0.java u/z.java uc/b.java uc/e.java uc/f.java uc/o0.java uj/c.java uk/c.java uk/m.java v6/o.java vf/f.java vj/c.java vl/c.java vy/c.java wc/b.java wl/m.java x40/u0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				x40/d0.java xc/b.java xc/b0.java xc/c.java xc/g0.java xc/i.java xc/k.java xc/r0.java xc/v.java xc/x.java yd/a.java yk/f.java z8/b.java
				ba/e.java chrono/artm/quebec/chronoapiclient/data/localDB/entity/DataActionEntity.java chrono/artm/quebec/chronoapiclient/data/rest/response/CommunautoCredentialResponse.java chrono/artm/quebec/chronoapiclient/data/rest/response/ConfigResponse.java chrono/artm/quebec/vehiclesharing/data/model/network/request/LoginBixiResquest.java com/stripe/android/PaymentConfiguration.java com/stripe/android/model/ConfirmSetupIntentParams.java com/stripe/android/model/ConfirmStripeIntentParams.java com/stripe/android/model/PaymentIntent.java com/stripe/android/model/SetupIntent.java com/stripe/android/model/SourceParams.java com/stripe/android/model/Stripe3ds2AuthParams.java com/stripe/android/model/parsers/Ephem

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	eralKeyJsonParser.java com/stripe/android/model/parsers/PaymentIntentJsonParser.java com/stripe/android/model/parsers/SetupIntentJsonParser.java com/stripe/android/model/parsers/SourceJsonParser.java com/stripe/android/networking/AnalyticsDataFactory.java com/stripe/android/networking/ApiRequest.java com/stripe/android/paymentsheet/DefaultPaymentSheetFlowController.java com/stripe/android/paymentsheet/PaymentSheetActivityStarter.java com/stripe/android/view/PaymentAuthWebView.java com/stripe/android/view/Stripe3ds2CompletionActivity.java g/b.java i9/t0.java j8/d.java ko/n.java kz/a.java l1/e7.java o1/n1.java o3/v0.java oc/k.java qc/e.java qc/g0.java qc/p0.java quebec/artm/chrono/ticketing/data/api/model/transitfare/InitResponse.java quebec/artm/chrono/ticketing/data/api/model/transitfare/ProviderKeyResponse.java ry/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	b/a.java od/c.java od/d.java rr/g.java rr/j.java rr/q.java rr/s.java wx/e.java
4	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	el/q.java of/a.java pj/g.java pk/b.java zk/c.java zm/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	ae/f.java iu/f.java iu/o.java j8/n.java jo/b5.java jo/k1.java jo/n1.java jo/r3.java kg/p8.java ko/q.java lu/v.java ne/t.java po/b0.java po/m.java sl/d.java uj/c.java vl/i.java wl/h.java wl/m.java zs/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	as/c.java cs/a.java ct/c.java ct/e.java dt/a.java dt/a1.java dt/b1.java dt/c0.java dt/u.java dt/y0.java dt/z0.java et/l0.java fs/a.java gs/a.java js/a.java ks/a.java ls/a.java ms/a.java os/a.java ps/c.java qs/b.java ru/e.java ss/a.java ts/d.java us/b.java vs/n.java ws/a.java xs/j0.java ys/p.java zs/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	ae/m.java ae/p.java ae/r.java ae/s.java be/q.java be/x.java be/y.java kg/h8.java kg/m.java kg/m6.java kg/s8.java kg/z4.java o7/d.java
8	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	ho/a.java pj/g.java
9	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	nx/b.java ra/a.java
10	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	cc/d.java kg/p8.java ne/t.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	b3/p.java
12	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	nx/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
13	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	cn/a.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	a00/i.java b3/m2.java bw/o.java com/stripe/android/view/PaymentAuthWebView.java com/stripe/android/view/PaymentAuthWebViewActivityViewModel.java h40/c.java hf/l.java j8/i.java jw/h.java kg/h8.java kg/p8.java kk/a.java net/openid/appauth/AuthorizationManagementActivity.java pe/a.java quebec/artm/chrono/ui/webview/WebViewActivity.java r0/p3.java r10/c.java s6/c.java s6/e.java t40/b.java u0/o2.java uk/c.java z8/b.java zw/l.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	a00/i.java h40/c.java j8/i.java kk/a.java net/openid/appauth/AuthorizationManagementActivity.java pe/a.java quebec/artm/chrono/ui/webview/WebViewActivity.java r10/c.java s6/c.java s6/e.java u0/o2.java uk/c.java
00091	Retrieve data from broadcast	collection	com/stripe/android/stripe3ds2/views/ChallengeActivity.java d8/c.java el/l.java el/s.java hf/l.java net/openid/appauth/AuthorizationManagementActivity.java qe/o0.java quebec/artm/chrono/ui/bookmark/create/BookmarkActivity.java quebec/artm/chrono/ui/main/MainActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	b9/b.java cc/e.java com/stripe/android/networking/FileUploadRequest.java d6/g.java el/i.java g7/d.java g7/i.java g7/o.java g7/q.java jc/c.java jc/d.java k8/g.java kr/h.java kr/k.java o4/m.java pj/g.java pj/n.java pk/i.java qe/l.java qj/i.java re/f.java s4/k.java s4/l.java s4/q.java sb/l.java t4/d.java uc/p.java uj/a.java wm/d.java wm/g.java xr/a0.java zr/r1.java
00114	Create a secure socket connection to the proxy address	network command	mr/l.java

RULE ID	BEHAVIOUR	LABEL	FILES
00034	Query the current data network type	collection network	qe/p0.java
00162	Create InetSocketAddress object and connecting to it	socket	rr/e.java rr/s.java
00163	Create new Socket and connecting to it	socket	q8/x.java rr/e.java rr/s.java
00022	Open a file from given absolute path of the file	file	b9/b.java cc/e.java io/realm/e.java io/realm/internal/OsSharedRealm.java io/realm/n0.java io/realm/o0.java j00/g.java nx/b.java qd/b.java qj/i.java sb/l.java sb/o.java uk/m.java wm/d.java
00024	Write file after Base64 decoding	reflection file	b9/b.java sb/o.java
00009	Put data in cursor to JSON object	file	be/q.java go/n.java j8/f.java j8/i.java

RULE ID	BEHAVIOUR	LABEL	FILES
00125	Check if the given file path exist	file	ae/m.java b9/b.java ho/a.java
00014	Read file into a stream and put it into a JSON object	file	b9/b.java cc/e.java qe/l.java qj/i.java re/f.java
00005	Get absolute path of file and put it to JSON object	file	b9/b.java cc/e.java qj/i.java
00121	Create a directory	file command	a8/d0.java b9/b.java
00004	Get filename and put it to JSON object	file collection	a8/d0.java b9/b.java
00089	Connect to a URL and receive input stream from the server	command network	ae/s.java al/e.java com/bumptech/glide/load/data/m.java
00109	Connect to a URL and get the response code	network command	ae/s.java al/e.java com/bumptech/glide/load/data/m.java d8/e.java ic/f.java ke/c.java kg/h5.java pd/a.java re/k.java

RULE ID	BEHAVIOUR	LABEL	FILES
00012	Read data and put it into a buffer stream	file	d6/g.java
00123	Save the response to JSON after connecting to the remote server	network command	er/p.java
00079	Hide the current app's icon	evasion	k8/l.java
00104	Check if the given path is directory	file	b9/b.java
00189	Get the content of a SMS message	sms	sf/d.java
00126	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	sf/d.java
00188	Get the address of a SMS message	sms	sf/d.java
00200	Query data from the contact list	collection contact	sf/d.java
00201	Query data from the call log	collection calllog	sf/d.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	sf/d.java
00096	Connect to a URL and set request method	command network	ae/s.java cc/b.java ic/f.java pd/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	pe/k.java s6/c.java uc/b.java uk/c.java zw/l.java
00147	Get the time of current location	collection location	u/w.java
00075	Get location of the device	collection location	u/w.java
00115	Get last known location of the device	collection location	u/w.java
00112	Get the date of the calendar event	collection calendar	b8/r0.java d40/z.java
00094	Connect to a URL and read data from it	command network	uk/c.java
00108	Read the input stream from given URL	network command	kg/b7.java kg/f5.java
00030	Connect to the remote server through the given URL	network	cc/b.java com/bumptech/glide/load/data/m.java kg/h5.java pd/a.java
00046	Method reflection	reflection	rr/e.java
00026	Method reflection	reflection	rr/e.java
00153	Send binary data over HTTP	http	ic/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00202	Make a phone call	control	h40/c.java
00203	Put a phone number into an intent	control	h40/c.java

