MOBSF

ANDROID STATIC ANALYSIS REPORT

🤖 Froedtert&MCW (8.87.1)
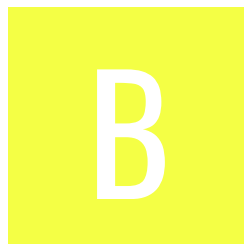
File Name:	com.froedtert.care_10000131.apk
Package Name:	com.froedtert.care
Scan Date:	Aug. 29, 2025, 10:34 p.m.
App Security Score:	**48/100 (MEDIUM RISK)**
Grade:	**B**
Trackers Detection:	3/432

📊 FINDINGS SEVERITY

🐛 HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
5	29	4	3	2

📦 FILE INFORMATION

File Name: com.froedtert.care_10000131.apk
Size: 143.69MB
MD5: 65bc5b3d26fd9bac0f795615adad90f5
SHA1: b4126e4bb08a7aa74e6297ea101123b22ac06114
SHA256: 065a3c1528c15ffa2906c39c56e68719a854d85a1dd5702c6781dc462f5032e8

ℹ APP INFORMATION

App Name: Froedtert&MCW
Package Name: com.froedtert.care
Main Activity: com.froedtert.care.MainActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 8.87.1

Android Version Code: 10000131

▪▪ APP COMPONENTS

Activities: 160
Services: 32
Receivers: 18
Providers: 14
Exported Activities: 7
Exported Services: 4
Exported Receivers: 3
Exported Providers: 0

❁ CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
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: 2020-03-04 18:36:11+00:00
Valid To: 2050-03-04 18:36:11+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xdf2a7986d3f2c707cb591949f928f10f276ca058
Hash Algorithm: sha256
md5: 799471deec54c1b9f50f579f54593757
sha1: 5adb512e40963729e6815a2758fa673a24b38d0b
sha256: 8d2b3fc3eff08b0173eae98b43d15b9c2e3a5c50846a8a3e970fb14583692b81
sha512: 16a5b66c5514b5a3f46df048f9d64674376a9b3b404a427661cc9017935d753cff9746a49102ccdab77b31ea51d41ad5cc3c212f1091137b68b0a2a557bd21a2
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 758d021fdbf5cf5bf7e0a4abc74571ba6a58a7a3569c74a376c537a73537fc50
Found 1 unique certificates

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.FOREGROUND_SERVICE_CONNECTED_DEVICE	normal	enables foreground services with connected device use.	Allows a regular application to use Service.startForeground with the type "connectedDevice".
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	normal	enables foreground services for media playback.	Allows a regular application to use Service.startForeground with the type "mediaPlayback".

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.froedtert.care.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.
android.permission.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.FOREGROUND_SERVICE_MICROPHONE	normal	permits foreground services with microphone use.	Allows a regular application to use Service.startForeground with the type "microphone".
android.permission.FOREGROUND_SERVICE_PHONE_CALL	normal	enables foreground services during phone calls.	Allows a regular application to use Service.startForeground with the type "phoneCall".
android.permission.FOREGROUND_SERVICE_MEDIA_PROJECTION	normal	allows foreground services for media projection.	Allows a regular application to use Service.startForeground with the type "mediaProjection".
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	dangerous	allows reading user-selected image or video files from external storage.	Allows an application to read image or video files from external storage that a user has selected via the permission prompt photo picker. Apps can check this permission to verify that a user has decided to use the photo picker, instead of granting access to READ_MEDIA_IMAGES or READ_MEDIA_VIDEO . It does not prevent apps from accessing the standard photo picker manually. This permission should be requested alongside READ_MEDIA_IMAGES and/or READ_MEDIA_VIDEO , depending on which type of media is desired.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.
android.permission.REORDER_TASKS	normal	reorder applications running	Allows an application to move tasks to the foreground and background. Malicious applications can force themselves to the front without your control.
com.froedtert.care.sdk.permission-group.ipc.sender	unknown	Unknown permission	Unknown permission from android reference

🔎 APKID ANALYSIS

FILE	DETAILS
65bc5b3d26fd9bac0f795615adad90f5.apk	**FINDINGS** / **DETAILS** Anti-VM Code — possible VM check
classes.dex	**FINDINGS** / **DETAILS** yara_issue — yara issue - dex file recognized by apkid but not yara module Compiler — unknown (please file detection issue!)

FILE	DETAILS
classes10.dex	<table><tr><td>FINDINGS</td><td>DETAILS</td></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>
classes11.dex	<table><tr><td>FINDINGS</td><td>DETAILS</td></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check possible Build.SERIAL check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

FILE	DETAILS
classes12.dex	**FINDINGS** / **DETAILS** yara_issue — yara issue - dex file recognized by apkid but not yara module Anti-VM Code — Build.FINGERPRINT check / Build.MANUFACTURER check / possible Build.SERIAL check / SIM operator check Compiler — unknown (please file detection issue!)
classes13.dex	**FINDINGS** / **DETAILS** yara_issue — yara issue - dex file recognized by apkid but not yara module Anti-VM Code — Build.MANUFACTURER check Compiler — unknown (please file detection issue!)

FILE	DETAILS
classes14.dex	**FINDINGS** / **DETAILS** **yara_issue** — yara issue - dex file recognized by apkid but not yara module **Anti-VM Code** — Build.MANUFACTURER check / Build.BOARD check **Compiler** — unknown (please file detection issue!)
classes2.dex	**FINDINGS** / **DETAILS** **yara_issue** — yara issue - dex file recognized by apkid but not yara module **Anti-VM Code** — Build.FINGERPRINT check / Build.MODEL check / Build.MANUFACTURER check / Build.PRODUCT check / network operator name check / possible VM check **Anti Debug Code** — Debug.isDebuggerConnected() check **Compiler** — unknown (please file detection issue!)

FILE	DETAILS
classes3.dex	<table><tr><td>FINDINGS</td><td>DETAILS</td></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check network operator name check possible VM check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

FILE	DETAILS
classes4.dex	**FINDINGS** — **DETAILS** yara_issue — yara issue - dex file recognized by apkid but not yara module Anti-VM Code — Build.FINGERPRINT check Build.MANUFACTURER check Build.BOARD check Compiler — unknown (please file detection issue!)
classes5.dex	**FINDINGS** — **DETAILS** yara_issue — yara issue - dex file recognized by apkid but not yara module Anti-VM Code — Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check Compiler — unknown (please file detection issue!)

FILE	DETAILS
classes6.dex	**FINDINGS** / **DETAILS** yara_issue — yara issue - dex file recognized by apkid but not yara module Anti-VM Code — Build.FINGERPRINT check / Build.MANUFACTURER check / Build.BOARD check Compiler — unknown (please file detection issue!)
classes7.dex	**FINDINGS** / **DETAILS** yara_issue — yara issue - dex file recognized by apkid but not yara module Anti-VM Code — Build.MODEL check / Build.MANUFACTURER check / Build.PRODUCT check Compiler — unknown (please file detection issue!)

FILE	DETAILS
classes8.dex	**FINDINGS** / **DETAILS** **yara_issue**: yara issue - dex file recognized by apkid but not yara module **Anti-VM Code**: Build.FINGERPRINT check / Build.MANUFACTURER check **Compiler**: unknown (please file detection issue!)
classes9.dex	**FINDINGS** / **DETAILS** **yara_issue**: yara issue - dex file recognized by apkid but not yara module **Anti-VM Code**: Build.FINGERPRINT check / Build.MODEL check / Build.MANUFACTURER check / Build.PRODUCT check / Build.HARDWARE check / Build.TAGS check / possible VM check **Anti Debug Code**: Debug.isDebuggerConnected() check **Compiler**: unknown (please file detection issue!)

📑 BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.froedtert.care.MainActivity	Schemes: froedterthc://, https://, Hosts: app, open, froedtert.link, froedtert.test-app.link, froedtert.app.link, Path Prefixes: /,
epic.mychart.android.library.prelogin.SplashActivity	Schemes: epicmychart://,
com.stripe.android.link.LinkRedirectHandlerActivity	Schemes: link-popup://, Hosts: complete, Paths: /com.froedtert.care,
com.stripe.android.payments.StripeBrowserProxyReturnActivity	Schemes: stripesdk://, Hosts: payment_return_url, Paths: /com.froedtert.care,
com.stripe.android.financialconnections.FinancialConnectionsSheetRedirectActivity	Schemes: stripe-auth://, stripe://, Hosts: link-accounts, link-native-accounts, native-redirect, auth-redirect, Paths: /com.froedtert.care/success, /com.froedtert.care/cancel, Path Prefixes: /com.froedtert.care/authentication_return, /com.froedtert.care,
com.okta.oidc.OktaRedirectActivity	Schemes: com.froedtert.care://,

🔒 NETWORK SECURITY

HIGH: **2** | WARNING: **1** | INFO: **0** | SECURE: **0**

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.
3	*	high	Base config is configured to trust user installed certificates.

🪪 CERTIFICATE ANALYSIS

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

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

🔍 MANIFEST ANALYSIS

HIGH: **0** | WARNING: **16** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. 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/wp_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 (epic.mychart.android.library.healthlinks.HealthConnectPrivacyPolicyActivity) 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	Activity-Alias (epic.mychart.android.library.HealthConnectViewPermissionsActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.START_VIEW_PERMISSION_USAGE [android:exported=true]	warning	An Activity-Alias 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.
5	Service (com.wix.reactnativenotifications.fcm.FcmInstanceIdListenerService) is not Protected. [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.
6	Activity (com.stripe.android.link.LinkRedirectHandlerActivity) 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
7	Activity (com.stripe.android.payments.StripeBrowserProxyReturnActivity) 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.
8	Activity (com.stripe.android.financialconnections.FinancialConnectionsSheetRedirectActivity) 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.
9	Service (androidx.health.platform.client.impl.sdkservice.HealthDataSdkService) is not Protected. [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.
10	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.
11	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
12	Activity (com.okta.oidc.OktaRedirectActivity) 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
13	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.
14	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
15	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.
16	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.
17	TaskAffinity is set for activity (com.zipow.videobox.conference.ui.ZmConfPipActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.

</> CODE ANALYSIS

HIGH: **3** | WARNING: **10** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				cl/json/RNShareImpl.java cl/json/RNSharePathUtil.java cl/json/social/InstagramShare.java cl/json/social/SingleShareIntent.java com/agontuk/RNFusedLocation/RNFusedLocationModule.java com/agontuk/RNFusedLocation/SingleLocationUpdate.java com/airbnb/android/react/lottie/LottieAnimationViewPropertyManager.java com/airbnb/android/react/maps/AirMapGradientPolyline.java com/airbnb/android/react/maps/AirMapHeatmap.java com/airbnb/android/react/maps/AirMapModule.java com/airbnb/android/react/maps/AirMapTileProvider.java com/airbnb/android/react/maps/AirMapTileWorker.java com/airbnb/android/react/maps/AirMapUrlTile.java com/airbnb/android/react/maps/FileUtil.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java com/amazonaws/amplify/rtnpushnotification/PushNotificationAWSPinpointUtilsKt.java com/amazonaws/amplify/rtnpushnotification/PushNotificationFirebaseMessagingService.java com/amazonaws/amplify/rtnpushnotification/PushNotificationLaunchActivity.java com/amazonaws/amplify/rtnpushnotification/Pus

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/amazonaws/amplify/rtnpushnotification/PushNotificationModule.java com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/model/ByteBufferEncoder.java
				com/bumptech/glide/load/model/ByteBufferFileLoader.java
				com/bumptech/glide/load/model/FileLoader.java
				com/bumptech/glide/load/model/ResourceLoader.java
				com/bumptech/glide/load/model/StreamEncoder.java
				com/bumptech/glide/load/resource/ImageDecoderResourceDecoder.java
				com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java
				com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java
				com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java
				com/bumptech/glide/load/resource/bitmap/Downsampler.java
				com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java
				com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java
				com/bumptech/glide/load/resource/bitmap/TransformationUtils.java
				com/bumptech/glide/load/resource/bitmap/VideoDecoder.java
				com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java
				com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java
				com/bumptech/glide/load/resource/gif/StreamGifDecoder.java
				com/bumptech/glide/manager/DefaultConnectivityMonitor.java
				com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java
				com/bumptech/glide/manager/RequestManagerFragment.java
				com/bumptech/glide/manager/RequestManagerRetriever.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/manager/RequestTracker.jav a com/bumptech/glide/manager/SupportRequestMa nagerFragment.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewT arget.java com/bumptech/glide/request/target/ViewTarget.ja va com/bumptech/glide/signature/ApplicationVersion Signature.java com/bumptech/glide/util/ContentLengthInputStrea m.java com/bumptech/glide/util/pool/FactoryPools.java com/davemorrissey/labs/subscaleview/Subsampli ngScaleImageView.java com/davemorrissey/labs/subscaleview/decoder/Sk iaPooledImageRegionDecoder.java com/epic/patientengagement/core/session/MyCha rtOrgToOrgJumpManager.java com/epic/patientengagement/core/ui/ProgressBar. java com/epic/patientengagement/core/ui/buttons/Cor eButton.java com/epic/patientengagement/core/ui/buttons/Cor eButtonUtils.java com/epic/patientengagement/core/ui/stickyheader /StickyHeaderAdapter.java com/epic/patientengagement/core/ui/tutorials/PET utorialFragment.java com/epic/patientengagement/core/utilities/Perfor manceLogger.java com/epic/patientengagement/core/utilities/broadc ast/BroadcastManager.java com/epic/patientengagement/core/webservice/We bServiceTask.java com/epic/patientengagement/onboarding/views/O rgTermsConditionsView.java com/epic/patientengagement/todo/progress/c.java com/froedtert/care/PushNotificationModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/froedtert/care/aws/pinpoint/PinpointNotificationService.java
				com/horcrux/svg/Brush.java
				com/horcrux/svg/ClipPathView.java
				com/horcrux/svg/ImageView.java
				com/horcrux/svg/LinearGradientView.java
				com/horcrux/svg/PatternView.java
				com/horcrux/svg/RadialGradientView.java
				com/horcrux/svg/UseView.java
				com/horcrux/svg/VirtualView.java
				com/ibits/react_native_in_app_review/AppReviewModule.java
				com/jakewharton/disklrucache/DiskLruCache.java
				com/learnium/RNDeviceInfo/RNDeviceModule.java
				com/learnium/RNDeviceInfo/RNInstallReferrerClient.java
				com/learnium/RNDeviceInfo/resolver/DeviceIdResolver.java
				com/microsoft/codepush/react/CodePushUtils.java
				com/oblador/keychain/KeychainModule.java
				com/oblador/keychain/cipherStorage/CipherStorageBase.java
				com/oblador/keychain/cipherStorage/CipherStorageFacebookConceal.java
				com/oblador/keychain/cipherStorage/CipherStorageKeystoreAesCbc.java
				com/oblador/keychain/cipherStorage/CipherStorageKeystoreRsaEcb.java
				com/oblador/keychain/decryptionHandler/DecryptionResultHandlerInteractiveBiometric.java
				com/oblador/keychain/decryptionHandler/DecryptionResultHandlerInteractiveBiometricManualRetry.java
				com/okta/oidc/OIDCConfig.java
				com/okta/oidc/OktaAuthenticationActivity.java
				com/okta/oidc/clients/AuthAPI.java
				com/okta/oidc/clients/web/SyncWebAuthClientImpl.java
				com/okta/oidc/net/request/TokenRequest.java
1	The App logs information. Sensitive	info	CWE: CWE-532: Insertion of Sensitive Information into Log File	com/okta/oidc/storage/OktaRepository.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
	information should never be logged.	Info	Information Into Log File OWASP MASVS: MSTG-STORAGE-3	com/okta/oidc/storage/security/EncryptionManager.java com/okta/oidc/storage/security/EncryptionManagerAPI23.java com/okta/oidc/util/CodeVerifierUtil.java com/okta/oidc/util/UriUtil.java com/prove/sdk/core/LoggerFactory.java com/reactcommunity/rndatetimepicker/Common.java com/reactcommunity/rndatetimepicker/MinuteIntervalSnappableTimePickerDialog.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/reactnativecommunity/webview/RNCWebView.java com/reactnativecommunity/webview/RNCWebViewClient.java com/reactnativecommunity/webview/RNCWebViewManagerImpl.java com/reactnativestripesdk/CardFieldView.java com/reactnativestripesdk/CustomerSheetFragment.java com/reactnativestripesdk/GooglePayButtonView.java com/reactnativestripesdk/StripeSdkModule.java com/reactnativestripesdk/addresssheet/AddressSheetView.java com/reactnativestripesdk/customersheet/ReactNativeCustomerAdapter.java com/reactnativestripesdk/pushprovisioning/PushProvisioningProxy.java com/reactnativestripesdk/pushprovisioning/TapAndPayProxy.java com/reactnativestripesdk/utils/MappersKt.java com/reactnativezendesk/ZendeskManager.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/stripe/android/IssuingCardPinService.java com/stripe/android/core/Logger.java com/stripe/android/core/storage/SharedPreferencesStorage.java com/stripe/android/core/utils/PluginDetector.java com/stripe/android/financialconnections/features/generic/GenericScreenKt.java com/stripe/android/stripe3ds2/transaction/Logger.java com/stripe/android/ui/core/elements/LpmSerializer.java com/stripe/android/uicore/image/ImageLruDiskCache.java com/stripe/android/uicore/image/UiUtilsKt.java com/stripe/hcaptcha/webview/HCaptchaDebugInfo.java com/stripe/hcaptcha/webview/HCaptchaWebView.java com/stripe/hcaptcha/webview/HCaptchaWebViewHelper.java com/sudoplz/rninappupdates/SpReactNativeInAppUpdatesModule.java com/swmansion/gesturehandler/react/RNGestureHandlerRootHelper.java com/swmansion/gesturehandler/react/RNGestureHandlerRootView.java com/swmansion/reanimated/NativeMethodsHelper.java com/swmansion/reanimated/ReanimatedModule.java com/swmansion/reanimated/ReanimatedUIManagerFactory.java com/swmansion/reanimated/keyboard/WindowsInsetsManager.java com/swmansion/reanimated/layoutReanimation/AnimationsManager.java com/swmansion/reanimated/layoutReanimation/ReanimatedNativeHierarchyManager.java com/swmansion/reanimated/layoutReanimation/ScreensHelper.java com/swmansion/reanimated/layoutReanimation/S