FIREBASE DATABASES ANALYSIS

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'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	8/25	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

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	4/44	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:

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
stripe.com	ok	**IP:** 52.54.252.87 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
googlemobileadssdk.page.link	ok	**IP:** 142.250.69.33 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.250.69.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 142.250.69.100 **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

DOMAIN	STATUS	GEOLOCATION
console.firebase.google.com	ok	**IP:** 142.250.69.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
svcchronomobile.artm.quebec	ok	**IP:** 13.107.246.36 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
connexion.chronoapp.quebec	ok	**IP:** 34.36.227.62 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
twitter.com	ok	**IP:** 162.159.140.229 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
errors.stripe.com	ok	**IP:** 198.202.176.41 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.797550 **Longitude:** -73.946190 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.69.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
firebaseinstallations.googleapis.com	ok	**IP:** 142.250.69.74 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app-measurement.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

DOMAIN	STATUS	GEOLOCATION
pagead2.googlesyndication.com	ok	**IP:** 142.250.69.98 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
support.google.com	ok	**IP:** 142.250.69.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
q.stripe.com	ok	**IP:** 54.187.119.242 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.69.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
securityservice.reservauto.net	ok	**IP:** 104.20.43.97 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.googleadservices.com	ok	**IP:** 142.250.69.34 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gle	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
secure.bixi.com	ok	**IP:** 34.198.228.124 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
hooks.stripe.com	ok	**IP:** 50.19.26.15 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
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
files.stripe.com	ok	**IP:** 50.19.26.15 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
chronoappmobile.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebase-settings.crashlytics.com	ok	**IP:** 142.250.69.131 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebaseremoteconfigrealtime.googleapis.com	ok	**IP:** 142.250.69.74 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gl	ok	**IP:** 142.250.69.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.artm.quebec	ok	**IP:** 67.215.10.22 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map
m.stripe.com	ok	**IP:** 52.26.158.133 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
overmind.datatheorem.com	ok	**IP:** 142.250.69.51 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.stripe.com	ok	**IP:** 34.237.253.141 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 142.250.69.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
opus.svd.spiws.net	ok	**IP:** 15.223.49.223 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map

✉ EMAILS

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

TRACKERS

TRACKER	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

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "45f170dce2ce443a8604f66b2aa40d3c"
"communauto_connect_api_authority" : "securityservice.reservauto.net"
"communauto_connect_api_scheme" : "https"
"communauto_connect_api_url" : "https://securityservice.reservauto.net"
"deeplink_base_communauto_auth_path" : "/auth/communauto"
"firebase_database_url" : "https://chronoappmobile.firebaseio.com"
"google_api_key" : "AIzaSyD3E-Wesn3A399_hSSFDAx1qm2reRRHCWA"
"google_crash_reporting_api_key" : "AIzaSyD3E-Wesn3A399_hSSFDAx1qm2reRRHCWA"
"google_maps_api_key" : "AIzaSyABojrPZ5Yi9gpmq3Wn3UfKrLoNO8OeLqs"

POSSIBLE SECRETS
"keen_write_key" : "8DA7CA42469F5E8FC48087D1CA3057C4D14CAE3424AE3E0C4D4F8088A71853649B427A771F99316CD29967E9D20C5E5C58889CF4B1B6C836714714A705C86B83C406FE4880427B6D8A487CF3E569A9BB2657141C22C7D54AEDECB74853D2F102"
6b8cf07d4ca75c88957d9d670591
b8adf1378a6eb73409fa6c9c637ba7f5
01AF286BCA1AF286BCA1AF286BCA1AF286BCA1AF286BC9FB8F6B85C556892C20A7EB964FE7719E74F490758D3B
B4C4EE28CEBC6C2C8AC12952CF37F16AC7EFB6A9F69F4B57FFDA2E4F0DE5ADE038CBC2FFF719D2C18DE0284B8BFEF3B52B8CC7A5F5BF0A3C8D2319A5312557E1
JAIugkcNQRXP51pRzjbhWzeihtmzLSCJCmT0+GTbkts=
1243ae1b4d71613bc9f780a03690e
040369979697AB43897789566789567F787A7876A65400435EDB42EFAFB2989D51FEFCE3C80988F41FF883
D2C0FB15760860DEF1EEF4D696E6768756151754
51DEF1815DB5ED74FCC34C85D709
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E27
a0784d7a4716f3feb4f64e7f4b39bf04
216EE8B189D291A0224984C1E92F1D16BF75CCD825A087A239B276D3167743C52C02D6E7232AA
1E589A8595423412134FAA2DBDEC95C8D8675E58
4E13CA542744D696E67687561517552F279A8C84

POSSIBLE SECRETS
115792089237316195423570985008687907853269984665640564039457584007908834671663
F1FD178C0B3AD58F10126DE8CE42435B53DC67E140D2BF941FFDD459C6D655E1
2866537B676752636A68F56554E12640276B649EF7526267
C8619ED45A62E6212E1160349E2BFA844439FAFC2A3FD1638F9E
03CE10490F6A708FC26DFE8C3D27C4F94E690134D5BFF988D8D28AAEAEDE975936C66BAC536B18AE2DC312CA493117DAA469C640CAF3
MQVwithSHA384KDFAndSharedInfo
77E2B07370EB0F832A6DD5B62DFC88CD06BB84BE
00C9BB9E8927D4D64C377E2AB2856A5B16E3EFB7F61D4316AE
FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551
520883949DFDBC42D3AD198640688A6FE13F41349554B49ACC31DCCD884539816F5EB4AC8FB1F1A6
12511cfe811d0f4e6bc688b4d
68A5E62CA9CE6C1C299803A6C1530B514E182AD8B0042A59CAD29F43
040503213F78CA44883F1A3B8162F188E553CD265F23C1567A16876913B0C2AC245849283601CCDA380F1C9E318D90F95D07E5426FE87E45C0E8184698E45962364E34116177DD2259
1093849038073734274511112390766805569936207598951683748994586394495953116150735016013708737573759623248592132296706313309438452531591012912142327488478985984
B4E134D3FB59EB8BAB57274904664D5AF50388BA

POSSIBLE SECRETS

BDB6F4FE3E8B1D9E0DA8C0D40FC962195DFAE76F56564677
0481AEE4BDD82ED9645A21322E9C4C6A9385ED9F70B5D916C1B43B62EEF4D0098EFF3B1F78E2D0D48D50D1687B93B97D5F7C6D5047406A5E688B352209BCB9F8227DDE385D566332ECC0EABFA9CF7822FDF209F70024A57B1AA000C55B881F8111B2DCDE494A5F485E5BCA4BD88A2763AED1CA2B2FA8F0540678CD1E0F3AD80892
5F49EB26781C0EC6B8909156D98ED435E45FD59918
03375D4CE24FDE434489DE8746E71786015009E66E38A926DD
29818893917731240733471273240314769927240550812383695689146495261604565990247
0021A5C2C8EE9FEB5C4B9A753B7B476B7FD6422EF1F3DD674761FA99D6AC27C8A9A197B272822F6CD57A55AA4F50AE317B13545F
0432C4AE2C1F1981195F9904466A39C9948FE30BBFF2660BE1715A4589334C74C7BC3736A2F4F6779C59BDCEE36B692153D0A9877CC62A474002DF32E52139F0A0
044A96B5688EF573284664698968C38BB913CBFC8223A628553168947D59DCC912042351377AC5FB32
06973B15095675534C7CF7E64A21BD54EF5DD3B8A0326AA936ECE454D2C
00689918DBEC7E5A0DD6DFC0AA55C7
0401F481BC5F0FF84A74AD6CDF6FDEF4BF6179625372D8C0C5E10025E399F2903712CCF3EA9E3A1AD17FB0B3201B6AF7CE1B05
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
00FDFB49BFE6C3A89FACADAA7A1E5BBC7CC1C2E5D831478814

POSSIBLE SECRETS
0051953EB9618E1C9A1F929A21A0B68540EEA2DA725B99B315F3B8B489918EF109E156193951EC7E937B1652C0BD3BB1BF073573DF883D2C34F1EF451FD46B503F00
0307AF69989546103D79329FCC3D74880F33BBE803CB
SHfJbyMgI7MrHewwYoTmYsM7CTkziBSZ0pvzhPCRWcLGoNw6AaEZWLqlKa0dpKuD
4105836372515214212932612978004726840911444101599372555483525631403946740129 1
60dcd2104c4cbc0be6eeefc2bdd610739ec34e317f9b33046c9e4788
0101BAF95C9723C57B6C21DA2EFF2D5ED588BDD5717E212F9D
af60eb711bd85bc1e4d3e0a462e074eea428a8
79885141663410976897627118935756323747307951916507639758300472692338873533959
c469684435deb378c4b65ca9591e2a5763059a2e
0370F6E9D04D289C4E89913CE3530BFDE903977D42B146D539BF1BDE4E9C92
91E38443A5E82C0D880923425712B2BB658B9196932E02C78B2582FE742DAA28
036b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
0405F939258DB7DD90E1934F8C70B0DFEC2EED25B8557EAC9C80E2E198F8CDBECD86B1205303676854FE24141CB98FE6D4B20D02B4516FF702350EDDB0826779C813F0DF45BE8112F4
70390085352083305199547718019018437841079516630045180471284346843705633502616
469A28EF7C28CCA3DC721D044F4496BCCA7EF4146FBF25C9

POSSIBLE SECRETS

8d5155894229d5e689ee01e6018a237e2cae64cd
64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1
3086d221a7d46bcde86c90e49284eb153dab
1A827EF00DD6FC0E234CAF046C6A5D8A85395B236CC4AD2CF32A0CADBDC9DDF620B0EB9906D0957F6C6FEACD615468DF104DE296CD8F
ZdMwT5n8r4APV4u4GhQlb1VCwOIVHkTm7kF7LnArEpyZnsv+C3G3q6fVFgtTcqcc
TvLSh+Eka5RyCXMK4IvAvP4vfksx/KqJwxjzSKu7qQs=
D7C134AA264366862A18302575D0FB98D116BC4B6DDEBCA3A5A7939F
678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4
Kx8fghNUQq+sA+EfmK6qh0KjuKvw753ECuaCFV8szVM=
55066263022277343669578718895168534326250603453777594175500187360389116729240
96341f1138933bc2f503fd44
E95E4A5F737059DC60DF5991D45029409E60FC09
57896044618658097711785492504343953927102133160255826820068844496087732066703
0400D9B67D192E0367C803F39E1A7E82CA14A651350AAE617E8F01CE94335607C304AC29E7DEFBD9CA01F596F927224CDECF6C

POSSIBLE SECRETS
B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF
6EE3CEEB230811759F20518A0930F1A4315A827DAC
04009D73616F35F4AB1407D73562C10F00A52830277958EE84D1315ED31886
ffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632551
36DF0AAFD8B8D7597CA10520D04B
255705fa2a306654b1f4cb03d6a750a30c250102d4988717d9ba15ab6d3e
42debb9da5b3d88cc956e08787ec3f3a09bba5f48b889a74aaf53174aa0fbe7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76137e792f3f0db859d095e4a5b932024f079ecf2ef09c797452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94cccf1449ac43d586d0beee43251b0b2287349d68de0d144403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1b27d0639f695e347d8d1cf9ac819a26ca9b04cb0eb9b7b035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffbc97134025fe8ce04c4399ad96569be91a546f4978693c7a
77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399
SKSJAjN3UKeguXyEasCGg04d/yJuUN8XZYgactMp4rfMtHcIJcD0mydl5RKvI49M
686479766013060971498190079908139321726943530014330540939446345918554318339765539424505774633321719753296399637136332111386476861244038034037280892707005449
43FC8AD242B0B7A6F3D1627AD5654447556B47BF6AA4A64B0C2AFE42CADAB8F93D92394C79A79755437B56995136
b68a437c18bb30db25f4cad4e5ead737
0101D556572AABAC800101D556572AABAC8001022D5C91DD173F8FB561DA6899164443051D
6127C24C05F38A0AAAF65C0EF02C

POSSIBLE SECRETS
0238af09d98727705120c921bb5e9e26296a3cdcf2f35757a0eafd87b830e7
E2E31EDFC23DE7BDEBE241CE593EF5DE2295B7A9CBAEF021D385F7074CEA043AA27272A7AE602BF2A7B9033DB9ED3610C6FB85487EAE97AAC5BC7928C1950148
3045AE6FC8422f64ED579528D38120EAE12196D5
790408F2EEDAF392B012EDEFB3392F30F4327C0CA3F31FC383C422AA8C16
0479BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8
94DC014C1D00112233445566778899001122334455667788990011223344556677 88
WfvM4SeNDVyFarUKUVpVTE2MRQkjnaN4GpgwC5lMrmyQkCennlTSSkgCAZvzOVXK
4A6E0856526436F2F88DD07A341E32D04184572BEB710
3071c8717539de5d5353f4c8cd59a032
deca87e736574c5c83c07314051fd93a
038D16C2866798B600F9F08BB4A8E860F3298CE04A5798
262470350957996892686231567445669818918529234911092133878156159009255188547380500890223880539757197866508724767 32087
6b8cf07d4ca75c88957d9d67059037a4
64033881142927202683649881450433473985931760268884941288852745803908878638612
K/sgHSTVeE1LLZ4HP+m5KF6ND+k7W4ID3M3VTul8bAI=

POSSIBLE SECRETS
3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784
O+vmm8flr2e7ZrTWUx/T8ClWwcEwLlJlfjM8sMGjZbg=
28091019353058090096996979000309560759124368558014865957655842872397301267595
5FF6108462A2DC8210AB403925E638A19C1455D21
Kq6mcF8LH4HqXGyg5/DR3VvLtDExNTPXoCRIPhkdOGM=
85E25BFE5C86226CDB12016F7553F9D0E693A268
10C0FB15760860DEF1EEF4D696E676875615175D
D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E24
e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf
g3h/WBQ8k1SqFyNwcX6aXlyabMyZPKS0QgL4qcVfix1XI+70++CdiHkDZKRlUPQw
dcb428fea25c40e7b99f81ae5981ee6a
QcEEfK1PwFv2Eb+NZQ+4kWKAUUVvycYqoBzmAjBexJV/sKEjaFlajeD5MAZYWXy5
d7YRusR2mxxBt1bBYjK2gXVvJl/MfqFw2IiZZVeFOFqksQBErGXLOKgf56kYtWpK
vvYcBqgI4aoC3GZZ7n1bdLp71k52s6EJLh0/nA6ME39LmvOZf3TBZ+H4xg1YfQXg

POSSIBLE SECRETS

5037EA654196CFF0CD82B2C14A2FCF2E3FF8775285B545722F03EACDB74B
C302F41D932A36CDA7A3462F9E9E916B5BE8F1029AC4ACC1
e8b4011604095303ca3b8099982be09fcb9ae616
36134250956749795798585127919587881956611106672985015071877198253568414405109
4230017757A767FAE42398569B746325D45313AF0766266479B75654E65F
1854BEBDC31B21B7AEFC80AB0ECD10D5B1B3308E6DBF11C1
985BD3ADBAD4D696E676875615175A21B43A97E3
9760508f15230bccb292b982a2eb840bf0581cf5
0202F9F87B7C574D0BDECF8A22E6524775F98CDEBDCB
1C97BEFC54BD7A8B65ACF89F81D4D4ADC565FA45
714114B762F2FF4A7912A6D2AC58B9B5C2FCFE76DAEB7129
MQVwithSHA512KDFAndSharedInfo
E8C2505DEDFC86DDC1BD0B2B6667F1DA34B82574761CB0E879BD081CFD0B6265EE3CB090F30D27614CB4574010DA90DD862EF9D4EBEE4761503190785A71C760
64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1