NO	ISSUE	SEVERITY	STANDARDS	FILES
				haredTransitionManager.java
				com/swmansion/reanimated/layoutReanimation/TabNavigatorObserver.java
				com/swmansion/reanimated/nativeProxy/NativeProxyCommon.java
				com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java
				com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java
				com/swmansion/rnscreens/ScreensModule.java
				com/swmansion/rnscreens/SearchBarManager.java
				com/swmansion/rnscreens/utils/ScreenDummyLayoutHelper.java
				com/th3rdwave/safeareacontext/SafeAreaView.java
				com/vonovak/AddCalendarEventModule.java
				com/wix/reactnativenotifications/RNNotificationsModule.java
				com/wix/reactnativenotifications/core/notification/PushNotification.java
				com/zendesk/logger/Logger.java
				com/zipow/videobox/ZMFirebaseMessagingService.java
				com/zipow/videobox/fragment/SettingAboutFragment.java
				com/zipow/videobox/sip/server/CmmSIPNosManager.java
				com/zoontek/rnbootsplash/RNBootSplashModuleImpl.java
				dagger/android/AndroidInjection.java
				epic/mychart/android/library/api/classes/WPAPIFirebaseMessagingService.java
				epic/mychart/android/library/appointments/FutureAppointmentFragment.java
				epic/mychart/android/library/appointments/c.java
				epic/mychart/android/library/campaigns/d.java
				epic/mychart/android/library/customactivities/JavaScriptWebViewActivity.java
				epic/mychart/android/library/customadapters/StickyHeaderSectionAdapter/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				epic/mychart/android/library/general/AccessResult.java
				epic/mychart/android/library/general/DeepLinkManager.java
				epic/mychart/android/library/healthlinks/b.java
				epic/mychart/android/library/location/fragments/a.java
				epic/mychart/android/library/location/services/AppointmentArrivalService.java
				epic/mychart/android/library/pushnotifications/CustomFcmListenerService.java
				epic/mychart/android/library/trackmyhealth/a.java
				epic/mychart/android/library/utilities/e0.java
				epic/mychart/android/library/utilities/f0.java
				epic/mychart/android/library/utilities/j.java
				epic/mychart/android/library/utilities/k.java
				epic/mychart/android/library/utilities/p.java
				epic/mychart/android/library/utilities/r.java
				epic/mychart/android/library/utilities/z.java
				expo/modules/ExpoModulesPackage.java
				expo/modules/adapters/react/services/UIManagerModuleWrapper.java
				expo/modules/apploader/AppLoaderProvider.java
				expo/modules/core/logging/OSLogHandler.java
				expo/modules/filesystem/FileSystemModule$downloadResumableTask$2.java
				expo/modules/filesystem/FileSystemModule.java
				io/invertase/firebase/app/ReactNativeFirebaseApp.java
				io/invertase/firebase/common/RCTConvertFirebase.java
				io/invertase/firebase/common/ReactNativeFirebaseEventEmitter.java
				io/invertase/firebase/common/SharedUtils.java
				io/invertase/firebase/dynamiclinks/ReactNativeFirebaseDynamicLinksModule.java
				io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java
				io/sentry/SystemOutLogger.java
				io/sentry/android/core/AndroidLogger.java
				io/sentry/android/core/SentryLogcatAdapter.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/sentry/android/replay/WindowManagerSpy.java io/sentry/android/replay/WindowSpy.java io/sentry/transport/StdoutTransport.java io/split/rnsplit/RNEventSourceModule.java org/altbeacon/beacon/BeaconParser.java org/altbeacon/beacon/logging/ApiTrackingLogger.java org/altbeacon/beacon/logging/InfoAndroidLogger.java org/altbeacon/beacon/logging/VerboseAndroidLogger.java org/altbeacon/beacon/logging/WarningAndroidLogger.java org/altbeacon/beacon/service/ScanHelper.java org/altbeacon/beacon/service/ScanState.java org/altbeacon/beacon/utils/EddystoneTelemetryAccessor.java org/greenrobot/eventbus/Logger.java org/wonday/orientation/OrientationActivityLifecycle.java org/wonday/orientation/OrientationModule.java timber/log/Timber.java us/zoom/proguard/vh4.java zendesk/chat/ChatLog.java zendesk/chat/ChatStateStore.java zendesk/chat/DeliveryStatusMonitor.java zendesk/chat/DnConverterUtils.java zendesk/chat/DnModels.java zendesk/classic/messaging/MessagingModel.java zendesk/core/MediaFileProvider.java zendesk/core/MediaFileResolver.java zendesk/support/request/MediaResultUtility.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/zipow/videobox/conference/ui/dialog/ZmBaseLiveStreamDialog.java com/zipow/videobox/view/sip/coverview/PhonePBXListCoverSummaryView.java com/zipow/videobox/view/sip/voicemail/encryption/ui/b.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/zmsg/deeplink/DeepLinkViewHelper.java us/zoom/zmsg/richtext/CustomActionModeProvider.java us/zoom/zmsg/view/mm/f.java
				com/amazonaws/amplify/rtnpushnotification/PushNotificationHeadlessTaskService.java com/amazonaws/amplify/rtnpushnotification/PushNotificationModuleKt.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/manager/RequestManagerRetriever.java com/epic/patientengagement/authentication/login/activities/PreloginInternalWebViewActivity.java com/epic/patientengagement/authentication/login/activities/PreloginInternalWebViewFragment.java com/epic/patientengagement/authentication/login/activities/SAMLLoginActivity.java com/epic/patientengagement/authentication/login/fragments/EnterPasscodeDialogFragment.java com/epic/patientengagement/authentication/login/fragments/LoginFragment.java com/epic/patientengagement/authentication/login/fragments/LongTextDialogFragment.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/epic/patientengagement/authentication/login /Fragments/OrgFragment.java com/epic/patientengagement/authentication/login /utilities/LoginHelper.java com/epic/patientengagement/authentication/login /utilities/LoginResultCode.java com/epic/patientengagement/authentication/login /utilities/OrganizationLoginHelper.java com/epic/patientengagement/authentication/login /utilities/SamlSessionManager.java com/epic/patientengagement/core/component/IAu thenticationComponentAPI.java com/epic/patientengagement/core/deeplink/Deep LinkLaunchParameters.java com/epic/patientengagement/core/mychartweb/Ex ternalJumpDialogFragment.java com/epic/patientengagement/core/mychartweb/M yChartWebQueryParameters.java com/epic/patientengagement/core/mychartweb/M yChartWebViewClient.java com/epic/patientengagement/core/mychartweb/M yChartWebViewFragment.java com/epic/patientengagement/core/mychartweb/W ebSessionWebServiceAPI.java com/epic/patientengagement/core/onboarding/On boardingHostFragment.java com/epic/patientengagement/core/onboarding/On boardingPageFragment.java com/epic/patientengagement/core/permissions/Pe rmissionProminentDisclosure.java com/epic/patientengagement/core/security/Securit yPoints.java com/epic/patientengagement/core/ui/VideoCardVi ew.java com/epic/patientengagement/core/utilities/PrintUt il.java com/epic/patientengagement/core/utilities/WebUti l.java com/epic/patientengagement/core/utilities/file/File ChooserTypeSelectionDialogFragment.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/epic/patientengagement/core/webservice/WebService.java
				com/epic/patientengagement/core/webservice/processor/MyChartResponseProcessor.java
				com/epic/patientengagement/homepage/HomePageComponentAPI.java
				com/froedtert/care/appstate/AppStateModuleKt.java
				com/microsoft/codepush/react/CodePushConstants.java
				com/microsoft/codepush/react/CodePushTelemetryManager.java
				com/nimbusds/jose/HeaderParameterNames.java
				com/nimbusds/jose/jwk/JWKParameterNames.java
				com/oblador/keychain/KeychainModule.java
				com/okta/oidc/net/request/ProviderConfiguration.java
				com/okta/oidc/net/request/web/WebRequest.java
				com/okta/oidc/net/response/TokenResponse.java
				com/okta/oidc/net/response/web/WebResponse.java
				com/oktareactnative/OktaSdkBridgeModule.java
				com/oktareactnative/OktaSdkConstant.java
				com/stripe/android/EphemeralKey.java
				com/stripe/android/PaymentConfiguration.java
				com/stripe/android/analytics/SessionSavedStateHandler.java
				com/stripe/android/auth/PaymentBrowserAuthContract.java
				com/stripe/android/core/injection/InjectorKt.java
				com/stripe/android/core/injection/NamedConstantsKt.java
				com/stripe/android/core/networking/AnalyticsFields.java
				com/stripe/android/core/networking/ApiRequest.java
				com/stripe/android/core/networking/NetworkConstantsKt.java
				com/stripe/android/core/networking/SendAnalyticsRequestV2WorkerKt.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/stripe/android/customersheet/CustomerSheet.java com/stripe/android/customersheet/CustomerSheetConfigViewModel.java com/stripe/android/customersheet/CustomerSheetContractKt.java com/stripe/android/customersheet/data/CachedCustomerEphemeralKey.java com/stripe/android/customersheet/data/CustomerSessionElementsSession.java com/stripe/android/financialconnections/FinancialConnectionsSheet.java com/stripe/android/financialconnections/analytics/DefaultFinancialConnectionsEventReporter.java com/stripe/android/financialconnections/di/NamedConstantsKt.java com/stripe/android/financialconnections/features/linkaccountpicker/LinkAccountPickerState.java com/stripe/android/financialconnections/features/linkstepupverification/LinkStepUpVerificationState.java com/stripe/android/financialconnections/features/networkinglinkverification/NetworkingLinkVerificationState.java com/stripe/android/financialconnections/features/networkingsavetolinkverification/NetworkingSaveToLinkVerificationState.java com/stripe/android/financialconnections/model/FinancialConnectionsSession.java com/stripe/android/financialconnections/model/GetFinancialConnectionsAcccountsParams.java com/stripe/android/financialconnections/network/NetworkConstants.java com/stripe/android/financialconnections/repository/CachedConsumerSession.java com/stripe/android/financialconnections/repository/FinancialConnectionsAccountsRepositoryImpl.java com/stripe/android/googlepaylauncher/GooglePayLauncherContract.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	[Files may contain hardcoded sensitive information like usernames, passwords, keys etc.](#)	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/stripe/android/googlepaylauncher/GooglePayLauncherViewModel.java com/stripe/android/googlepaylauncher/GooglePayPaymentMethodLauncherContract.java com/stripe/android/googlepaylauncher/GooglePayPaymentMethodLauncherViewModel.java com/stripe/android/link/serialization/PopupPayload.java com/stripe/android/model/AttachConsumerToLinkAccountSession.java com/stripe/android/model/ConfirmPaymentIntentParams.java com/stripe/android/model/ConfirmSetupIntentParams.java com/stripe/android/model/ConfirmStripeIntentParams.java com/stripe/android/model/ConsumerSession.java com/stripe/android/model/ConsumerSessionLookup.java com/stripe/android/model/ConsumerSessionSignup.java com/stripe/android/model/CreateFinancialConnectionsSessionParams.java com/stripe/android/model/ElementsSession.java com/stripe/android/model/ElementsSessionParams.java com/stripe/android/model/FinancialConnectionsSession.java com/stripe/android/model/PaymentIntent.java com/stripe/android/model/PaymentMethodCreateParams.java com/stripe/android/model/RadarSessionWithHCaptcha.java com/stripe/android/model/SetupIntent.java com/stripe/android/model/Source.java com/stripe/android/model/SourceParams.java com/stripe/android/model/Stripe3ds2AuthParams.java com/stripe/android/model/Stripe3ds2Fingerprint.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/stripe/android/model/StripeIntent.java com/stripe/android/model/parsers/ConsumerSessionJsonParser.java
				com/stripe/android/model/parsers/ElementsSessionJsonParser.java
				com/stripe/android/model/parsers/EphemeralKeyJsonParser.java
				com/stripe/android/model/parsers/FinancialConnectionsSessionJsonParser.java
				com/stripe/android/model/parsers/NextActionDataParser.java
				com/stripe/android/model/parsers/PaymentIntentJsonParser.java
				com/stripe/android/model/parsers/RadarSessionWithHCaptchaJsonParser.java
				com/stripe/android/model/parsers/SetupIntentJsonParser.java
				com/stripe/android/model/parsers/SourceJsonParser.java
				com/stripe/android/payments/PaymentFlowResult.java
				com/stripe/android/payments/bankaccount/CollectBankAccountForInstantDebitsLauncher.java
				com/stripe/android/payments/bankaccount/CollectBankAccountLauncher.java
				com/stripe/android/payments/bankaccount/navigation/CollectBankAccountContract.java
				com/stripe/android/payments/bankaccount/ui/CollectBankAccountViewEffect.java
				com/stripe/android/payments/core/authentication/threeds2/Stripe3ds2TransactionContract.java
				com/stripe/android/payments/paymentlauncher/PaymentLauncherContract.java
				com/stripe/android/paymentsheet/ExternalPaymentMethodProxyActivity.java
				com/stripe/android/paymentsheet/IntentConfirmationDefinition.java
				com/stripe/android/paymentsheet/IntentConfirmationHandler.java
				com/stripe/android/paymentsheet/IntentConfirma