POSSIBLE SECRETS
bae8e37fc83441b16034566b
00F50B028E4D696E676875615175290472783FB1
000E0D4D696E6768756151750CC03A4473D03679
7ae96a2b657c07106e64479eac3434e99cf0497512f58995c1396c28719501ee
0340340340340340340340340340340340340340340340340340340323C313FAB50589703B5EC68D3587FEC60D161CC149C1AD4A91
07B6882CAAEFA84F9554FF8428BD88E246D2782AE2
F5CE40D95B5EB899ABBCCFF5911CB8577939804D6527378B8C108C3D2090FF9BE18E2D33E3021ED2EF32D85822423B6304F726AA854BAE07D0396E9A9ADDC40F
D35E472036BC4FB7E13C785ED201E065F98FCFA5B68F12A32D482EC7EE8658E98691555B44C59311
A7F561E038EB1ED560B3D147DB782013064C19F27ED27C6780AAF77FB8A547CEB5B4FEF422340353
KvkOAolI09ZSAixqGUOtipMDBdKXVlslzVnQOpfDZOEJW+xbFKrK173Gu3h1RVkI
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B31F166E6CAC0425A7CF3AB6AF6B7FC3103B883202E9046565
c49d360886e704936a6678e1139d26b7819f7e90
DB7C2ABF62E35E7628DFAC6561C5
048BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F046997
115792089210356248762697446949407573530086143415290314195533631308867097853948

POSSIBLE SECRETS

E95E4A5F737059DC60DFC7AD95B3D8139515620C
F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C03
0713612DCDDCB40AAB946BDA29CA91F73AF958AFD9
027B680AC8B8596DA5A4AF8A19A0303FCA97FD7645309FA2A581485AF6263E313B79A2F5
02A29EF207D0E9B6C55CD260B306C7E007AC491CA1B10C62334A9E8DCD8D20FB7
115792089237316195423570985008687907853269984665640564039457584007913129639319
9ObkV+9nuY0gPBNLH25GoxM7YATuF1pi7IORvVFb3+Q=
07A11B09A76B562144418FF3FF8C2570B8
D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FF
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F0
91A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C40094DBACDB586FB20
0228F9D04E900069C8DC47A08534FE76D2B900B7D7EF31F5709F200C4CA205
0163F35A5137C2CE3EA6ED8667190B0BC43ECD69977702709B
LYoHKR17UvbUNibqKPKJklawQJNaw1zk7CnhZAC68YBTzC7x4MYQVXp9Sihs98Ok

POSSIBLE SECRETS
A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377
9ba48cba5ebcb9b6bd33b92830b2a2e0e192f10a
avDZD6/xoSbFYvWCy23XLncB75oD5DxKdrTKFY2O0hY=
l4qa5EABhdRHJHltXD4U8dy0wNZl4oyoZ9TbFONnMI4=
5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B
7830A3318B603B89E2327145AC234CC594CBDD8D3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CA
0452DCB034293A117E1F4FF11B30F7199D3144CE6DFEAFFEF2E331F296E071FA0DF9982CFEA7D43F2E
68363196144955700784444165611827252895102170888761442055095051287550314083023
659EF8BA043916EEDE8911702B22
f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a
1AB597A5B4477F59E39539007C7F977D1A567B92B043A49C6B61984C3FE3481AAF454CD41BA1F051626442B3C10
NtWyZSC7qBNyKPaXbOjRpNaZGUUAwpDpvYkB4v1ZH9M=
7d7374168ffe3471b60a857686a19475d3bfa2ff
74D59FF07F6B413D0EA14B344B20A2DB049B50C3
5HcA415u1KU8m2yVlDZBhQQK+0IFNRmmWPxuAq0DnfPzSdJ/uWlnYMD1kKfkH6cZ

POSSIBLE SECRETS

42941826148615804143873447737955502392672345968607143066798112994089471231420027060385216699563848719957657284814898909770759462613437669456364882730370838934791080835932647976778601915343474400961034231316672578686920482194932878633360203384797092684342247621055760235016132614780652761028509445403338652341
7167EFC92BB2E3CE7C8AAAFF34E12A9C557003D7C73A6FAF003F99F6CC8482E540F7
02120FC05D3C67A99DE161D2F4092622FECA701BE4F50F4758714E8A87BBF2A658EF8C21E7C5EFE965361F6C2999C0C247B0DBD70CE6B7
470fa2b4ae81cd56ecbcda9735803434cec591fa
10B7B4D696E676875615175137C8A16FD0DA2211
115792089210356248762697446949407573529996955224135760342422259061068512044369
24B7B137C8A14D696E6768756151756FD0DA2E5C
7B425ED097B425ED097B425ED097B425ED097B425ED097B4260B5E9C7710C864
046B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C2964FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5
026108BABB2CEEBCF787058A056CBE0CFE622D7723A289E08A07AE13EF0D10D171DD8D
0403F0EBA16286A2D57EA0991168D4994637E8343E3600D51FBC6C71A0094FA2CDD545B11C5C0C797324F1
00C9517D06D5240D3CFF38C74B20B6CD4D6F9DD4D9
4D41A619BCC6EADF0448FA22FAD567A9181D37389CA

POSSIBLE SECRETS
db92371d2126e9700324977504e8c90e
83257109614890299855467512895201081792878530488613155947092059024805031998844192244386437603929473330780865116278 71
E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B
044AD5F7048DE709AD51236DE65E4D4B482C836DC6E410664002BB3A02D4AAADACAE24817A4CA3A1B014B5270432DB27D2
eUrWQVF8FAlcOLX3Auj55rxdEWjF+0P5JAPLCHVKKQw=
32879423AB1A0375895786C4BB46E9565FDE0B5344766740AF268ADB32322E5C
003088250CA6E7C7FE649CE85820F7
tnRfJM39LV6MDlXml8e8fAfi5JhKcsRyFSmagsP97rbE/0XgA5fRVLlLbAYUcu57
962eddcc369cba8ebb260ee6b6a126d9346e38c5
bFK3lRg0oaTUwYDrSsMiLa/j4LG9nRlI5KKEyt63x08=
1053CDE42C14D696E67687561517533BF3F83345
040D9029AD2C7E5CF4340823B2A87DC68C9E4CE3174C1E6EFDEE12C07D58AA56F772C0726F24C6B89E4ECDAC24354B9E99CAA3F6D3761402CD
D6031998D1B3BBFEBF59CC9BBFF9AEE1
7fffffffffffffffffffffff800000cfa7e8594377d414c03821bc582063
t+CAjrsoEFEWDgC/oCfdqxFl31lIReQPqb6CaFb+1Y0=

POSSIBLE SECRETS
fHaUCxrr3fcbpdQPVJw6OSoHeHoizr6wmxmAsnLvDUhuNG2u8ebKX4VPxAoXSx4W
3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CADC083E67984050B75EBAE5DD2809BD638016F723
036768ae8e18bb92cfcf005c949aa2c6d94853d0e660bbf854b1c9505fe95a
6db14acc9e21c820ff28b1d5ef5de2b0
044BA30AB5E892B4E1649DD0928643ADCD46F5882E3747DEF36E956E97
040303001D34B856296C16C0D40D3CD7750A93D1D2955FA80AA5F40FC8DB7B2ABDBDE53950F4C0D293CDD711A35B67FB1499AE60038614F1394ABFA3B4C850D927E1E7769C8EEC2D19037BF27342DA639B6DCCFFFEB73D69D78C6C27A6009CBBCA1980F8533921E8A684423E43BAB08A576291AF8F461BB2A8B3531D2F0485C19B16E2F1516E23DD3C1A4827AF1B8AC15B
iz9pI8M74OdFMOjBXhk6CVKK/c29GtinDT3TfbuphLdYOSnoV+Rg8WuW9whaa7rD
295F9BAE7428ED9CCC20E7C359A9D41A22FCCD9108E17BF7BA9337A6F8AE9513
7CBBBCF9441CFAB76E1890E46884EAE321F70C0BCB4981527897504BEC3E36A62BCDFA2304976540F6450085F2DAE145C22553B465763689180EA2571867423E
108576C80499DB2FC16EDDF6853BBB278F6B6FB437D9
517cc1b727220a94fe13abe8fa9a6ee0
662C61C430D84EA4FE66A7733D0B76B7BF93EBC4AF2F49256AE58101FEE92B04
047B6AA5D85E572983E6FB32A7CDEBC14027B6916A894D3AEE7106FE805FC34B44
6jGSPrUM0+2YrTO2vsTOKq3+XL/IfUFs5oxZaSEvsQg=

POSSIBLE SECRETS
127971af8721782ecffa3
115792089210356248762697446949407573530086143415290314195533631308867097853951
9CA8B57A934C54DEEDA9E54A7BBAD95E3B2E91C54D32BE0B9DF96D8D35
0667ACEB38AF4E488C407433FFAE4F1C811638DF20
046AB1E344CE25FF3896424E7FFE14762ECB49F8928AC0C76029B4D5800374E9F5143E568CD23F3F4D7C0D4B1E41C8CC0D1C6ABD5F1A46DB4C
0400FAC9DFCBAC8313BB2139F1BB755FEF65BC391F8B36F8F8EB7371FD558B01006A08A41903350678E58528BEBF8A0BEFF867A7CA36716F7E01F81052
EE353FCA5428A9300D4ABA754A44C00FDFEC0C9AE4B1A1803075ED967B7BB73F
1A62BA79D98133A16BBAE7ED9A8E03C32E0824D57AEF72F88986874E5AAE49C27BED49A2A95058068426C2171E99FD3B43C5947C857D
7A556B6DAE535B7B51ED2C4D7DAA7A0B5C55F380
07A526C63D3E25A256A007699F5447E32AE456B50E
30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d2029d83c1c158547f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346d3f529252
AMztxBQmasdCMrU1nlH2RhtlfSPsjcYFxTHFmKvCDYM=
115792089237316195423570985008687907853269984665640564039457584007913129639316
04026EB7A859923FBC82189631F8103FE4AC9CA2970012D5D46024804801841CA44370958493B205E647DA304DB4CEB08CBBD1BA39494776FB988B47174DCA88C7E2945283A01C89720349DC807F4FBF374F4AEADE3BCA95314DD58CEC9F307A54FFC61EFC006D8A2C9D4979C0AC44AEA74FBEBBB9F772AEDCB620B01A7BA7AF1B320430C8591984F601CD4C143EF1C7A3

POSSIBLE SECRETS
040060F05F658F49C1AD3AB1890F7184210EFD0987E307C84C27ACCFB8F9F67CC2C460189EB5AAAA62EE222EB1B35540CFE902374601E369050B7C4E42ACBA1DACBF04299C3460782F918EA427E6325165E9EA10E3DA5F6C42E9C55215AA9CA27A5863EC48D8E0286B
FFFFFFFE0000000075A30D1B9038A115
3086d221a7d46bcde86c90e49284eb15
70B5E1E14031C1F70BBEFE96BDDE66F451754B4CA5F48DA241F331AA396B8D1839A855C1769B1EA14BA53308B5E2723724E090E02DB9
u7Ufq5yuXkEXg69T8jpWuOOX55Q9g2DSVI1gtbNUvY8=
308204a830820390a003020102020900d585b86c7dd34ef5300d06092a864886f70d0101040500308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d301e170d3038303431353233333635365a170d3335303930313233333635365a308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d30820120300d06092a864886f70d01010105000382010d00308201080282010100d6ce2e080abfe2314dd18db3cfd3185cb43d33fa0c74e1bdb6d1db8913f62c5c39df56f846813d65bec0f3ca426b07c5a8ed5a3990c167e76bc999b927894b8f0b22001994a92915e572c56d2a301ba36fc5fc113ad6cb9e7435a16d23ab7dfaeee165e4df1f0a8dbda70a869d516c4e9d051196ca7c0c557f175bc375f948c56aae86089ba44f8aa6a4dd9a7dbf2c0a352282ad06b8cc185eb15579eef86d080b1d6189c0f9af98b1c2ebd107ea45abdb68a3c7838a5e5488c76c53d40b121de7bbd30e620c188ae1aa61dbbc87dd3c645f2f55f3d4c375ec4070a93f7151d83670c16a971abe5ef2d11890e1b8aef3298cf066bf9e6ce144ac9ae86d1c1b0f020103a381fc3081f9301d0603551d0e041604148d1cc5be954c433c61863a15b04cbc03f24fe0b23081c90603551d230481c13081be80148d1cc5be954c433c61863a15b04cbc03f24fe0b2a1819aa48197308194310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e20566965773110300e060355040a1307416e64726f69643110300e060355040b1307416e64726f69643110300e06035504031307416e64726f69643122302006092a864886f70d0109011613616e64726f696440616e64726f69642e636f6d820900d585b86c7dd34ef5300c0603551d13040530030101ff300d06092a864886f70d0101040500038201010019d30cf105fb78923f4c0d7dd223233d40967acfce00081d5bd7c6e9d6ed206b0e11209506416ca244939913d26b4aa0e0f524cad2bb5c6e4ca1016a15916ea1ec5dc95a5e3a010036f49248d5109bbf2e1e618186673a3be56daf0b77b1c229e3c255e3e84c905d2387efba09cbf13b202b4e5a22c93263484a23d2fc29fa9f1939759733afd8aa160f4296c2d0163e8182859c6643e9c1962fa0c18333335bc090ff9a6b22ded1ad444229a539a94eefadabd065ced24b3e51e5dd7b66787bef12fe97fba484c423fb4ff8cc494c02f0f5051612ff6529393e8e46eac5bb21f277c151aa5f2aa627d1e89da70ab6033569de3b9897bfff7ca9da3e1243f60b
6BA06FE51464B2BD26DC57F48819BA9954667022C7D03

POSSIBLE SECRETS
B3EEABB8EE11C2BE770B684D95219ECB
021085E2755381DCCCE3C1557AFA10C2F0C0C2825646C5B34A394CBCFA8BC16B22E7E789E927BE216F02E1FB136A5F
027d29778100c65a1da1783716588dce2b8b4aee8e228f1896
c39c6c3b3a36d7701b9c71a1f5804ae5d0003f4
002757A1114D696E6768756151755316C05E0BD4
9162fbe73984472a0a9d0590
5667676A654B20754F356EA92017D946567C46675556F19556A04616B567D223A5E05656FB549016A96656A557
0443BD7E9AFB53D8B85289BCC48EE5BFE6F20137D10A087EB6E7871E2A10A599C710AF8D0D39E2061114FDD05545EC1CC8AB4093247F77275E0743FFED117182EAA9C77877AAAC6AC7D35245D1692E8EE1
cc22d6dfb95c6b25e49c0d6364a4e5980c393aa21668d953
bb85691939b869c1d087f601554b96b80cb4f55b35f433c2
fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17
043B4C382CE37AA192A4019E763036F4F5DD4D7EBB938CF935318FDCED6BC28286531733C3F03C4FEE
M2RhhRYJhjrQUa7n9jg23IBcTQvCkUFLA/9ZbQYvHFo=
0100FAF51354E0E39E4892DF6E319C72C8161603FA45AA7B998A167B8F1E629521
6C01074756099122221056911C77D77E77A777E7E7E77FCB

POSSIBLE SECRETS
A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5374
0289FDFBE4ABE193DF9559ECF07AC0CE78554E2784EB8C1ED1A57A
2E2F85F5DD74CE983A5C4237229DAF8A3F35823BE
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
DB7C2ABF62E35E668076BEAD2088
115792089237316195423570985008687907852837564279074904382605163141518161494337
91771529896554605945588149018382750217296858393520724172743325725474374979801
7F519EADA7BDA81BD826DBA647910F8C4B9346ED8CCDC64E4B1ABD11756DCE1D2074AA263B88805CED70355A33B471EE
010092537397ECA4F6145799D62B0A19CE06FE26AD
71169be7330b3038edb025f1
803e2d166a3ea6662c37e08db7f5ade5
808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
103FAEC74D696E676875615175777FC5B191EF30
C49D360886E704936A6678E1139D26B7819F7E90
GC4CZUnPsyUcm5NrWw7C8gSktjb/gtBCDrSKBLlqImuOnQy7zHyo6XlIzkH3EMVH