NO	ISSUE	SEVERITY	STANDARDS	FILES
				tionInterceptor.java
				com/stripe/android/paymentsheet/PaymentSheet.java
				com/stripe/android/paymentsheet/PaymentSheetContract.java
				com/stripe/android/paymentsheet/addresselement/AddressDetails.java
				com/stripe/android/paymentsheet/addresselement/AddressElementActivityContract.java
				com/stripe/android/paymentsheet/addresselement/AddressElementNavigator.java
				com/stripe/android/paymentsheet/addresselement/AddressLauncher.java
				com/stripe/android/paymentsheet/flowcontroller/DefaultFlowController.java
				com/stripe/android/paymentsheet/flowcontroller/FlowControllerActivityResultCaller.java
				com/stripe/android/paymentsheet/flowcontroller/FlowControllerViewModel.java
				com/stripe/android/paymentsheet/paymentdatacollection/ach/USBankAccountFormViewModel.java
				com/stripe/android/paymentsheet/paymentdatacollection/polling/PollingContract.java
				com/stripe/android/paymentsheet/paymentdatacollection/polling/PollingViewModel.java
				com/stripe/android/paymentsheet/repositories/CustomerRepository.java
				com/stripe/android/paymentsheet/state/CustomerState.java
				com/stripe/android/polling/IntentStatusPoller.java
				com/stripe/android/stripe3ds2/observability/DefaultSentryConfig.java
				com/stripe/android/stripe3ds2/transaction/AcsData.java
				com/stripe/android/stripe3ds2/transaction/AuthenticationRequestParameters.java
				com/stripe/android/stripe3ds2/transaction/DefaultAcsDataParser.java
				com/stripe/android/stripe3ds2/transaction/IntentData.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/stripe/android/uicore/elements/AddressType.java
				com/stripe/android/view/AddPaymentMethodViewModel.java
				com/stripe/android/view/PaymentAuthWebViewClient.java
				com/stripe/hcaptcha/config/HCaptchaConfig.java
				com/sudoplz/rninappupdates/SpReactNativeInAppUpdatesModule.java
				com/zipow/videobox/confapp/meeting/reaction/ZmBulletEmojiEmitter.java
				com/zipow/videobox/login/model/UserAccount.java
				com/zipow/videobox/ptapp/AutoLogoffChecker.java
				com/zipow/videobox/ptapp/ZmMoveMeetingHelper.java
				com/zipow/videobox/ptapp/ZmZRMgr.java
				com/zipow/videobox/sip/server/CmmSIPCallHistoryItemBean.java
				epic/mychart/android/library/api/classes/WPAPIAuthentication.java
				epic/mychart/android/library/healthlinks/d.java
				expo/modules/adapters/react/NativeModulesProxy.java
				expo/modules/interfaces/permissions/PermissionsResponse.java
				io/invertase/firebase/common/TaskExecutorService.java
				io/reactivex/internal/schedulers/SchedulerPoolFactory.java
				io/sentry/Baggage.java
				io/sentry/RequestDetailsResolver.java
				io/sentry/SpanDataConvention.java
				io/sentry/TraceContext.java
				io/sentry/protocol/User.java
				org/altbeacon/beacon/service/MonitoringData.java
				org/altbeacon/beacon/service/RangingData.java
				org/altbeacon/beacon/service/SettingsData.java
				org/altbeacon/beacon/service/StartRMData.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/kaazing/gateway/client/transport/ws/WebSock etDelegateImpl.java
				us/zoom/feature/pbo/ui/ZmPBOUI.java
				us/zoom/libtools/storage/PreferenceUtil.java
				us/zoom/libtools/storage/ZmSharePreferenceHelp er.java
				us/zoom/libtools/utils/ZmDeviceUtils.java
				us/zoom/module/api/zcalendar/IZCalendarService. java
				us/zoom/proguard/bh0.java
				us/zoom/proguard/cx4.java
				us/zoom/proguard/d14.java
				us/zoom/proguard/id.java
				us/zoom/proguard/iw1.java
				us/zoom/proguard/jn1.java
				us/zoom/proguard/u84.java
				us/zoom/proguard/x83.java
				us/zoom/zimmsg/chats/IMThreadsFragment.java
				us/zoom/zmsg/MMImageListActivity.java
				zendesk/answerbot/AnswerBotArticleActivity.java
				zendesk/answerbot/AnswerBotSettings.java
				zendesk/answerbot/LocaleProvider.java
				zendesk/chat/ChatLogBlacklister.java
				zendesk/chat/ChatProvidersStorage.java
				zendesk/chat/PayloadAnonymousVisitorLogin.java
				zendesk/chat/PayloadAuthenticatedVisitorLogin.jav a
				zendesk/chat/UserAgentAndClientHeadersIntercept or.java
				zendesk/classic/messaging/MessagingActivity.java
				zendesk/commonui/PhotoPickerLifecycleObserver. java
				zendesk/core/Constants.java
				zendesk/core/LegacyIdentityMigrator.java
				zendesk/core/ZendeskCoreSettingsStorage.java
				zendesk/core/ZendeskIdentityStorage.java
				zendesk/core/ZendeskMachineIdStorage.java
				zendesk/core/ZendeskStorage.java
				zendesk/support/CreateRequest.java
				zendesk/support/LegacyRequestMigrator.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	[App can read/write to External Storage. Any App can read data written to External Storage.](#)	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	zendesk/support/ZendeskArticleVoteStorage.java zendesk/support/ZendeskHelpCenterSettingsProvider.java zendesk/support/ZendeskRequestStorage.java zendesk/support/ZendeskSupportSettingsProvider.java zendesk/support/requestlist/RequestListModel.java zendesk/support/requestlist/RequestListView.java com/epic/patientengagement/core/utilities/DeviceUtil.java com/epic/patientengagement/core/utilities/file/FileChooserType.java com/epic/patientengagement/core/utilities/file/FileUtil.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnativecommunity/webview/RNCWebViewModuleImpl.java com/zipow/annotate/AnnoUtil.java com/zipow/cmmlib/AppUtil.java epic/mychart/android/library/utilities/DeviceUtil.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/sentry/android/core/DeviceInfoUtil.java us/zoom/libtools/utils/ZmDeviceUtils.java us/zoom/proguard/ez1.java us/zoom/proguard/gh0.java us/zoom/proguard/k15.java us/zoom/proguard/kx0.java us/zoom/proguard/l93.java us/zoom/proguard/mx4.java us/zoom/proguard/ph0.java us/zoom/proguard/qa2.java us/zoom/proguard/wl1.java us/zoom/videomeetings/richtext/ZMRichTextUtil.java us/zoom/zimmsg/chatlist/MMChatsListFragment.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	[Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.](#)	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/epic/patientengagement/core/mychartweb/MyChartWebViewFragment.java com/stripe/hcaptcha/webview/HCaptchaWebViewHelper.java epic/mychart/android/library/prelogin/AccountManagementWebViewActivity.java us/zoom/proguard/wl1.java
6	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/airbnb/android/react/maps/AirMapModule.java com/airbnb/android/react/maps/FileUtil.java com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/utilities/file/FileUtil.java com/epic/patientengagement/pdfviewer/pdf/PdfFile.java com/reactnativecommunity/webview/RNCWebViewModuleImpl.java com/zipow/videobox/MMShareActivity.java epic/mychart/android/library/customviews/PdfViewerActivity.java epic/mychart/android/library/utilities/k.java io/sentry/react/RNSentryModuleImpl.java us/zoom/proguard/jq0.java us/zoom/proguard/nc4.java us/zoom/proguard/oo0.java us/zoom/proguard/ri0.java us/zoom/zmsg/fragment/MMChatInputFragment.java us/zoom/zmsg/view/mm/VoiceRecordView.java us/zoom/zmsg/view/mm/VoiceTalkView.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/airbnb/lottie/network/NetworkCache.java com/stripe/hcaptcha/webview/HCaptchaDebugInfo.java epic/mychart/android/library/utilities/k.java expo/modules/asset/AssetModule.java expo/modules/filesystem/FileSystemModule.java us/zoom/proguard/cu0.java us/zoom/proguard/l93.java us/zoom/proguard/n32.java us/zoom/proguard/z75.java
8	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/nimbusds/jose/jwk/Curve.java us/zoom/proguard/ao.java us/zoom/proguard/l34.java us/zoom/proguard/n32.java
9	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java
10	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	us/zoom/proguard/n32.java zendesk/chat/BaseModule.java zendesk/chat/ChatVisitorClient.java zendesk/core/ZendeskNetworkModule.java zendesk/support/SupportSdkModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/epic/patientengagement/homepage/itemfeed/webservice/items/ZeroStateFeedItem.java com/epic/patientengagement/todo/models/QuestionnaireSeries.java com/zipow/videobox/conference/ui/controller/SymbioticActivityController.java epic/mychart/android/library/utilities/r.java org/kaazing/gateway/client/impl/wsn/WebSocketNativeEncoderImpl.java org/kaazing/gateway/client/transport/ws/WebSocketDelegateImpl.java zendesk/chat/Utils.java
12	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	com/epic/patientengagement/core/utilities/EncryptionUtil.java io/sentry/util/StringUtils.java org/kaazing/gateway/client/transport/ws/WebSocketDelegateImpl.java
13	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/zipow/videobox/ZoomApplication.java us/zoom/proguard/um4.java
14	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/RootChecker.java
15	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/DeviceInfoUtil.java io/sentry/android/core/internal/util/RootChecker.java us/zoom/proguard/ym4.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
16	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	com/epic/patientengagement/core/utilities/EncryptionUtil.java com/nimbusds/jose/crypto/impl/AESCBC.java com/nimbusds/jose/jca/JCASupport.java us/zoom/proguard/sk.java
17	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/epic/patientengagement/core/mychartweb/MyChartWebViewFragment.java

◉ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

🔝 BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
			cl/json/RNShareImpl.java cl/json/social/InstagramShare.java cl/json/social/SingleShareIntent.java com/amazonaws/amplify/rtnpushnotification/PushNotificationAWSPinpointUtilsKt.java com/epic/patientengagement/authentication/login/activities/PreloginInternalWebView

RULE ID	BEHAVIOUR	LABEL	FILES
			Fragment.java com/epic/patientengagement/authentication/login/activities/SAMLLoginActivity.java com/epic/patientengagement/authentication/login/fragments/LongTextDialogFragment.java com/epic/patientengagement/authentication/login/fragments/OrgFragment.java com/epic/patientengagement/authentication/login/utilities/PreloginDeeplinkManager.java com/epic/patientengagement/core/extensibility/ExtensibilityLaunchManager.java com/epic/patientengagement/core/file/FileViewActivity.java com/epic/patientengagement/core/file/FileViewKt.java com/epic/patientengagement/core/mychartweb/MyChartWebViewFragment.java com/epic/patientengagement/core/utilities/IntentUtil.java com/epic/patientengagement/core/utilities/WebUtil.java com/okta/oidc/util/AuthorizationException.java com/stripe/android/financialconnections/FinancialConnectionsSheetActivity.java com/stripe/android/financialconnections/FinancialConnectionsSheetRedirectActivity.java com/stripe/android/financialconnections/FinancialConnectionsSheetViewModel.java com/stripe/android/financialconnections/browser/BrowserManager.java com/stripe/android/financialconnections/ui/FinancialConnectionsSheetNativeActivity$observeViewEffects$1.java com/stripe/android/link/LinkActivityResultKt.java com/stripe/android/link/LinkForegroundActivity.java com/stripe/android/payments/StripeBrowserLauncherViewModel.java com/stripe/android/ui/core/elements/AfterpayClearpayElementUIKt.java com/stripe/android/uicore/text/HtmlKt.java com/stripe/android/view/PaymentAuthWebViewActivityViewModel.java com/stripe/android/view/PaymentAuthWebViewClient.java com/zipow/videobox/JoinByURLActivity.java com/zipow/videobox/LauncherActivity.java com/zipow/videobox/MMShareActivity.java com/zipow/videobox/ZmMainServiceImpl.java com/zipow/videobox/confapp/meeting/confhelper/ZoomRateHelper.java com/zipow/videobox/fragment/AddrBookItemDetailsFragment.java com/zipow/videobox/fragment/MyProfileFragment.java com/zipow/videobox/fragment/PermissionGuideFragment.java com/zipow/videobox/util/NotificationMgr.java com/zipow/videobox/utils/ZmUtils.java com/zipow/videobox/view/sip/sms/PbxSmsTextItemView.java com/zipow/videobox/widget/MeetingsWidget.java epic/mychart/android/library/accountsettings/AccountSettingsActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
			epic/mychart/android/library/campaigns/c.java
			epic/mychart/android/library/community/WebCommunityManageMyAccountsActivity.java
			epic/mychart/android/library/customactivities/JavaScriptWebViewActivity.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	epic/mychart/android/library/customactivities/TitledWebViewActivity.java
			epic/mychart/android/library/general/DeepLinkManager.java
			epic/mychart/android/library/general/FDILauncherActivity.java
			epic/mychart/android/library/general/e.java
			epic/mychart/android/library/healthlinks/l.java
			epic/mychart/android/library/insurance/e.java
			epic/mychart/android/library/letters/WebLettersActivity.java
			epic/mychart/android/library/personalize/c.java
			epic/mychart/android/library/prelogin/AccountManagementWebViewActivity.java
			epic/mychart/android/library/springboard/BaseFeatureType.java
			epic/mychart/android/library/springboard/CustomFeature.java
			epic/mychart/android/library/todo/PatientAssignedQuestionnaireWebViewActivity.java
			epic/mychart/android/library/utilities/CommunityUtil.java
			epic/mychart/android/library/utilities/k.java
			epic/mychart/android/library/welcomewizard/WelcomeWizardWebViewFragmentManager.java
			expo/modules/adapters/react/permissions/PermissionsService.java
			expo/modules/filesystem/FileSystemModule.java
			expo/modules/intentlauncher/IntentLauncherModule.java
			io/invertase/firebase/dynamiclinks/ReactNativeFirebaseDynamicLinksModule.java
			us/zoom/internal/impl/b.java
			us/zoom/libtools/utils/ZmMimeTypeUtils.java
			us/zoom/proguard/bn0.java
			us/zoom/proguard/bq3.java
			us/zoom/proguard/ch.java
			us/zoom/proguard/de3.java
			us/zoom/proguard/di4.java
			us/zoom/proguard/e21.java
			us/zoom/proguard/ep.java
			us/zoom/proguard/eq0.java
			us/zoom/proguard/fk.java
			us/zoom/proguard/fk1.java
			us/zoom/proguard/hi1.java
			us/zoom/proguard/k15.java
			us/zoom/proguard/k55.java
			us/zoom/proguard/ku1.java