POSSIBLE SECRETS
5EEEFCA380D02919DC2C6558BB6D8A5D
041D1C64F068CF45FFA2A63A81B7C13F6B8847A3E77EF14FE3DB7FCAFE0CBD10E8E826E03436D646AAEF87B2E247D4AF1E8ABE1D7520F9C2A45CB1EB8E95CFD55262B70B29FEEC5864E19C054FF99129280E4646217791811142820341263C5315
04AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25DBF55296C3A545E3872760AB73617DE4A96262C6F5D9E98BF9292DC29F8F41DBD289A147CE9DA3113B5F0B8C00A60B1CE1D7E819D7A431D7C90EA0E5F
FLgp79R6LGLnWDio6G1XBjsjORgKSjLkdakyn5bigQludVyQtVZMhDAlppvakfKf
0402FE13C0537BBC11ACAA07D793DE4E6D5E5C94EEE80289070FB05D38FF58321F2E800536D538CCDAA3D9
29C41E568B77C617EFE5902F11DB96FA9613CD8D03DB08DA
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA70330870553E5C414CA92619418661197FAC10471DB1D381085DDADDB58796829CA90069
139454871199115825601409655107690713107041707059928031797758001454375765357722984094124368522288239833039114681648076688236921220737322672160740747771700911134550432053804647694904686120113087816240740184800477047157336662926249423571248823968542221753660143391485680840520336859458494803187341288580489525163
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC53
E0D2EE25095206F5E2A4F9ED229F1F256E79A0E2B455970D8D0D865BD94778C576D62F0AB7519CCD2A1A906AE30D
7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9
D09E8800291CB85396CC6717393284AAA0DA64BA
02F40E7E2221F295DE297117B7F3D62F5C6A97FFCB8CEFF1CD6BA8CE4A9A18AD84FFABBD8EFA59332BE7AD6756A66E294AFD185A78FF12AA520E4DE739BACA0C7FFEFF7F2955727A

POSSIBLE SECRETS
A335926AA319A27A1D00896A6773A4827ACDAC73
25FBC363582DCEC065080CA8287AAFF09788A66DC3A9E
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186160697311 2319
04C0A0647EAAB6A48753B033C56CB0F0900A2F5C4853375FD614B690866ABD5BB88B5F4828C1490002E6773FA2FA299B8F
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
4099B5A457F9D69F79213D094C4BCD4D4262210B
32010857077C5431123A46B808906756F543423E8D27877578125778AC76
36864200e0eaf5284d884a0e77d31646
BDB6F4FE3E8B1D9E0DA8C0D46F4C318CEFE4AFE3B6B8551F
26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6
0418DE98B02DB9A306F2AFCD7235F72A819B80AB12EBD653172476FECD462AABFFC4FF191B946A5F54D8D0AA2F418808CC25AB056962D30651A114AFD2755AD336747F93475B7A1FCA3B88F2B6A208CCFE469408584DC2B2912675BF5B9E582928
1A8F7EDA389B094C2C071E3647A8940F3C123B697578C213BE6DD9E6C8EC7335DCB228FD1EDF4A39152CBCAAF8C0398828041055F94CEEEC7E21340780FE41BD
401028774D7777C7B7666D1366EA432071274F89FF01E718
Rx5KxmHu63h8QT7T4cYR2mu7F4LQnYkocG/Azb9HP8ZHyjUHnRxxCuB99BIp3kbl

POSSIBLE SECRETS
04B199B13B9B34EFC1397E64BAEB05ACC265FF2378ADD6718B7C7C1961F0991B842443772152C9E0AD
04BED5AF16EA3F6A4F62938C4631EB5AF7BDBCDBC31667CB477A1A8EC338F94741669C976316DA6321
8E4cUkgIY9w8/0qt+Oeyh9wfu9tQKpeKsR+Ou+hsYewuB4uFdKW1FI4W+bAZwe0B
22123dc2395a05caa7423daeccc94760a7d462256bd56916
FC1217D4320A90452C760A58EDCD30C8DD069B3C34453837A34ED50CB54917E1C2112D84D164F444F8F74786046A
3EE30B568FBAB0F883CCEBD46D3F3BB8A2A73513F5EB79DA66190EB085FFA9F492F375A97D860EB4
687D1B459DC841457E3E06CF6F5E2517B97C7D614AF138BCBF85DC806C4B289F3E965D2DB1416D217F8B276FAD1AB69C50F78BEE1FA3106EFB8CCBC7C5140116
04640ECE5C12788717B9C1BA06CBC2A6FEBA85842458C56DDE9DB1758D39C0313D82BA51735CDB3EA499AA77A7D6943A64F7A3F25FE26F06B51BAA2696FA9035DA5B534BD595F5AF0FA2C892376C84ACE1BB4E3019B71634C01131159CAE03CEE9D9932184BEEF216BD71DF2DADF86A627306ECFF96DBB8BACE198B61E00F8B332
SkMlFTLt8H3eQLYvgf87g2pXBfp4xPpxL3RMs974XSU=
28E9FA9E9D9F5E344D5A9E4BCF6509A7F39789F515AB8F92DDBCBD414D940E93
70390085352083305199547718019018437841079516630045180471284346843705633502619
A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7
040356DCD8F2F95031AD652D23951BB366A80648F06D867940A5366D9E265DE9EB240F
0108B39E77C4B108BED981ED0E890E117C511CF072

POSSIBLE SECRETS
6A91174076B1E0E19C39C031FE8685C1CAE040E5C69A28EF
5kY1EQ+6snGNdZX1BEywItRy0EAwZ4DbRiPucqHAgfZR8kr75HzXIMEIf0cE9z11
7BC382C63D8C150C3C72080ACE05AFA0C2BEA28E4FB22787139165EFBA91F90F8AA5814A503AD4EB04A8C7DD22CE2826
DB7C2ABF62E35E668076BEAD208B
DC9203E514A721875485A529D2C722FB187BC8980EB866644DE41C68E143064546E861C0E2C9EDD92ADE71F46FCF50FF2AD97F951FDA9F2A2EB6546F39689BD3
04015D4860D088DDB3496B0C6064756260441CDE4AF1771D4DB01FFE5B34E59703DC255A868A1180515603AEAB60794E54BB7996A70061B1CFAB6BE5F32BBFA78324ED106A7636B9C5A7BD198D0158AA4F5488D08F38514F1FDF4B4F40D2181B3681C364BA0273C706
AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F3
115792089237316195423570985008687907853073762908499243225378155805079068850323
100997906755055304772081815535925224869841082572053457874823515875577147990529272777244152852699298796483356699682842027972896052747173175480590485607134746852141928680912561502802222185647539190902656116367847270145019066794290930185446216399730872221732889830323194097355403213400972588322876850946740663962
2472E2D0197C49363F1FE7F5B6DB075D52B6947D135D8CA445805D39BC345626089687742B6329E70680231988
6JHAw9/xzu8LcH4q9f7Udi9sTntehS9dfukXhX8DEHhp54WYBhd6ZhWkqnOAMGmY
010090512DA9AF72B08349D98A5DD4C7B0532ECA51CE03E2D10F3B7AC579BD87E909AE40A6F131E9CFCE5BD967
b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae466748d9b5a536

POSSIBLE SECRETS
95475cf5d93e596c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bbdd84c9836be1f31c0777725aeb6c2fc38b85f48076fa76bcd8146cc89a6fb2f706dd719898c2083dc8d896f84062e2c9c94d137b054a8d8096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9eb60eee8b030376b236bc73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520086746175c8885925ebc64c6147906773496990cb714ec667304e261faee33b3cbdf008e0c3fa90650d97d3909c9275bf4ac86ffcb3d03e6dfc8ada5934242dd6d3bcca2a406cb0b
0620048D28BCBD03B6249C99182B7C8CD19700C362C46A01
lnMUlT0qopStslq/RfZHkyvg0xAUTVuMPsMot4SEaYA=
04B70E0CBD6BB4BF7F321390B94A03C1D356C21122343280D6115C1D21BD376388B5F723FB4C22DFE6CD4375A05A07476444D5819985007E34
04925BE9FB01AFC6FB4D3E7D4990010F813408AB106C4F09CB7EE07868CC136FFF3357F624A21BED5263BA3A7A27483EBF6671DBEF7ABB30EBEE084E58A0B077AD42A5A0989D1EE71B1B9BC0455FB0D2C3
04B8266A46C55657AC734CE38F018F2192
04A1455B334DF099DF30FC28A169A467E9E47075A90F7E650EB6B7A45C7E089FED7FBA344282CAFBD6F7E319F7C0B0BD59E2CA4BDB556D61A5
0401A57A6A7B26CA5EF52FCDB816479700B3ADC94ED1FE674C06E695BABA1D
B4050A850C04B3ABF54132565044B0B7D7BFD8BA270B39432355FFB4
6b016c3bdcf18941d0d654921475ca71a9db2fb27d1d37796185c2942c0a
b3fb3400dec5c4adceb8655d4c94
0400C6858E06B70404E9CD9E3ECB662395B4429C648139053FB521F828AF606B4D3DBAA14B5E77EFE75928FE1DC127A2FFA8DE3348B3C1856A429BF97E7E31C2E5BD66011839296A789A3BC0045C8A5FB42C7D1BD998F54449579B446817AFBD17273E662C97EE72995EF42640C550B9013FAD0761353C7086A272C24088BE94769FD16650
0095E9A9EC9B297BD4BF36E059184F

POSSIBLE SECRETS
C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86294
10D9B4A3D9047D8B154359ABFB1B7F5485B04CEB868237DDC9DEDA982A679A5A919B626D4E50A8DD731B107A9962381FB5D807BF2618
2580F63CCFE44138870713B1A92369E33E2135D266DBB372386C400B
D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FC
E87579C11079F43DD824993C2CEE5ED3
C2173F1513981673AF4892C23035A27CE25E2013BF95AA33B22C656F277E7335
5DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2
32670510020758816978083085130507043184471273380659243275938904335757337482424
03eea2bae7e1497842f2de7769cfe9c989c072ad696f48034a
254d9f31-1321-48ba-b83d-75b0cbb2d4c1
03F7061798EB99E238FD6F1BF95B48FEEB4854252B
686479766013060971498190079908139321726943530014330540939446345918554318339765605212255964066145455497729631139148085803712198799971664381257402829111505 7151
324A6EDDD512F08C49A99AE0D3F961197A76413E7BE81A400CA681E09639B5FE12E59A109F78BF4A373541B3B9A1
004D696E67687561517512D8F03431FCE63B88F4
04161FF7528B899B2D0C28607CA52C5B86CF5AC8395BAFEB13C02DA292DDED7A83

POSSIBLE SECRETS
0409487239995A5EE76B55F9C2F098A89CE5AF8724C0A23E0E0FF77500
13D56FFAEC78681E68F9DEB43B35BEC2FB68542E27897B79
10E723AB14D696E6768756151756FEBF8FCB49A9
3FCDA526B6CDF83BA1118DF35B3C31761D3545F32728D003EEB25EFE96
114ca50f7a8e2f3f657c1108d9d44cfd8
3fysZeGzwX+hqd2f4+qtlSho+oF+DeFl9kzKrTFOSWo=
340E7BE2A280EB74E2BE61BADA745D97E8F7C300
072546B5435234A422E0789675F432C89435DE5242
FD0D693149A118F651E6DCE6802085377E5F882D1B510B44160074C1288078365A0396C8E681
7d73d21f1bd82c9e5268b6dcf9fde2cb
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316
3045AE6FC8422F64ED579528D38120EAE12196D5
BDDB97E555A50A908E43B01C798EA5DAA6788F1EA2794EFCF57166B8C14039601E55827340BE
f8183668ba5fc5bb06b5981e6d8b795d30b8978d43ca0ec572e37e09939a9773
883423532389192164791648750360308885314476597252960362792450860609699839

POSSIBLE SECRETS
617fab6832576cbbfed50d99f0249c3fee58b94ba0038c7ae84c8c832f2c
2AA058F73A0E33AB486B0F610410C53A7F132310
0017858FEB7A98975169E171F77B4087DE098AC8A911DF7B01
4B337D934104CD7BEF271BF60CED1ED20DA14C08B3BB64F18A60888D
2E45EF571F00786F67B0081B9495A3D95462F5DE0AA185EC
9douHjmTTjq3N4YYUdzzHaKyxIqsB5K92p8t26vKQB1HahpVak+32YHan4LmgLPE
4843956129390645175905258525279791420276294952604174799584408071708240463528 6
5D9306BACD22B7FAEB09D2E049C6E2866C5D1677762A8F2F2DC9A11C7F7BE8340AB2237C7F2A0
8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC50
B99B99B099B323E02709A4D696E6768756151751
0217C05610884B63B9C6C7291678F9D341
fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7

POSSIBLE SECRETS
308204433082032ba003020102020900c2e08746644a308d300d06092a864886f70d0101040500307431 0b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3038303832313233313333345a170d3336303130373233313333345a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820120300d06092a864886f70d01010105000382010d00308201080282010100ab562e00d83ba208ae0a966f124e29da11f2ab56d08f58e2cca91303e9b754d372f640a71b1dcb130967624e4656a7776a92193db2e5bfb724a91e77188b0e6a47a43b33d9609b77183145ccdf7b2e586674c9e1565b1f4c6a5955bff251a63dabf9c55c27222252e875e4f8154a645f897168c0b1bfc612eabf785769bb34aa7984dc7e2ea2764cae8307d8c17154d7ee5f64a51a44a602c249054157dc02cd5f5c0e55fbef8519fbe327f0b1511692c5a06f19d18385f5c4dbc2d6b93f68cc2979c70e18ab93866b3bd5db8999552a0e3b4c99df58fb918bedc182ba35e003c1b4b10dd244a8ee24fffd333872ab5221985edab0fc0d0b145b6aa192858e79020103a381d93081d6301d0603551d0e04160414c77d8cc2211756259a7fd382df6be398e4d786a53081a60603551d2304819e30819b8014c77d8cc2211756259a7fd382df6be398e4d786a5a178a4763074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964820900c2e08746644a308d300c0603551d13040530030101ff300d06092a864886f70d010104050003820101006dd252ceef85302c360aaace939bcff2cca904bb5d7a1661f8ae46b2994204d0ff4a68c7ed1a531ec4595a623ce60763b167297a7ae35712c407f208f0cb109429124d7b106219c084ca3eb3f9ad5fb871ef92269a8be28bf16d44c8d9a08e6cb2f005bb3fe2cb96447e868e731076ad45b33f6009ea19c161e62641aa99271dfd5228c5c587875ddb7f452758d661f6cc0cccb7352e424cc4365c523532f7325137593c4ae341f4db41edda0d0b1071a7c440f0fe9ea01cb627ca674369d084bd2fd911ff06cdbf2cfa10dc0f893ae35762919048c7efc64c7144178342f70581c9de573af55b390dd7fdb9418631895d5f759f30112687ff621410c069308a
e43bb460f0b80cc0c0b075798e948060f8321b7d
a1NlcnZlckNvbmZpZ3VyYXRpb25MYXN0VmVyc2lvbktleQ==
57896044618658097711785492504343953926634992332820282019728792003956564823190
E95E4A5F737059DC60DFC7AD95B3D8139515620F
31a92ee2029fd10d901b113e990710f0d21ac6b6
00E8BEE4D3E2260744188BE0E9C723
fe0e87005b4e83761908c5131d552a850b3f58b749c37cf5b84d6768
033C258EF3047767E7EDE0F1FDAA79DAEE3841366A132E163ACED4ED2401DF9C6BDCDE98E8E707C07A2239B1B097