RULE ID	BEHAVIOUR	LABEL	FILES
			us/zoom/proguard/l22.java
			us/zoom/proguard/lc4.java
			us/zoom/proguard/nc1.java
			us/zoom/proguard/nh.java
			us/zoom/proguard/no3.java
			us/zoom/proguard/oo0.java
			us/zoom/proguard/ou1.java
			us/zoom/proguard/qh3.java
			us/zoom/proguard/rg2.java
			us/zoom/proguard/u03.java
			us/zoom/proguard/v74.java
			us/zoom/proguard/vi0.java
			us/zoom/proguard/xr2.java
			us/zoom/proguard/xv1.java
			us/zoom/zapp/fragment/ZappUIComponent.java
			us/zoom/zapp/misc/BasicModeUIMgr.java
			us/zoom/zclips/ui/recording/ZClipsRecordingPage.java
			us/zoom/zimmsg/comm/MMCommMsgListFragment.java
			us/zoom/zimmsg/contacts/ShowMyQrCodeFragment.java
			us/zoom/zimmsg/filecontent/MMSessionFilesFragment.java
			us/zoom/zimmsg/fragment/IMShareInviteDialog.java
			us/zoom/zimmsg/view/mm/MMMessageRemoveHistory.java
			us/zoom/zmsg/fragment/MMChatInputFragment.java
			us/zoom/zmsg/fragment/a.java
			us/zoom/zmsg/markdown/a.java
			us/zoom/zmsg/mediaplayer/ZMMediaPlayerActivity.java
			us/zoom/zmsg/view/mm/MMContentFileViewerFragment.java
			us/zoom/zmsg/view/mm/f.java
			us/zoom/zmsg/view/mm/message/MessageRemoveHistoryView.java
			us/zoom/zmsg/view/mm/message/i0.java
			zendesk/answerbot/AnswerBotArticleActivity.java
			zendesk/classic/messaging/ui/UtilsAttachment.java
			zendesk/support/guide/ViewArticleActivity.java
			zendesk/support/request/ComponentInputForm.java
			zendesk/support/requestlist/RequestListView.java
			cl/json/RNSharePathUtil.java
			cl/json/ShareFile.java
			cl/json/ShareFiles.java
			com/airbnb/lottie/LottieCompositionFactory.java

RULE ID	BEHAVIOUR	LABEL	FILES
			com/airbnb/lottie/network/NetworkCache.java
			com/airbnb/lottie/network/NetworkFetcher.java
			com/epic/patientengagement/core/utilities/DeviceUtil.java
			com/microsoft/codepush/react/CodePush.java
			com/microsoft/codepush/react/CodePushUpdateUtils.java
			com/microsoft/codepush/react/CodePushUtils.java
			com/microsoft/codepush/react/FileUtils.java
			com/oblador/vectoricons/VectorIconsModuleImpl.java
			com/zipow/annotate/AnnoUtil.java
			com/zipow/cmmlib/AppContext.java
			com/zipow/videobox/CameraActivity.java
			com/zipow/videobox/VideoBoxApplication.java
			com/zipow/videobox/broadcast/ZmPtBroadCastReceiver.java
			com/zipow/videobox/config/ConfigWriter.java
			com/zipow/videobox/stabilility/StabilityService.java
			com/zipow/videobox/utils/ZmUtils.java
			com/zipow/videobox/view/mm/a.java
			com/zipow/videobox/view/ptvideo/PBXVideoRecordActivity.java
			epic/mychart/android/library/customviews/VideoPlayerActivity.java
			epic/mychart/android/library/messages/Attachment.java
			expo/modules/filesystem/FileSystemModule.java
			io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java
			io/sentry/DirectoryProcessor.java
			io/sentry/EnvelopeSender.java
			io/sentry/OutboxSender.java
			io/sentry/PreviousSessionFinalizer.java
			io/sentry/SentryOptions.java
			io/sentry/android/core/AndroidOptionsInitializer.java
			io/sentry/android/core/DeviceInfoUtil.java
			io/sentry/android/core/cache/AndroidEnvelopeCache.java
			io/sentry/android/replay/ReplayCache.java
			io/sentry/android/replay/capture/BufferCaptureStrategy.java
			io/sentry/cache/CacheStrategy.java
			io/sentry/cache/CacheUtils.java
			io/sentry/cache/EnvelopeCache.java
			io/sentry/instrumentation/file/FileIOSpanManager.java
			io/sentry/react/RNSentryModuleImpl.java
00022	Open a file from given absolute path of the file	file	org/altbeacon/beacon/service/ScanState.java
			us/zoom/apm/stats/ZMStats.java
			us/zoom/libtools/utils/ZmMimeTypeUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
			us/zoom/proguard/ax1.java us/zoom/proguard/be3.java us/zoom/proguard/bu2.java us/zoom/proguard/f93.java
			us/zoom/proguard/gh0.java us/zoom/proguard/in1.java us/zoom/proguard/j5.java us/zoom/proguard/jh0.java us/zoom/proguard/jt1.java us/zoom/proguard/k04.java us/zoom/proguard/k15.java us/zoom/proguard/k93.java us/zoom/proguard/kx0.java us/zoom/proguard/l93.java us/zoom/proguard/my2.java us/zoom/proguard/ns.java us/zoom/proguard/oh.java us/zoom/proguard/ol2.java us/zoom/proguard/ph0.java us/zoom/proguard/qa2.java us/zoom/proguard/ql.java us/zoom/proguard/uf3.java us/zoom/proguard/ul0.java us/zoom/proguard/wj0.java us/zoom/proguard/yl2.java us/zoom/proguard/z75.java us/zoom/zimmsg/chatlist/MMChatsListFragment.java us/zoom/zimmsg/contacts/ShowMyQrCodeFragment.java us/zoom/zimmsg/reminder/MMRemindersFragment.java us/zoom/zmsg/fragment/MMChatInputFragment.java us/zoom/zmsg/fragment/a.java us/zoom/zmsg/ptapp/trigger/ZoomMessenger.java us/zoom/zmsg/util/ImagePickHelper.java us/zoom/zmsg/view/mm/MMContentFileViewerFragment.java us/zoom/zmsg/view/mm/f.java us/zoom/zmsg/view/mm/message/i.java zendesk/core/MediaFileResolver.java zendesk/core/ZendeskSessionStorage.java zendesk/support/request/AttachmentUploadService.java zendesk/support/request/CellAttachmentLoadingUtil.java

RULE ID	BEHAVIOUR	LABEL	FILES
			com/airbnb/android/react/lottie/LottieAnimationViewPropertyManager.java com/airbnb/android/react/maps/AirMapLocalTile.java com/airbnb/android/react/maps/AirMapTileProvider.java com/airbnb/android/react/maps/FileUtil.java
00013	Read file and put it into a stream	file	com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/epic/patientengagement/pdfviewer/utilities/FileUtils.java com/jakewharton/disklrucache/DiskLruCache.java com/microsoft/codepush/react/CodePushUpdateUtils.java com/microsoft/codepush/react/FileUtils.java com/nimbusds/jose/util/IOUtils.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/stripe/android/core/networking/FileUploadRequest.java com/zipow/annotate/ImageUtil.java com/zipow/cmmlib/AppContext.java com/zipow/videobox/VideoBoxApplication.java com/zipow/zm2d/Zm2DImageUtil.java epic/mychart/android/library/customobjects/StoredFile.java epic/mychart/android/library/customviews/PhotoViewerActivity.java epic/mychart/android/library/utilities/DeviceUtil.java epic/mychart/android/library/utilities/i.java expo/modules/asset/AssetModule.java expo/modules/core/logging/PersistentFileLog.java expo/modules/filesystem/FileSystemModule.java io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/PreviousSessionFinalizer.java io/sentry/android/core/SentryPerformanceProvider.java io/sentry/android/replay/ReplayCache.java io/sentry/cache/CacheStrategy.java io/sentry/cache/CacheUtils.java io/sentry/cache/EnvelopeCache.java io/sentry/config/FilesystemPropertiesLoader.java io/sentry/instrumentation/file/FileInputStreamInitData.java io/sentry/instrumentation/file/SentryFileInputStream.java io/sentry/util/FileUtils.java okio/Okio__JvmOkioKt.java

RULE ID	BEHAVIOUR	LABEL	FILES
			org/altbeacon/beacon/distance/ModelSpecificDistanceCalculator.java
			org/altbeacon/beacon/service/MonitoringStatus.java
			org/altbeacon/beacon/service/ScanState.java
			us/zoom/proguard/bh.java
			us/zoom/proguard/bu2.java
			us/zoom/proguard/ce1.java
			us/zoom/proguard/g93.java
			us/zoom/proguard/gc1.java
			us/zoom/proguard/j5.java
			us/zoom/proguard/jh0.java
			us/zoom/proguard/jt1.java
			us/zoom/proguard/k04.java
			us/zoom/proguard/k93.java
			us/zoom/proguard/kg2.java
			us/zoom/proguard/l93.java
			us/zoom/proguard/o32.java
			us/zoom/proguard/ph0.java
			us/zoom/proguard/r3.java
			us/zoom/proguard/r51.java
			us/zoom/proguard/ss2.java
			us/zoom/proguard/t9.java
			us/zoom/proguard/ul0.java
			us/zoom/proguard/um4.java
			us/zoom/proguard/wt2.java
			us/zoom/zimmsg/chatlist/MMChatsListFragment.java
			us/zoom/zimmsg/reminder/MMRemindersFragment.java
			us/zoom/zmsg/view/ZMFileReaderView.java
			us/zoom/zmsg/view/mm/MMContentFileViewerFragment.java
			us/zoom/zmsg/view/mm/VoiceTalkRecordView.java
			us/zoom/zmsg/view/mm/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/epic/patientengagement/authentication/login/fragments/LoginFragment.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.java com/okta/oidc/OktaAuthenticationActivity.java com/stripe/android/link/LinkForegroundActivity.java com/wix/reactnativenotifications/core/NotificationIntentAdapter.java com/zipow/videobox/IMActivity.java com/zipow/videobox/conference/ui/view/share/ZmBaseShareView.java com/zipow/videobox/fragment/IMAddrBookListFragment.java com/zipow/videobox/fragment/SettingAboutFragment.java epic/mychart/android/library/appointments/FutureAppointmentFragment.java epic/mychart/android/library/billing/PaymentConfirmationActivity.java epic/mychart/android/library/billing/RecentStatementActivity.java epic/mychart/android/library/healthadvisories/HealthAdvisoryMarkCompleteActivity.java epic/mychart/android/library/medications/MedRefillActivity.java epic/mychart/android/library/messages/ComposeActivity.java epic/mychart/android/library/personalize/PersonalizeFragment.java epic/mychart/android/library/springboard/CustomWebModeJumpActivity.java epic/mychart/android/library/testresults/TestResultDetailActivity.java us/zoom/proguard/e40.java us/zoom/proguard/jt1.java us/zoom/proguard/k72.java us/zoom/proguard/rn0.java us/zoom/proguard/u03.java us/zoom/zimmsg/filecontent/MMSessionFilesFragment.java us/zoom/zimmsg/filecontent/a.java us/zoom/zimmsg/reminder/MMRemindersFragment.java us/zoom/zmsg/fragment/MMChatInputFragment.java us/zoom/zmsg/fragment/a.java us/zoom/zmsg/view/mm/MMContentFileViewerFragment.java us/zoom/zmsg/view/mm/f.java
			cl/json/social/InstagramShare.java com/amazonaws/amplify/rtnpushnotification/PushNotificationAWSPinpointUtilsKt.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/epic/patientengagement/authentication/login/activities/PreloginInternalWebViewFragment.java com/stripe/android/financialconnections/FinancialConnectionsSheetRedirectActivity.java com/stripe/android/financialconnections/browser/BrowserManager.java com/stripe/android/link/LinkForegroundActivity.java com/stripe/android/payments/StripeBrowserLauncherViewModel.java com/stripe/android/uicore/text/HtmlKt.java com/zipow/videobox/ZmMainServiceImpl.java com/zipow/videobox/confapp/meeting/confhelper/ZoomRateHelper.java com/zipow/videobox/fragment/AddrBookItemDetailsFragment.java com/zipow/videobox/fragment/MyProfileFragment.java com/zipow/videobox/view/sip/sms/PbxSmsTextItemView.java com/zipow/videobox/widget/MeetingsWidget.java epic/mychart/android/library/accountsettings/AccountSettingsActivity.java epic/mychart/android/library/springboard/BaseFeatureType.java epic/mychart/android/library/utilities/k.java expo/modules/adapters/react/permissions/PermissionsService.java expo/modules/intentlauncher/IntentLauncherModule.java us/zoom/internal/impl/b.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/ch.java us/zoom/proguard/e21.java us/zoom/proguard/k15.java us/zoom/proguard/nc1.java us/zoom/proguard/nh.java us/zoom/proguard/no3.java us/zoom/proguard/qh3.java us/zoom/zapp/fragment/ZappUIComponent.java us/zoom/zapp/misc/BasicModeUIMgr.java us/zoom/zimmsg/comm/MMCommMsgListFragment.java us/zoom/zimmsg/contacts/ShowMyQrCodeFragment.java us/zoom/zimmsg/fragment/IMShareInviteDialog.java us/zoom/zmsg/fragment/MMChatInputFragment.java us/zoom/zmsg/fragment/a.java us/zoom/zmsg/view/mm/f.java us/zoom/zmsg/view/mm/message/i0.java zendesk/classic/messaging/ui/UtilsAttachment.java zendesk/support/guide/ViewArticleActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00125	Check if the given file path exist	file	com/epic/patientengagement/core/pdfviewer/PdfFragment.java com/epic/patientengagement/pdfviewer/PdfViewerFragment.java com/zipow/videobox/CallingActivity.java com/zipow/videobox/VideoBoxApplication.java com/zipow/videobox/fragment/AddrBookItemDetailsFragment.java com/zipow/videobox/fragment/MyProfileFragment.java com/zipow/videobox/fragment/PermissionGuideFragment.java com/zipow/videobox/ptapp/PTUI.java com/zipow/videobox/view/mm/a.java com/zipow/videobox/view/ptvideo/PBXVideoRecordActivity.java expo/modules/filesystem/FileSystemModule.java us/zoom/proguard/b51.java us/zoom/proguard/bq3.java us/zoom/proguard/de3.java us/zoom/proguard/gc1.java us/zoom/proguard/gh0.java us/zoom/proguard/jt1.java us/zoom/proguard/nc4.java us/zoom/proguard/oo0.java us/zoom/zapp/jni/common/ZappCallBackUIImpl.java us/zoom/zimmsg/chatlist/MMChatsListFragment.java us/zoom/zimmsg/chats/session/b.java us/zoom/zmsg/fragment/MMChatInputFragment.java us/zoom/zmsg/fragment/a.java us/zoom/zmsg/ptapp/callback/ZoomBaseMessengerUI.java us/zoom/zmsg/ptapp/trigger/ZoomMessenger.java us/zoom/zmsg/view/mm/MMContentFileViewerFragment.java us/zoom/zmsg/view/mm/b.java us/zoom/zmsg/view/mm/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00056	Modify voice volume	control	org/webrtc/voiceengine/AudioDeviceAndroid.java org/webrtc/voiceengine/AudioDeviceAndroidOpenSLESHelper.java us/zoom/proguard/gc1.java us/zoom/proguard/jt1.java us/zoom/proguard/oo2.java us/zoom/zimmsg/reminder/MMRemindersFragment.java us/zoom/zmsg/util/MMAudioMessagePlayer.java us/zoom/zmsg/view/mm/f.java
00012	Read data and put it into a buffer stream	file	com/microsoft/codepush/react/FileUtils.java epic/mychart/android/library/utilities/i.java io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/cache/CacheStrategy.java io/sentry/cache/EnvelopeCache.java io/sentry/config/FilesystemPropertiesLoader.java io/sentry/util/FileUtils.java us/zoom/proguard/bh.java us/zoom/proguard/kg2.java us/zoom/proguard/l93.java us/zoom/proguard/r3.java us/zoom/proguard/wt2.java
00112	Get the date of the calendar event	collection calendar	com/zipow/videobox/view/schedule/ZmScheduleTimeAndRecurringLayout.java epic/mychart/android/library/healthlinks/HealthDataSyncService.java epic/mychart/android/library/healthlinks/b.java epic/mychart/android/library/healthlinks/k.java us/zoom/proguard/vq0.java us/zoom/proguard/xq0.java us/zoom/proguard/zz4.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/webview/CoreWebViewDownloadManager$download$2.java com/okta/oidc/net/HttpClientImpl.java com/oktareactnative/HttpClientImpl.java com/prove/sdk/mobileauth/internal/http/AndroidHttpClient.java com/prove/sdk/mobileauth/rest/AbstractRestClient.java com/stripe/android/core/networking/ConnectionFactory.java com/stripe/android/stripe3ds2/transaction/StripeHttpClient.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/utilities/g.java io/sentry/transport/HttpConnection.java org/kaazing/gateway/client/transport/http/HttpRequestDelegateImpl.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/webservice/WebServiceTask.java com/epic/patientengagement/core/webview/CoreWebViewDownloadManager$download$2.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.java com/microsoft/codepush/react/CodePushUpdateManager.java com/nimbusds/jose/util/DefaultResourceRetriever.java com/okta/oidc/net/HttpClientImpl.java com/oktareactnative/HttpClientImpl.java com/prove/sdk/mobileauth/internal/http/AndroidHttpClient.java com/stripe/android/stripe3ds2/transaction/StripeHttpClient.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/utilities/g.java io/sentry/transport/HttpConnection.java org/altbeacon/beacon/distance/DistanceConfigFetcher.java org/kaazing/gateway/client/transport/http/HttpRequestDelegateImpl.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/webservice/WebServiceTask.java com/epic/patientengagement/onboarding/views/OrgTermsConditionsView.java com/okta/oidc/net/HttpClientImpl.java com/oktareactnative/HttpClientImpl.java com/prove/sdk/mobileauth/internal/http/AndroidHttpClient.java com/prove/sdk/mobileauth/rest/AbstractRestClient.java com/stripe/android/stripe3ds2/transaction/StripeHttpClient.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java epic/mychart/android/library/utilities/g.java io/sentry/transport/HttpConnection.java org/kaazing/gateway/client/transport/http/HttpRequestDelegateImpl.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java com/epic/patientengagement/core/webservice/WebServiceTask.java com/epic/patientengagement/core/webview/CoreWebViewDownloadManager$download$2.java com/nimbusds/jose/util/DefaultResourceRetriever.java com/okta/oidc/net/HttpClientImpl.java com/oktareactnative/HttpClientImpl.java com/prove/sdk/mobileauth/internal/http/AndroidHttpClient.java com/prove/sdk/mobileauth/rest/AbstractRestClient.java com/stripe/android/payments/core/authentication/RealRedirectResolver.java com/stripe/android/stripe3ds2/transaction/StripeHttpClient.java epic/mychart/android/library/customactivities/TitledWebViewActivity.java io/sentry/transport/HttpConnection.java org/altbeacon/beacon/distance/DistanceConfigFetcher.java org/kaazing/gateway/client/transport/http/HttpRequestDelegateImpl.java

RULE ID	BEHAVIOUR	LABEL	FILES
00094	Connect to a URL and read data from it	command network	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java epic/mychart/android/library/healthlinks/d.java org/kaazing/gateway/client/transport/http/HttpRequestDelegateImpl.java us/zoom/core/model/a.java
00108	Read the input stream from given URL	network command	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java epic/mychart/android/library/customobjects/a.java org/kaazing/gateway/client/transport/http/HttpRequestDelegateImpl.java
00024	Write file after Base64 decoding	reflection file	cl/json/ShareFile.java cl/json/ShareFiles.java com/airbnb/lottie/LottieCompositionFactory.java epic/mychart/android/library/messages/Attachment.java expo/modules/filesystem/FileSystemModule.java us/zoom/proguard/wl1.java
00183	Get current camera parameters and change the setting.	camera	com/zipow/nydus/camera/CameraCaptureImplV1.java com/zipow/nydus/camera/CameraMgrV1.java us/zoom/proguard/r8.java us/zoom/proguard/t8.java
00075	Get location of the device	collection location	us/zoom/proguard/aw4.java
00137	Get last known location of the device	location collection	us/zoom/proguard/aw4.java
00187	Query a URI and check the result	collection sms calllog calendar	us/zoom/core/data/preference/a.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/m7.java us/zoom/proguard/o23.java

RULE ID	BEHAVIOUR	LABEL	FILES
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java us/zoom/core/data/preference/a.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/l93.java us/zoom/proguard/m7.java us/zoom/proguard/o23.java zendesk/support/request/MediaResultUtility.java

RULE ID	BEHAVIOUR	LABEL	FILES
00036	Get resource file from res/raw directory	reflection	cl/json/RNSharePathUtil.java com/airbnb/android/react/maps/AirMapMarker.java com/airbnb/android/react/maps/ImageReader.java com/amazonaws/amplify/rtnpushnotification/PushNotificationAWSPinpointUtilsKt.java com/davemorrissey/labs/subscaleview/SubsamplingScaleImageView.java com/wix/reactnativenotifications/core/notification/NotificationChannel.java com/zipow/videobox/confapp/meeting/confhelper/ZoomRateHelper.java com/zipow/videobox/util/NotificationMgr.java com/zipow/videobox/utils/ZmUtils.java com/zipow/videobox/widget/MeetingsWidget.java epic/mychart/android/library/accountsettings/AccountSettingsActivity.java epic/mychart/android/library/prelogin/WebServer.java epic/mychart/android/library/springboard/BaseFeatureType.java epic/mychart/android/library/springboard/CustomFeature.java epic/mychart/android/library/utilities/k.java expo/modules/adapters/react/permissions/PermissionsService.java expo/modules/filesystem/FileSystemModule.java expo/modules/intentlauncher/IntentLauncherModule.java io/invertase/firebase/common/SharedUtils.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/bn0.java us/zoom/proguard/di4.java us/zoom/proguard/eq0.java us/zoom/proguard/hh2.java us/zoom/proguard/hz4.java us/zoom/proguard/j5.java us/zoom/proguard/k15.java us/zoom/proguard/l93.java us/zoom/proguard/lc4.java us/zoom/proguard/qh3.java us/zoom/proguard/v74.java us/zoom/proguard/xr2.java

RULE ID	BEHAVIOUR	LABEL	FILES
00189	Get the content of a SMS message	sms	com/vonovak/Utils.java us/zoom/core/data/preference/a.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/l93.java us/zoom/proguard/o23.java zendesk/support/request/MediaResultUtility.java
00188	Get the address of a SMS message	sms	com/vonovak/Utils.java us/zoom/core/data/preference/a.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/l93.java us/zoom/proguard/o23.java zendesk/support/request/MediaResultUtility.java
00200	Query data from the contact list	collection contact	com/vonovak/Utils.java us/zoom/core/data/preference/a.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/l93.java us/zoom/proguard/o23.java zendesk/support/request/MediaResultUtility.java
00201	Query data from the call log	collection calllog	com/vonovak/Utils.java us/zoom/core/data/preference/a.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/l93.java us/zoom/proguard/o23.java zendesk/support/request/MediaResultUtility.java
00121	Create a directory	file command	com/zipow/videobox/view/mm/a.java expo/modules/filesystem/FileSystemModule.java us/zoom/zapp/jni/common/ZappCallBackUIImpl.java us/zoom/zimmsg/chatlist/MMChatsListFragment.java us/zoom/zmsg/fragment/MMChatInputFragment.java

RULE ID	BEHAVIOUR	LABEL	FILES
00104	Check if the given path is directory	file	com/zipow/videobox/VideoBoxApplication.java com/zipow/videobox/fragment/SettingAboutFragment.java expo/modules/filesystem/FileSystemModule.java us/zoom/zimmsg/chatlist/MMChatsListFragment.java
00102	Set the phone speaker on	command	com/zipow/videobox/confapp/AudioSessionMgr.java com/zipow/videobox/sip/server/n.java org/webrtc/voiceengine/AudioDeviceAndroid.java org/webrtc/voiceengine/AudioDeviceAndroidAAudio.java org/webrtc/voiceengine/AudioDeviceAndroidOpenSLESHelper.java
00005	Get absolute path of file and put it to JSON object	file	com/airbnb/lottie/LottieCompositionFactory.java com/microsoft/codepush/react/CodePushUtils.java us/zoom/apm/stats/ZMStats.java us/zoom/proguard/ol2.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java us/zoom/proguard/l34.java
00078	Get the network operator name	collection telephony	com/learnium/RNDeviceInfo/RNDeviceModule.java
00038	Query the phone number	collection	com/learnium/RNDeviceInfo/RNDeviceModule.java com/zipow/videobox/sip/server/CmmSIPCallManager.java
00130	Get the current WIFI information	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java us/zoom/proguard/l34.java us/zoom/proguard/ny2.java
00134	Get the current WiFi IP address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java us/zoom/proguard/l34.java

RULE ID	BEHAVIOUR	LABEL	FILES
00082	Get the current WiFi MAC address	collection wifi	com/learnium/RNDeviceInfo/RNDeviceModule.java us/zoom/proguard/l34.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/airbnb/android/react/maps/AirMapTileProvider.java com/airbnb/android/react/maps/ImageUtil.java com/zipow/annotate/ImageUtil.java com/zipow/videobox/CameraActivity.java com/zipow/zm2d/Zm2DImageUtil.java us/zoom/proguard/ph0.java
00191	Get messages in the SMS inbox	sms	com/epic/patientengagement/core/file/FileViewKt.java us/zoom/core/data/preference/a.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/i81.java us/zoom/proguard/l93.java
00092	Send broadcast	command	us/zoom/proguard/qh3.java
00147	Get the time of current location	collection location	com/agontuk/RNFusedLocation/LocationUtils.java
00153	Send binary data over HTTP	http	com/okta/oidc/net/HttpClientImpl.java com/oktareactnative/HttpClientImpl.java epic/mychart/android/library/utilities/g.java
00175	Get notification manager and cancel notifications	notification	com/wix/reactnativenotifications/core/notificationdrawer/PushNotificationsDrawer.java com/zipow/videobox/util/NotificationMgr.java
00192	Get messages in the SMS inbox	sms	cl/json/RNSharePathUtil.java us/zoom/proguard/f93.java us/zoom/proguard/l93.java us/zoom/videomeetings/richtext/ZMRichTextUtil.java

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	org/altbeacon/beacon/distance/ModelSpecificDistanceCalculator.java
00204	Get the default ringtone	collection	us/zoom/proguard/ir3.java us/zoom/proguard/ns.java
00004	Get filename and put it to JSON object	file collection	com/airbnb/lottie/LottieCompositionFactory.java
00199	Stop recording and release recording resources	record	us/zoom/proguard/u12.java
00198	Initialize the recorder and start recording	record	us/zoom/proguard/u12.java
00194	Set the audio source (MIC) and recorded file format	record	us/zoom/proguard/u12.java
00197	Set the audio encoder and initialize the recorder	record	us/zoom/proguard/u12.java
00196	Set the recorded file format and output path	record file	us/zoom/proguard/u12.java
00023	Start another application from current application	reflection control	com/zipow/videobox/auto/ZmAutoMeetingScreen$onClickMeet$1.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	us/zoom/core/data/preference/a.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/l93.java

RULE ID	BEHAVIOUR	LABEL	FILES
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	us/zoom/core/data/preference/a.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/l93.java
00064	Monitor incoming call status	control	com/zipow/videobox/sip/server/n.java us/zoom/proguard/oo2.java
00009	Put data in cursor to JSON object	file	com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java
00209	Get pixels from the latest rendered image	collection	com/zipow/nydus/camera/CameraCaptureImplV2.java com/zipow/videobox/CameraActivity.java us/zoom/proguard/gm1.java us/zoom/proguard/ho4.java
00065	Get the country code of the SIM card provider	collection	us/zoom/proguard/t33.java
00132	Query The ISO country code	telephony collection	us/zoom/proguard/t33.java
00162	Create InetSocketAddress object and connecting to it	socket	org/kaazing/gateway/client/transport/ws/BridgeSocketImpl.java
00163	Create new Socket and connecting to it	socket	org/kaazing/gateway/client/transport/ws/BridgeSocketImpl.java
00033	Query the IMEI number	collection	com/zipow/videobox/sip/server/CmmSIPCallManager.java
00072	Write HTTP input stream into a file	command network file	com/epic/patientengagement/core/pdfviewer/PdfViewModel.java com/epic/patientengagement/core/webview/CoreWebViewDownloadManager$download$2.java com/microsoft/codepush/react/CodePushUpdateManager.java

RULE ID	BEHAVIOUR	LABEL	FILES
00028	Read file from assets directory	file	us/zoom/proguard/k72.java
00208	Capture the contents of the device screen	collection screen	us/zoom/proguard/gm1.java us/zoom/proguard/ho4.java
00043	Calculate WiFi signal strength	collection wifi	com/reactnativecommunity/netinfo/ConnectivityReceiver.java us/zoom/proguard/ny2.java
00016	Get location info of the device and put it to JSON object	location collection	epic/mychart/android/library/location/models/MonitoredForArrivalAppointment.java
00002	Open the camera and take picture	camera	com/zipow/nydus/camera/CameraCaptureImplV1.java
00123	Save the response to JSON after connecting to the remote server	network command	com/prove/sdk/mobileauth/rest/AbstractRestClient.java

🗄 FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://dexcare-2e804.firebaseio.com
App talks to a Firebase database	info	The app talks to Firebase database at https://haiku-push-notifications.firebaseio.com

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/797292586211/namespaces/firebase:fetch?key=AIzaSyDpkQxJzsMEEEacLsY2q6mJwatqsBCBxdU. This is indicated by the response: {'state': 'NO_TEMPLATE'}