POSSIBLE SECRETS
023809B2B7CC1B28CC5A87926AAD83FD28789E81E2C9E3BF10
04A3E8EB3CC1CFE7B7732213B23A656149AFA142C47AAFBC2B79A191562E1305F42D996C823439C56D7F7B22E14644417E69BCB6DE39D027001DABE8F35B25C9BE
ngqbGKXcQCvq0ft27xRzOzNoEVN+ei+Vq2+CNx9QQMc=
04A8C7DD22CE28268B39B55416F0447C2FB77DE107DCD2A62E880EA53EEB62D57CB4390295DBC9943AB78696FA504C11
03188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012
0yxvRSsGg+/BBPRqwe1F54W0T+vv1NRnE+jebtT36Vo=
3826F008A8C51D7B95284D9D03FF0E00CE2CD723A
4D696E676875615175985BD3ADBADA21B43A97E2
28792665814854611296992347458380284135028636778229113005756334730996303888124
0257927098FA932E7C0A96D3FD5B706EF7E5F5C156E16B7E7C86038552E91D
040081BAF91FDF9833C40F9C181343638399078C6E7EA38C001F73C8134B1B4EF9E150
10B51CC12849B234C75E6DD2028BF7FF5C1CE0D991A1
04017232BA853A7E731AF129F22FF4149563A419C26BF50A4C9D6EEFAD612601DB537DECE819B7F70F555A67C427A8CD9BF18AEB9B56E0C11056FAE6A3
04B6B3D4C356C139EB31183D4749D423958C27D2DCAF98B70164C97A2DD98F5CFF6142E0F7C8B204911F9271F0F3ECEF8C2701C307E8E4C9E183115A1554062CFB

POSSIBLE SECRETS
2661740802050217063228768716723360960729859168756973147706671368418802944996427808491545080627771902352094241225065558662157113545570916814161637315895999846
04188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF101207192B95FFC8DA78631011ED6B24CDD573F977A11E794811
V8P78mWO+MxnWR283vMX+BSDXEvrm8XlQCYXMpvUe5w=
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
MQVwithSHA256KDFAndSharedInfo
0429A0B6A887A983E9730988A68727A8B2D126C44CC2CC7B2A6555193035DC76310804F12E549BDB011C103089E73510ACB275FC312A5DC6B76553F0CA
C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86297
1CEF494720115657E18F938D7A7942394FF9425C1458C57861F9EEA6ADBE3BE10
04DB4FF10EC057E9AE26B07D0280B7F4341DA5D1B1EAE06C7D9B2F2F6D9C5628A7844163D015BE86344082AA88D95E2F9D
BD71344799D5C7FCDC45B59FA3B9AB8F6A948BC5
71FE1AF926CF847989EFEF8DB459F66394D90F32AD3F15E8
02197B07845E9BE2D96ADB0F5F3C7F2CFFBD7A3EB8B6FEC35C7FD67F26DDF6285A644F740A2614
9cdbd84c9f1ac2f38d0f80f42ab952e7338bf511
70390085352083305199547718019018437840920882647164081035322601458352298396601
03E5A88919D7CAFCBF415F07C2176573B2

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
94DC01F41D00112233445566778899001122334455667788990011223344556677788
5363ad4cc05c30e0a5261c028812645a122e22ea20816678df02967c1b23bd72
SxHy+zpC+eGmQUPW4BYYcldQdVxiSSVnY0gIrWauGKU=
10686D41FF744D4449FCCF6D8EEA03102E6812C93A9D60B978B702CF156D814EF
6A941977BA9F6A435199ACFC51067ED587F519C5ECB541B8E44111DE1D40
030024266E4EB5106D0A964D92C4860E2671DB9B6CC5
0njjbCFUq6vJ1UgnErUI7KEtLgZLN7V9IJ5yZ3QtzXmjMaTjzKInpeDNakYTgh0P
3d84f26c12238d7b4f3d516613c1759033b1a5800175d0b1
BB8E5E8FBC115E139FE6A814FE48AAA6F0ADA1AA5DF91985
7A1F6653786A68192803910A3D30B2A2018B21CD54
0066647EDE6C332C7F8C0923BB58213B333B20E9CE4281FE115F7D8F90AD
F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C00
71169be7330b3038edb025f1d0f9
gYgEHbtWs2qrOou4Pi9x8/evNQKl7xufkAwk8FBwpKpll2nmAbj5wvKo77J2SETY

POSSIBLE SECRETS
020ffa963cdca8816ccc33b8642bedf905c3d358573d3f27fbbd3b3cb9aaaf
020A601907B8C953CA1481EB10512F78744A3205FD
0236B3DAF8A23206F9C4F299D7B21A9C369137F2C84AE1AA0D
b869c82b35d70e1b1ff91b28e37a62ecdc34409b
393C7F7D53666B5054B5E6C6D3DE94F4296C0C599E2E2E241050DF18B6090BDC90186904968BB
7503CFE87A836AE3A61B8816E25450E6CE5E1C93ACF1ABC1778064FDCBEFA921DF1626BE4FD036E93D75E6A50E3A41E98028FE5FC235F5B889A589CB5215F2A4
e4437ed6010e88286f547fa90abfe4c42212
12702124828893241746590704277717644352578765350891653581281750726570503126098509849742318833348340118092599999512098893413065920561499672425412104927434935707492031276956145168922411057931124881261022967853463840169352001328899500036226068422275081353230700451734163368500454106258697141688368677884253782038 3
142011741597563481196368286022318089743276138395243738762872573441927459393512718973631166078467600360848946623567625795282774719212241929071046134208380636394084512691828894000571524625445295769349356752728956831541775441763139384457191755096847107846595662547942312293338483924514339614727760681880609734239
7BC86E2102902EC4D5890E8B6B4981ff27E0482750FEFC03
133531813272720673433859519948319001217942375967847486899482359599369642528734712461590403327731821410328012529253871914788598993103310567744136196364803064721377826656898686468463277710150809401182608770201615324990468332931294920912776241137878030224355746606283971659376426832674269780880061631528163475887
043AE9E58C82F63C30282E1FE7BBF43FA72C446AF6F4618129097E2C5667C2223A902AB5CA449D0084B7E5B3DE7CCC01C9
57896044618658097711785492504343953926634992332820282019728792003956564823193

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 Details: ARTM, ARTM, None, http://www.artm.quebec/application-mobile-chrono/, 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.

SCAN LOGS

Timestamp	Event	Error
2025-11-27 18:51:05	Generating Hashes	OK
2025-11-27 18:51:06	Extracting APK	OK
2025-11-27 18:51:06	Unzipping	OK

2025-11-27 18:51:08	Parsing APK with androguard	OK
2025-11-27 18:51:08	Extracting APK features using aapt/aapt2	OK
2025-11-27 18:51:09	Getting Hardcoded Certificates/Keystores	OK
2025-11-27 18:51:16	Parsing AndroidManifest.xml	OK
2025-11-27 18:51:16	Extracting Manifest Data	OK
2025-11-27 18:51:16	Manifest Analysis Started	OK
2025-11-27 18:51:16	Reading Network Security config from network_security_config.xml	OK
2025-11-27 18:51:16	Parsing Network Security config	OK
2025-11-27 18:51:16	Performing Static Analysis on: Chrono (quebec.artm.chrono)	OK
2025-11-27 18:51:17	Fetching Details from Play Store: quebec.artm.chrono	OK
2025-11-27 18:51:17	Checking for Malware Permissions	OK

2025-11-27 18:51:17	Fetching icon path	OK
2025-11-27 18:51:17	Library Binary Analysis Started	OK
2025-11-27 18:51:18	Reading Code Signing Certificate	OK
2025-11-27 18:51:19	Running APKiD 3.0.0	OK
2025-11-27 18:51:25	Detecting Trackers	OK
2025-11-27 18:51:31	Decompiling APK to Java with JADX	OK
2025-11-27 18:54:52	Converting DEX to Smali	OK
2025-11-27 18:54:52	Code Analysis Started on - java_source	OK
2025-11-27 18:57:44	Android SBOM Analysis Completed	OK
2025-11-27 18:58:04	Android SAST Completed	OK
2025-11-27 18:58:04	Android API Analysis Started	OK

2025-11-27 18:58:26	Android API Analysis Completed	OK
2025-11-27 18:58:27	Android Permission Mapping Started	OK
2025-11-27 18:58:57	Android Permission Mapping Completed	OK
2025-11-27 18:59:02	Android Behaviour Analysis Started	OK
2025-11-27 18:59:38	Android Behaviour Analysis Completed	OK
2025-11-27 18:59:38	Extracting Emails and URLs from Source Code	OK
2025-11-27 18:59:58	Email and URL Extraction Completed	OK
2025-11-27 18:59:58	Extracting String data from APK	OK
2025-11-27 18:59:58	Extracting String data from Code	OK
2025-11-27 18:59:58	Extracting String values and entropies from Code	OK
2025-11-27 19:02:30	Performing Malware check on extracted domains	OK

2025-11-27 19:02:34	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.