⠿ ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/25	android.permission.INTERNET, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.READ_PHONE_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.VIBRATE, android.permission.WAKE_LOCK, android.permission.SYSTEM_ALERT_WINDOW
Other Common Permissions	11/44	android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.CALL_PHONE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.FOREGROUND_SERVICE, android.permission.BLUETOOTH, android.permission.READ_CALENDAR, android.permission.BLUETOOTH_ADMIN, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.CHANGE_NETWORK_STATE, android.permission.BROADCAST_STICKY

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 MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
pinterest.com	ok	**IP:** 151.101.192.84 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
link.com	ok	**IP:** 52.10.212.243 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
merchant-ui-api.stripe.com	ok	**IP:** 44.240.26.72 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
support.link.co	ok	**IP:** 18.238.109.124 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
codepush.appcenter.ms	ok	No Geolocation information available.
widget-mediator.zopim.com	ok	**IP:** 54.218.133.74 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
api.stripe.com	ok	**IP:** 52.26.14.11 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
www.zendesk.com	ok	**IP:** 104.18.34.51 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
plus.google.com	ok	**IP:** 64.233.185.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.logo2.com	ok	**IP:** 13.248.169.48 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
device.payfone.com	ok	**IP:** 74.63.181.56 **Country:** United States of America **Region:** North Carolina **City:** Charlotte **Latitude:** 35.137260 **Longitude:** -80.936119 **View:** Google Map
play.google.com	ok	**IP:** 172.253.124.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.112.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
www.logo1.com	ok	**IP:** 76.223.54.146 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
twitter.com	ok	**IP:** 172.66.0.227 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
errors.stripe.com	ok	**IP:** 198.137.150.161 **Country:** United States of America **Region:** Ohio **City:** Miamisburg **Latitude:** 39.630859 **Longitude:** -84.262108 **View:** Google Map
ichart2.epic.com	ok	**IP:** 199.204.56.101 **Country:** United States of America **Region:** Wisconsin **City:** Madison **Latitude:** 43.073051 **Longitude:** -89.401230 **View:** Google Map
10.0.2.2	ok	**IP:** 10.0.2.2 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
checkout.link.com	ok	**IP:** 18.238.96.79 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
blog.zoom.us	ok	**IP:** 170.114.52.63 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.333698 **Longitude:** -121.889297 **View:** Google Map
www.image.url	ok	No Geolocation information available.
js.hcaptcha.com	ok	**IP:** 104.19.230.21 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
schemas.datacontract.org	ok	**IP:** 207.46.232.160 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
docs.swmansion.com	ok	**IP:** 172.67.142.188 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
zoomus.zendesk.com	ok	**IP:** 216.198.54.2 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
files.stripe.com	ok	**IP:** 54.191.201.88 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
www.logo3.com	ok	**IP:** 195.30.84.13 **Country:** Germany **Region:** Bayern **City:** Munich **Latitude:** 48.137428 **Longitude:** 11.575490 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ppm.stripe.com	ok	**IP:** 35.166.203.173 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
clients3.google.com	ok	**IP:** 108.177.122.139 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
m.stripe.com	ok	**IP:** 52.32.168.38 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
www.image.com	ok	**IP:** 204.236.174.42 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
link.co	ok	**IP:** 13.224.53.87 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map
docs.stripe.com	ok	**IP:** 52.10.212.243 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
www.example.com	ok	**IP:** 23.56.109.241 **Country:** France **Region:** Provence-Alpes-Cote-d'Azur **City:** Marseille **Latitude:** 43.296951 **Longitude:** 5.381070 **View:** Google Map
www.epic.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
haiku-push-notifications.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
rex.webqa.epic.com	ok	No Geolocation information available.
www.cdn.stripe.com	ok	No Geolocation information available.
www.shareeverywhere.com	ok	**IP:** 199.204.56.202 **Country:** United States of America **Region:** Wisconsin **City:** Madison **Latitude:** 43.073051 **Longitude:** -89.401230 **View:** Google Map
www.zoom.us	ok	**IP:** 170.114.52.2 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.333698 **Longitude:** -121.889297 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
static.afterpay.com	ok	**IP:** 104.16.223.179 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.my.froedtert.com	ok	**IP:** 192.227.60.63 **Country:** United States of America **Region:** Wisconsin **City:** Milwaukee **Latitude:** 43.047852 **Longitude:** -88.043373 **View:** Google Map
support.stripe.com	ok	**IP:** 198.137.150.111 **Country:** United States of America **Region:** Ohio **City:** Miamisburg **Latitude:** 39.630859 **Longitude:** -84.262108 **View:** Google Map
www.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
mobilepreview.epic.com	ok	**IP:** 199.204.56.221 **Country:** United States of America **Region:** Wisconsin **City:** Madison **Latitude:** 43.073051 **Longitude:** -89.401230 **View:** [Google Map](#)
ichart1.epic.com	ok	**IP:** 204.187.138.40 **Country:** United States of America **Region:** Wisconsin **City:** Verona **Latitude:** 42.990845 **Longitude:** -89.568443 **View:** [Google Map](#)
b.stripecdn.com	ok	**IP:** 151.101.192.176 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** [Google Map](#)
schemas.microsoft.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
hooks.stripe.com	ok	**IP:** 44.240.26.72 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** [Google Map](#)
www.googleapis.com	ok	**IP:** 173.194.219.95 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)
s3.amazonaws.com	ok	**IP:** 3.5.30.107 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** [Google Map](#)
stripe.com	ok	**IP:** 52.40.139.248 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
www.mychart.org	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **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
schemas.android.com	ok	No Geolocation information available.
support.zoom.us	ok	**IP:** 170.114.46.6 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.333698 **Longitude:** -121.889297 **View:** Google Map
tools.android.com	ok	**IP:** 142.250.105.121 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
altbeacon.github.io	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** [Google Map](#)
www.zoomgov.com	ok	**IP:** 160.1.56.158 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** [Google Map](#)
id.zopim.com	ok	**IP:** 99.80.101.103 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** [Google Map](#)
xmlpull.org	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
www.amazon.com	ok	**IP:** 18.238.90.46 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
shopify.github.io	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
zoom.us	ok	**IP:** 170.114.52.2 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.333698 **Longitude:** -121.889297 **View:** Google Map
dexcare-2e804.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
www.institutionurl.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
r.stripe.com	ok	**IP:** 54.187.159.182 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** [Google Map](#)

✉ EMAILS

EMAIL	FILE
example@example.com	com/zipow/videobox/view/ABItemDetailsList.java
this@zmsettingfragment.getfragmen	com/zipow/videobox/fragment/settings/ZmSettingFragment.java
support@stripe.com	com/stripe/android/core/exception/APIConnectionException.java
support@stripe.com	com/stripe/android/core/networking/ApiRequest.java
support@stripe.com	com/stripe/android/core/frauddetection/FraudDetectionDataRequest.java
test@test.com valid@email.com	com/stripe/android/financialconnections/features/networkinglinksignup/NetworkingLinkSignupPreviewParameterProvider.java
hatcouldbreakalayout@email.com	com/stripe/android/financialconnections/features/networkingsavetolinkverification/NetworkingSaveToLinkVerificationPreviewParameterProvider.java

EMAIL	FILE
hatcouldbreakalayout@email.com	com/stripe/android/financialconnections/features/linkstepupverification/LinkStepUpVerificationPreviewParameterProvider.java
hatcouldbreakalayout@email.com	com/stripe/android/financialconnections/features/networkinglinkverification/NetworkingLinkVerificationPreviewParameterProvider.java
email@test.com	com/stripe/android/financialconnections/features/networkinglinkloginwarmup/NetworkingLinkLoginWarmupPreviewParameterProvider.java
email@email.com	com/stripe/android/paymentsheet/paymentdatacollection/bacs/ComposableSingletons$BacsMandateConfirmationFormKt.java
theop@email.com	com/stripe/android/link/ui/LinkButtonKt.java
email@me.co	com/stripe/android/link/ui/inline/ComposableSingletons$LinkInlineSignupKt.java
email@me.co	com/stripe/android/link/ui/inline/ComposableSingletons$LinkOptionalInlineSignupKt.java
example@example.com user@example.com zdc.pr@zoom.us no-reply@zoom.us support@stripe.com	Android String Resource

🕵 TRACKERS

TRACKER	CATEGORIES	URL
AltBeacon		https://reports.exodus-privacy.eu.org/trackers/219

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"CodePushDeploymentKey" : "PAfbxivQs5qwK-BbM1pLMcemJfI7anepsMIiX"
"GOOGLE_API_KEY" : "AIzaSyA5Sv7kwqJ-jglqBVT9gQWztAbjr020ftI"
"firebase_database_url" : "https://dexcare-2e804.firebaseio.com"
"google_api_key" : "AIzaSyDpkQxJzsMEEEacLsY2q6mJwatqsBCBxdU"
"google_crash_reporting_api_key" : "AIzaSyDpkQxJzsMEEEacLsY2q6mJwatqsBCBxdU"
"google_maps_key" : "AIzaSyA5Sv7kwqJ-jglqBVT9gQWztAbjr020ftI"
"wp_key_preferences_about" : "wp_preference_about"
"wp_key_preferences_allow_all_locales" : "wp_key_preferences_allow_all_locales"
"wp_key_preferences_app_review_header" : "wp_preferences_app_review_header"
"wp_key_preferences_app_review_mode_switch" : "wp_key_preferences_app_review_mode_switch"

POSSIBLE SECRETS
"wp_key_preferences_clear_disc_webview_cache" : "wp_key_preferences_clear_disc_webview_cache"
"wp_key_preferences_clear_ram_webview_cache" : "wp_key_preferences_clear_ram_webview_cache"
"wp_key_preferences_clear_webview_cache" : "wp_key_preferences_clear_webview_cache"
"wp_key_preferences_custom_locale" : "wp_key_preferences_custom_locale"
"wp_key_preferences_custom_phone_book" : "wp_preference_custom_phone_book"
"wp_key_preferences_custom_server" : "wp_preference_custom_server"
"wp_key_preferences_custom_server_switch" : "wp_preference_custom_server_switch"
"wp_key_preferences_enable_webview_cache" : "wp_key_preferences_enable_webview_cache"
"wp_key_preferences_health_connect_switch" : "wp_key_preferences_health_connect_switch"
"wp_key_preferences_health_data_debug_switch" : "wp_key_preferences_health_data_debug_switch"
"wp_key_preferences_screenshots" : "wp_preference_screenshots"
"wp_key_preferences_testing_header" : "wp_preferences_testing_header"
"wp_key_preferences_tool_tip" : "wp_key_preferences_tool_tip"
"wp_key_preferences_webivew_cache_header" : "wp_preferences_webview_cache_header"
"wp_login_password" : "Password"

POSSIBLE SECRETS
"wp_login_username" : "Username"
"wp_share_everywhere_dismiss_token_button_title" : "Dismiss"
"wp_two_factor_authenticate_code_button" : "Verify"
"wp_two_factor_authentication_success_accessibility_announcement" : "Success!"
"zm_deeplink_private_channel_approve_380105" : "Approve"
"zm_deeplink_private_channel_cancel_552125" : "Cancel"
"zm_deeplink_private_channel_decline_380105" : "Decline"
"zm_facebook_live_key_426839" : "facebook"
"zm_fb_workplace_live_key_426839" : "fb_workplace"
"zm_google_private_meeting_317030" : "Busy"
"zm_im_mention_session_link_552428" : "(#%s)"
"zm_im_session_members_external_393577" : "External"
"zm_im_session_members_external_keywords_393577" : "external"
"zm_mm_call_session_list_format" : "[%s]"
"zm_open_app_feature_shortcut_key_304115" : "feature"

POSSIBLE SECRETS

"zm_pbx_private_call_park_brackets_599001" : "(%s)"

"zm_pbx_voicemail_forward_private_330349" : "Private"

"zm_search_authenticate_212554" : "Authenticate"

"zm_sip_sms_session_alert_137657" : "Alert"

"zm_sip_sms_session_member_item_detail_desc_137657" : "Button"

"zm_sip_sms_session_name_other_136896" : "Others"

"zm_twitch_live_key_426839" : "twitch"

"zm_youtube_live_key" : "youtube"

"zm_zapp_guest_mode_promote_authorize_add_dialog_add_519982" : "Add"

FFFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A93AD2CAFFFFFFFFFFFFFFFFFF

DB7C2ABF62E35E668076BEAD2088

POSSIBLE SECRETS

FFFFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DCC4024FFFFFFFFFFFFFFFF

0400FAC9DFCBAC8313BB2139F1BB755FEF65BC391F8B36F8F8EB7371FD558B01006A08A41903350678E58528BEBF8A0BEFF867A7CA36716F7E01F81052

41058363725152142129326129780047268409114441015993725554835256314039467401291

0400D9B67D192E0367C803F39E1A7E82CA14A651350AAE617E8F01CE94335607C304AC29E7DEFBD9CA01F596F927224CDECF6C

3FA8124359F96680B83D1C3EB2C070E5C545C9858D03ECFB744BF8D717717EFC

E95E4A5F737059DC60DFC7AD95B3D8139515620F

FFFFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AACAA68FFFFFFFFFFFFFFFFFF

0620048D28BCBD03B6249C99182B7C8CD19700C362C46A01

2580F63CCFE44138870713B1A92369E33E2135D266DBB372386C400B

74D59FF07F6B413D0EA14B344B20A2DB049B50C3

POSSIBLE SECRETS

26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6

0370F6E9D04D289C4E89913CE3530BFDE903977D42B146D539BF1BDE4E9C92

046AB1E344CE25FF3896424E7FFE14762ECB49F8928AC0C76029B4D5800374E9F5143E568CD23F3F4D7C0D4B1E41C8CC0D1C6ABD5F1A46DB4C

FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3D
F1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB1
82B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9C
E98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B423861285C97FFFFFFFFFFFFFFFFFF

04AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25DBF55296C3A545E3872760AB73617DE4A96262C6F5D9E98BF9292DC29F
8F41DBD289A147CE9DA3113B5F0B8C00A60B1CE1D7E819D7A431D7C90EA0E5F

FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3D
F1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB1
82B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9C
E98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99
C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF6
9EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B
6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1
A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23
BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855
322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C
1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C
6272B045B3B71F9DC6B80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CCFF46AAA36AD004CF600C8381E425A31D951AE64FDB23FCEC
9509D43687FEB69EDD1CC5E0B8CC3BDF64B10EF86B63142A3AB8829555B2F747C932665CB2C0F1CC01BD70229388839D2AF05E454504AC78B7582822846C0BA35C
35F5C59160CC046FD8251541FC68C9C86B022BB7099876A460E7451A8A93109703FEE1C217E6C3826E52C51AA691E0E423CFC99E9E31650C1217B624816CDAD9A95
F9D5B8019488D9C0A0A1FE3075A577E23183F81D4A3F2FA4571EFC8CE0BA8A4FE8B6855DFE72B0A66EDED2FBABFBE58A30FAFABE1C5D71A87E2F741EF8C1FE86FEA
6BBFDE530677F0D97D11D49F7A8443D0822E506A9F4614E011E2A94838FF88CD68C8BB7C5C6424CFFFFFFFFFFFFFFFFFF

1E589A8595423412134FAA2DBDEC95C8D8675E58

POSSIBLE SECRETS

04A1455B334DF099DF30FC28A169A467E9E47075A90F7E650EB6B7A45C7E089FED7FBA344282CAFBD6F7E319F7C0B0BD59E2CA4BDB556D61A5

A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377

MQVwithSHA512KDFAndSharedInfo

0136024004378801593602050S

000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F

266174080205021706322876871672336096072985916875697314770667136841880294499642780849154508062777190235209424122506555866215711354557091681416163731589599846

04B8266A46C55657AC734CE38F018F2192

F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C03

88342353238919216479164875036030888531447659725296036279245086060969839

9cdbd84c9f1ac2f38d0f80f42ab952e7338bf511

115792089210356248762697446949407573529996955224135760342422259061068512044369

2866537B676752636A68F56554E12640276B649EF7526267

FC1217D4320A90452C760A58EDCD30C8DD069B3C34453837A34ED50CB54917E1C2112D84D164F444F8F74786046A

POSSIBLE SECRETS

FFFFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3D
F1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB1
82B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9C
E98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99
C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF6
9EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B
6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1
A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23
BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855
322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C
1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C
6272B045B3B71F9DC6B80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CD0E40E65FFFFFFFFFFFFFFFFFF

91A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C40094DBACDB586FB20

3FCDA526B6CDF83BA1118DF35B3C31761D3545F32728D003EEB25EFE96

3045AE6FC8422F64ED579528D38120EAE12196D5

AC6BDB41324A9A9BF166DE5E1389582FAF72B6651987EE07FC3192943DB56050A37329CBB4A099ED8193E0757767A13DD52312AB4B03310DCD7F48A9DA04FD50E
8083969EDB767B0CF6095179A163AB3661A05FBD5FAAAE82918A9962F0B93B855F97993EC975EEAA80D740ADBF4FF747359D041D5C33EA71D281E446B14773BCA9
7B43A23FB801676BD207A436C6481F1D2B9078717461A5B9D32E688F87748544523B524B0D57D5EA77A2775D2ECFA032CFBDBF52FB3786160279004E57AE6AF874E
7303CE53299CCC041C7BC308D82A5698F3A8D0C38271AE35F8E9DBFBB694B5C803D89F7AE435DE236D525F54759B65E372FCD68EF20FA7111F9E4AFF73

04188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF101207192B95FFC8DA78631011ED6B24CDD573F977A11E794811

10938490380737342745111123907668055699362075989516837489945863944959531161507350160137087375737596232485921322967063133094384525315910
129121423274884789859844

04A8C7DD22CE28268B39B55416F0447C2FB77DE107DCD2A62E880EA53EEB62D57CB4390295DBC9943AB78696FA504C11

64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1

POSSIBLE SECRETS

0101D556572AABAC800101D556572AABAC8001022D5C91DD173F8FB561DA6899164443051D

39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643

F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C00

5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B

07A526C63D3E25A256A007699F5447E32AE456B50E

7503CFE87A836AE3A61B8816E25450E6CE5E1C93ACF1ABC1778064FDCBEFA921DF1626BE4FD036E93D75E6A50E3A41E98028FE5FC235F5B889A589CB5215F2A4

0307AF69989546103D79329FCC3D74880F33BBE803CB

04A3E8EB3CC1CFE7B7732213B23A656149AFA142C47AAFBC2B79A191562E1305F42D996C823439C56D7F7B22E14644417E69BCB6DE39D027001DABE8F35B25C9BE

FFFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3D
F1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB1
82B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9C
E98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99
C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF6
9EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B
6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1
A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E655F6AFFFFFFFFFFFFFFFFFF

790408F2EEDAF392B012EDEFB3392F30F4327C0CA3F31FC383C422AA8C16

3045AE6FC8422f64ED579528D38120EAE12196D5

10686D41FF744D4449FCCF6D8EEA03102E6812C93A9D60B978B702CF156D814EF

POSSIBLE SECRETS

64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1

0257927098FA932E7C0A96D3FD5B706EF7E5F5C156E16B7E7C86038552E91D

0238af09d98727705120c921bb5e9e26296a3cdcf2f35757a0eafd87b830e7

FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551

fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17

2758019355995970587784901184038904809305690585636156852142870730198868924130986086513626076488374510776543976123 0575

0479BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8

00F50B028E4D696E676875615175290472783FB1

ffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632551

678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4

FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C934063199FFFFFFFFFFFFFFFF

662C61C430D84EA4FE66A7733D0B76B7BF93EBC4AF2F49256AE58101FEE92B04

POSSIBLE SECRETS

B4E134D3FB59EB8BAB57274904664D5AF50388BA

02A29EF207D0E9B6C55CD260B306C7E007AC491CA1B10C62334A9E8DCD8D20FB7

040369979697AB43897789566789567F787A7876A65400435EDB42EFAFB2989D51FEFCE3C80988F41FF883

42debb9da5b3d88cc956e08787ec3f3a09bba5f48b889a74aaf53174aa0fbe7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76137e792f3f0db859d095e4a5b932024f079ecf2ef09c797452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94cccf1449ac43d586d0beee43251b0b2287349d68de0d144403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1b27d0639f695e347d8d1cf9ac819a26ca9b04cb0eb9b7b035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffbc97134025fe8ce04c4399ad96569be91a546f4978693c7a

2AA058F73A0E33AB486B0F610410C53A7F132310

4099B5A457F9D69F79213D094C4BCD4D4262210B

040081BAF91FDF9833C40F9C181343638399078C6E7EA38C001F73C8134B1B4EF9E150

91E38443A5E82C0D880923425712B2BB658B9196932E02C78B2582FE742DAA28

A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5374

7d7374168ffe3471b60a857686a19475d3bfa2ff

3826F008A8C51D7B95284D9D03FF0E00CE2CD723A

6db14acc9e21c820ff28b1d5ef5de2b0

985BD3ADBAD4D696E676875615175A21B43A97E3

048BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F046997

POSSIBLE SECRETS

3086d221a7d46bcde86c90e49284eb15

b8adf1378a6eb73409fa6c9c637ba7f5

9760508f15230bccb292b982a2eb840bf0581cf5

AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F0

010092537397ECA4F6145799D62B0A19CE06FE26AD

714114B762F2FF4A7912A6D2AC58B9B5C2FCFE76DAEB7129

6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151

FD0D693149A118F651E6DCE6802085377E5F882D1B510B44160074C1288078365A0396C8E681

E95E4A5F737059DC60DF5991D45029409E60FC09

10E723AB14D696E6768756151756FEBF8FCB49A9

041D1C64F068CF45FFA2A63A81B7C13F6B8847A3E77EF14FE3DB7FCAFE0CBD10E8E826E03436D646AAEF87B2E247D4AF1E8ABE1D7520F9C2A45CB1EB8E95CFD55262B70B29FEEC5864E19C054FF99129280E4646217791811142820341263C5315

044AD5F7048DE709AD51236DE65E4D4B482C836DC6E410664002BB3A02D4AAADACAE24817A4CA3A1B014B5270432DB27D2

020ffa963cdca8816ccc33b8642bedf905c3d358573d3f27fbbd3b3cb9aaaf

6b8cf07d4ca75c88957d9d670591

71FE1AF926CF847989EFEF8DB459F66394D90F32AD3F15E8

POSSIBLE SECRETS

043AE9E58C82F63C30282E1FE7BBF43FA72C446AF6F4618129097E2C5667C2223A902AB5CA449D0084B7E5B3DE7CCC01C9

5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

216EE8B189D291A0224984C1E92F1D16BF75CCD825A087A239B276D3167743C52C02D6E7232AA

3086d221a7d46bcde86c90e49284eb153dab

3E1AF419A269A5F866A7D3C25C3DF80AE979259373FF2B182F49D4CE7E1BBC8B

0021A5C2C8EE9FEB5C4B9A753B7B476B7FD6422EF1F3DD674761FA99D6AC27C8A9A197B272822F6CD57A55AA4F50AE317B13545F

0402FE13C0537BBC11ACAA07D793DE4E6D5E5C94EEE80289070FB05D38FF58321F2E800536D538CCDAA3D9

262470350957996892686231567445669818918529234911092133878156159009255188547380500890223880539757197866508724767320877

5667676A654B20754F356EA92017D946567C46675556F19556A04616B567D223A5E05656FB549016A96656A557

C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86297

4D696E676875615175985BD3ADBADA21B43A97E2

A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7

0429A0B6A887A983E9730988A68727A8B2D126C44CC2CC7B2A6555193035DC76310804F12E549BDB011C103089E73510ACB275FC312A5DC6B76553F0CA

D35E472036BC4FB7E13C785ED201E065F98FCFA5B68F12A32D482EC7EE8658E98691555B44C59311

POSSIBLE SECRETS

020A601907B8C953CA1481EB10512F78744A3205FD

1A8F7EDA389B094C2C071E3647A8940F3C123B697578C213BE6DD9E6C8EC7335DCB228FD1EDF4A39152CBCAAF8C0398828041055F94CEEEC7E21340780FE41BD

32879423AB1A0375895786C4BB46E9565FDE0B5344766740AF268ADB32322E5C

A59A749A11242C58C894E9E5A91804E8FA0AC64B56288F8D47D51B1EDC4D65444FECA0111D78F35FC9FDD4CB1F1B79A3BA9CBEE83A3F811012503C8117F98E5048B089E387AF6949BF8784EBD9EF45876F2E6A5A495BE64B6E770409494B7FEE1DBB1E4B2BC2A53D4F893D418B7159592E4FFFDF6969E91D770DAEBD0B5CB14C00AD68EC7DC1E5745EA55C706C4A1C5C88964E34D09DEB753AD418C1AD0F4FDFD049A955E5D78491C0B7A2F1575A008CCD727AB376DB6E695515B05BD412F5B8C2F4C77EE10DA48ABD53F5DD498927EE7B692BBBCDA2FB23A516C5B4533D73980B2A3B60E384ED200AE21B40D273651AD6060C13D97FD69AA13C5611A51B9085

71169be7330b3038edb025f1

5E5CBA992E0A680D885EB903AEA78E4A45A469103D448EDE3B7ACCC54D521E37F84A4BDD5B06B0970CC2D2BBB715F7B82846F9A0C393914C792E6A923E2117AB805276A975AADB5261D91673EA9AAFFEECBFA6183DFCB5D3B7332AA19275AFA1F8EC0B60FB6F66CC23AE4870791D5982AAD1AA9485FD8F4A60126FEB2CF05DB8A7F0F09B3397F3937F2E90B9E5B9C9B6EFEF642BC48351C46FB171B9BFA9EF17A961CE96C7E7A7CC3D3D03DFAD1078BA21DA425198F07D2481622BCE45969D9C4D6063D72AB7A0F08B2F49A7CC6AF335E08C4720E31476B67299E231F8BD90B39AC3AE3BE0C6B6CACEF8289A2E2873D58E51E029CAFBD55E6841489AB66B5B4B9BA6E2F784660896AFF387D92844CCB8B69475496DE19DA2E58259B090489AC8E62363CDF82CFD8EF2A427ABCD65750B506F56DDE3B988567A88126B914D7828E2B63A6D7ED0747EC59E0E0A23CE7D8A74C1D2C2A7AFB6A29799620F00E11C33787F7DED3B30E1A22D09F1FBDA1ABBBFBF25CAE05A13F812E34563F99410E73B

040503213F78CA44883F1A3B8162F188E553CD265F23C1567A16876913B0C2AC245849283601CCDA380F1C9E318D90F95D07E5426FE87E45C0E8184698E45962364E34116177DD2259

00E8BEE4D3E2260744188BE0E9C723

FFFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE65381FFFFFFFFFFFFFFFFFF

13353181327272067343385951994831900121794237596784748689948235959936964252873471246159040332773182141032801252925387191478859899310331056774413619636480306472137782665689868646846327771015080940118260877020161532499046833293129492091277624113787803022435574660628397165937642683267426978088006163152816347588

POSSIBLE SECRETS

B99B99B099B323E02709A4D696E6768756151751

90066455B5CFC38F9CAA4A48B4281F292C260FEEF01FD61037E56258A7795A1C7AD46076982CE6BB956936C6AB4DCFE05E6784586940CA544B9B2140E1EB523F009D20A7E7880E4E5BFA690F1B9004A27811CD9904AF70420EEFD6EA11EF7DA129F58835FF56B89FAA637BC9AC2EFAAB903402229F491D8D3485261CD068699B6BA58A1DDBBEF6DB51E8FE34E8A78E542D7BA351C21EA8D8F1D29F5D5D15939487E27F4416B0CA632C59EFD1B1EB66511A5A0FBF615B766C5862D0BD8A3FE7A0E0DA0FB2FE1FCB19E8F9996A8EA0FCCDE538175238FC8B0EE6F29AF7F642773EBE8CD5402415A01451A840476B2FCEB0E388D30D4B376C37FE401C2A2C2F941DAD179C540C1C8CE030D460C4D983BE9AB0B20F69144C1AE13F9383EA1C08504FB0BF321503EFE43488310DD8DC77EC5B8349B8BFE97C2C560EA878DE87C11E3D597F1FEA742D73EEC7F37BE43949EF1A0D15C3F3E3FC0A8335617055AC91328EC22B50FC15B941D3D1624CD88BC25F3E941FDDC6200689581BFEC416B4B2CB73

03CE10490F6A708FC26DFE8C3D27C4F94E690134D5BFF988D8D28AAEAEDE975936C66BAC536B18AE2DC312CA493117DAA469C640CAF3

9B9F605F5A858107AB1EC85E6B41C8AACF846E86789051D37998F7B9022D759B

AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F3

043B4C382CE37AA192A4019E763036F4F5DD4D7EBB938CF935318FDCED6BC28286531733C3F03C4FEE

79885141663410976897627118935756323747307951916507639758300472692338873533959

90EAF4D1AF0708B1B612FF35E0A2997EB9E9D263C9CE659528945C0D

8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f

00C9BB9E8927D4D64C377E2AB2856A5B16E3EFB7F61D4316AE

8e722de3125bddb05580164bfe20b8b432216a62926c57502ceede31c47816edd1e89769124179d0b695106428815065

D6031998D1B3BBFEBF59CC9BBFF9AEE1

2762c874eafb8e94376855402628e842

POSSIBLE SECRETS

b3fb3400dec5c4adceb8655d4c94

0401F481BC5F0FF84A74AD6CDF6FDEF4BF6179625372D8C0C5E10025E399F2903712CCF3EA9E3A1AD17FB0B3201B6AF7CE1B05

24B7B137C8A14D696E6768756151756FD0DA2E5C

F1FD178C0B3AD58F10126DE8CE42435B53DC67E140D2BF941FFDD459C6D655E1

030024266E4EB5106D0A964D92C4860E2671DB9B6CC5

10B7B4D696E676875615175137C8A16FD0DA2211

3EE30B568FBAB0F883CCEBD46D3F3BB8A2A73513F5EB79DA66190EB085FFA9F492F375A97D860EB4

9CA8B57A934C54DEEDA9E54A7BBAD95E3B2E91C54D32BE0B9DF96D8D35

D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E24

3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784

03F7061798EB99E238FD6F1BF95B48FEEB4854252B

6b8cf07d4ca75c88957d9d67059037a4

AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA70330870553E5C414CA92619418661197FAC10471DB1D381085DDADDB58796829CA90069

962eddcc369cba8ebb260ee6b6a126d9346e38c5

051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00

POSSIBLE SECRETS

E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B

0202F9F87B7C574D0BDECF8A22E6524775F98CDEBDCB

E0D2EE25095206F5E2A4F9ED229F1F256E79A0E2B455970D8D0D865BD94778C576D62F0AB7519CCD2A1A906AE30D

bb85691939b869c1d087f601554b96b80cb4f55b35f433c2

06973B15095675534C7CF7E64A21BD54EF5DD3B8A0326AA936ECE454D2C

115792089210356248762697446949407573530086143415290314195533631308867097853948

cc22d6dfb95c6b25e49c0d6364a4e5980c393aa21668d953

401028774D7777C7B7666D1366EA432071274F89FF01E718

FFFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA237327FFFFFFFFFFFFFFFF

115792089237316195423570985008687907853269984665640564039457584007908834671663

0481AEE4BDD82ED9645A21322E9C4C6A9385ED9F70B5D916C1B43B62EEF4D0098EFF3B1F78E2D0D48D50D1687B93B97D5F7C6D5047406A5E688B352209BCB9F8227DDE385D566332ECC0EABFA9CF7822FDF209F70024A57B1AA000C55B881F8111B2DCDE494A5F485E5BCA4BD88A2763AED1CA2B2FA8F0540678CD1E0F3AD80892

044A96B5688EF573284664698968C38BB913CBFC8223A628553168947D59DCC912042351377AC5FB32

db92371d2126e9700324977504e8c90e

b869c82b35d70e1b1ff91b28e37a62ecdc34409b

POSSIBLE SECRETS

659EF8BA043916EEDE8911702B22

0452DCB034293A117E1F4FF11B30F7199D3144CE6DFEAFFEF2E331F296E071FA0DF9982CFEA7D43F2E

03E5A88919D7CAFCBF415F07C2176573B2

04026EB7A859923FBC82189631F8103FE4AC9CA2970012D5D46024804801841CA44370958493B205E647DA304DB4CEB08CBBD1BA39494776FB988B47174DCA88C7E2945283A01C89720349DC807F4FBF374F4AEADE3BCA95314DD58CEC9F307A54FFC61EFC006D8A2C9D4979C0AC44AEA74FBEBBB9F772AEDCB620B01A7BA7AF1B320430C8591984F601CD4C143EF1C7A3

D2C0FB15760860DEF1EEF4D696E6768756151754

255705fa2a306654b1f4cb03d6a750a30c250102d4988717d9ba15ab6d3e

32010857077C5431123A46B808906756F543423E8D27877578125778AC76

4D41A619BCC6EADF0448FA22FAD567A9181D37389CA

0017858FEB7A98975169E171F77B4087DE098AC8A911DF7B01

MQVwithSHA256KDFAndSharedInfo

CFA0478A54717B08CE64805B76E5B14249A77A4838469DF7F7DC987EFCCFB11D

469A28EF7C28CCA3DC721D044F4496BCCA7EF4146FBF25C9

aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7

01AF286BCA1AF286BCA1AF286BCA1AF286BCA1AF286BC9FB8F6B85C556892C20A7EB964FE7719E74F490758D3B

41ECE55743711A8C3CBF3783CD08C0EE4D4DC440D4641A8F366E550DFDB3BB67

POSSIBLE SECRETS

85E25BFE5C86226CDB12016F7553F9D0E693A268

77E2B07370EB0F832A6DD5B62DFC88CD06BB84BE

0713612DCDDCB40AAB946BDA29CA91F73AF958AFD9

77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399

04B199B13B9B34EFC1397E64BAEB05ACC265FF2378ADD6718B7C7C1961F0991B842443772152C9E0AD

BB8E5E8FBC115E139FE6A814FE48AAA6F0ADA1AA5DF91985

D09E8800291CB85396CC6717393284AAA0DA64BA

ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n

6BA06FE51464B2BD26DC57F48819BA9954667022C7D03

8d5155894229d5e689ee01e6018a237e2cae64cd

520883949DFDBC42D3AD198640688A6FE13F41349554B49ACC31DCCD884539816F5EB4AC8FB1F1A6

e43bb460f0b80cc0c0b075798e948060f8321b7d

7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9

0418DE98B02DB9A306F2AFCD7235F72A819B80AB12EBD653172476FECD462AABFFC4FF191B946A5F54D8D0AA2F418808CC25AB056962D30651A114AFD2755AD336747F93475B7A1FCA3B88F2B6A208CCFE469408584DC2B2912675BF5B9E582928

POSSIBLE SECRETS

C196BA05AC29E1F9C3C72D56DFFC6154A033F1477AC88EC37F09BE6C5BB95F51C296DD20D1A28A067CCC4D4316A4BD1DCA55ED1066D438C35AEBAABF57E7DAE4
28782A95ECA1C143DB701FD48533A3C18F0FE23557EA7AE619ECACC7E0B51652A8776D02A425567DED36EABD90CA33A1E8D988F0BBB92D02D1D20290113BB562C
E1FC856EEB7CDD92D33EEA6F410859B179E7E789A8F75F645FAE2E136D252BFFAFF89528945C1ABE705A38DBC2D364AADE99BE0D0AAD82E5320121496DC65B3930
E38047294FF877831A16D5228418DE8AB275D7D75651CEFED65F78AFC3EA7FE4D79B35F62A0402A1117599ADAC7B269A59F353CF450E6982D3B1702D9CA83

0443BD7E9AFB53D8B85289BCC48EE5BFE6F20137D10A087EB6E7871E2A10A599C710AF8D0D39E2061114FDD05545EC1CC8AB4093247F77275E0743FFED117182EAA
9C77877AAAC6AC7D35245D1692E8EE1

c103703e120ae8cc73c9248622f3cd1e

00FDFB49BFE6C3A89FACADAA7A1E5BBC7CC1C2E5D831478814

00C9517D06D5240D3CFF38C74B20B6CD4D6F9DD4D9

023b1660dd701d0839fd45eec36f9ee7b32e13b315dc02610aa1b636e346df671f790f84c5e09b05674dbb7e45c803dd

517cc1b727220a94fe13abe8fa9a6ee0

7A1F6653786A68192803910A3D30B2A2018B21CD54

FFFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3D
F1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB1
82B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9C
E98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99
C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF6
9EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B66C62E37FFFFFFFFFFFFFFFFF

1CEF494720115657E18F938D7A7942394FF9425C1458C57861F9EEA6ADBE3BE10

fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f
9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7

POSSIBLE SECRETS

49f946663a8deb7054212b8adda248c6

326705100207588169780830851305070431844712733806592432759389043357573374 82424

95475cf5d93e596c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bbdd84c9836be1f31c0777725aeb6c2fc38b85f48076fa76bcd8146cc89a6fb2f706 dd719898c2083dc8d896f84062e2c9c94d137b054a8d8096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9eb60eee8b030376b236bc 73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520086746175c8885925ebc64c6147906773496990cb714ec 667304e261faee33b3cbdf008e0c3fa90650d97d3909c9275bf4ac86ffcb3d03e6dfc8ada5934242dd6d3bcca2a406cb0b

0217C05610884B63B9C6C7291678F9D341

6C0107475609912222105691 1C77D77E77A777E7E7E77FCB

021085E2755381DCCCE3C1557AFA10C2F0C0C2825646C5B34A394CBCFA8BC16B22E7E789E927BE216F02E1FB136A5F

115792089210356248762697446949407573530086143415290314195533631308867097853951

D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FF

04B6B3D4C356C139EB31183D4749D423958C27D2DCAF98B70164C97A2DD98F5CFF6142E0F7C8B204911F9271F0F3ECEF8C2701C307E8E4C9E183115A1554062CFB

68647976601306097149819007990813932172694353001433054093944634591855431833976553942450577463332171975329639963713633211138647686124403 80340372808892707005449

4A6E0856526436F2F88DD07A341E32D04184572BEB710

03eea2bae7e1497842f2de7769cfe9c989c072ad696f48034a

7F519EADA7BDA81BD826DBA647910F8C4B9346ED8CCDC64E4B1ABD11756DCE1D2074AA263B88805CED70355A33B471EE

7fffffffffffffffffffffff800000cfa7e8594377d414c03821bc582063

POSSIBLE SECRETS

C8619ED45A62E6212E1160349E2BFA844439FAFC2A3FD1638F9E

30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d2029d83c1c1585 47f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346d3f529252

0051953EB9618E1C9A1F929A21A0B68540EEA2DA725B99B315F3B8B489918EF109E156193951EC7E937B1652C0BD3BB1BF073573DF883D2C34F1EF451FD46B503F0 0

BDB6F4FE3E8B1D9E0DA8C0D46F4C318CEFE4AFE3B6B8551F

258EAFA5-E914-47DA-95CA-C5AB0DC85B11

0066647EDE6C332C7F8C0923BB58213B333B20E9CE4281FE115F7D8F90AD

295F9BAE7428ED9CCC20E7C359A9D41A22FCCD9108E17BF7BA9337A6F8AE9513

0340340340340340340340340340340340340340340340340340340323C313FAB50589703B5EC68D3587FEC60D161CC149C1AD4A91

5D9306BACD22B7FAEB09D2E049C6E2866C5D1677762A8F2F2DC9A11C7F7BE8340AB2237C7F2A0

040303001D34B856296C16C0D40D3CD7750A93D1D2955FA80AA5F40FC8DB7B2ABDBDE53950F4C0D293CDD711A35B67FB1499AE60038614F1394ABFA3B4C850D9 27E1E7769C8EEC2D19037BF27342DA639B6DCCFFFEB73D69D78C6C27A6009CBBCA1980F8533921E8A684423E43BAB08A576291AF8F461BB2A8B3531D2F0485C19B 16E2F1516E23DD3C1A4827AF1B8AC15B

1b9fa3e518d683c6b65763694ac8efbaec6fab44f2276171a42726507dd08add4c3b3f4c1ebc5b1222ddba077f722943b24c3edfa0f85fe24d0c8c01591f0be6f63

0095E9A9EC9B297BD4BF36E059184F

1A62BA79D98133A16BBAE7ED9A8E03C32E0824D57AEF72F88986874E5AAE49C27BED49A2A95058068426C2171E99FD3B43C5947C857D

7A556B6DAE535B7B51ED2C4D7DAA7A0B5C55F380

POSSIBLE SECRETS

28E9FA9E9D9F5E344D5A9E4BCF6509A7F39789F515AB8F92DDBCBD414D940E93

25FBC363582DCEC065080CA8287AAFF09788A66DC3A9E

43FC8AD242B0B7A6F3D1627AD5654447556B47BF6AA4A64B0C2AFE42CADAB8F93D92394C79A79755437B56995136

5363ad4cc05c30e0a5261c028812645a122e22ea20816678df02967c1b23bd72

EEAF0AB9ADB38DD69C33F80AFA8FC5E86072618775FF3C0B9EA2314C9C256576D674DF7496EA81D3383B4813D692C6E0E0D5D8E250B98BE48E495C1D6089DAD15
DC7D7B46154D6B6CE8EF4AD69B15D4982559B297BCF1885C529F566660E57EC68EDBC3C05726CC02FD4CBF4976EAA9AFD5138FE8376435B9FC61D2FC0EB06E3

0101BAF95C9723C57B6C21DA2EFF2D5ED588BDD5717E212F9D

9B9F605F5A858107AB1EC85E6B41C8AACF846E86789051D37998F7B9022D7598

9B9F605F5A858107AB1EC85E6B41C8AA582CA3511EDDFB74F02F3A6598980BB9

9177152989655460594558814901838275021729685839352072417274332572547437497980 1

96341f1138933bc2f503fd44

1420117415975634811963682860223180897432761383952437387628725734419274593935127189736311660784676003608489466235676257952827747192122 4
1929071046134208380636394084512691828894000571524625445295769349356752728956831541775441763139384457191755096847107846595662547942312 2
9333848392451433961472776068188060973423 9

A335926AA319A27A1D00896A6773A4827ACDAC73

1AB597A5B4477F59E39539007C7F977D1A567B92B043A49C6B61984C3FE3481AAF454CD41BA1F051626442B3C10

0409487239995A5EE76B55F9C2F098A89CE5AF8724C0A23E0E0FF77500

POSSIBLE SECRETS

6b016c3bdcf18941d0d654921475ca71a9db2fb27d1d37796185c2942c0a

c469684435deb378c4b65ca9591e2a5763059a2e

340E7BE2A280EB74E2BE61BADA745D97E8F7C300

308201e53082014ea00302010202044faa0a6b300d06092a864886f70d01010505003036310b30090603550406130255533127302 5060355040a131e5a6f6f6d20566964656f20436f6d6d756e69636174696f6e7320496e632e3020170d3132303530393036313035315a1 80f32303036323034323732036313035315a3036310b3009060355040613025553312730250 60355040a131e5a6f6f6d20566964656f20436f6d6d756e69636174696f6e7320496e632e30819f300d06092a864886f70d0101010500 03818d00308189028181009b463f2d26827dcd115aecc70e5124b9d68cd78e401489c9eae4cd19bc4ca0576ad28168a81f71e8d8b5a7cdc 956d937510df3cfa956c28d55668894c33ce0805 2946ae4af1455becfd2243897f1731fd17a547260c5a52daaebf8ab8a9aad1ad18f99ff696dcf7d713f6540f102c274fbfbc895045f25af67 d0fe8dedc536510203010001300 d06092a864886f70d0101050500038181000db7990467b840f362bad88c35874abe4d10d3a872356e57581f06fcbac79ebf6d82bb380d14 461eded133d9630d77a6b7bcc 9953f1ab02437c6317646218b6a37f3c75e833096fa24a473a9b53b1cca4269f0c753ec33239c9a293ea87c27121f424cb9ec1d7765c7fc 0c51b7ee2ec4ab9d15a896eeb150 ac06fe67086f1c70

683631961449557007844441656118272528951021708887614420550950512875503140 83023

7CBBBCF9441CFAB76E1890E46884EAE321F70C0BCB4981527897504BEC3E36A62BCDFA2304976540F6450085F2DAE145C22553B465 763689180EA2571867423E

0228F9D04E900069C8DC47A08534FE76D2B900B7D7EF31F5709F200C4CA205

040060F05F658F49C1AD3AB1890F7184210EFD0987E307C84C27ACCFB8F9F67CC2C460189EB5AAAA62EE222EB1B35540CFE90237 4601E369050B7C4E42ACBA1DACB F04299C3460782F918EA427E6325165E9EA10E3DA5F6C42E9C55215AA9CA27A5863EC48D8E0286B

000E0D4D696E6768756151750CC03A4473D03679

F5CE40D95B5EB899ABBCCFF5911CB8577939804D6527378B8C108C3D2090FF9BE18E2D33E3021ED2EF32D85822423B6304F726AA854 BAE07D0396E9A9ADDC40F

7830A3318B603B89E2327145AC234CC594CBDD8D3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72 BF2C7B9E7C1AC4D77FC94CA

3d84f26c12238d7b4f3d516613c1759033b1a5800175d0b1

POSSIBLE SECRETS

2E2F85F5DD74CE983A5C4237229DAF8A3F35823BE

6A91174076B1E0E19C39C031FE8685C1CAE040E5C69A28EF

42941826148615804143873447737955502392672345968607143066798112994089471231420027060385216699563848719957657284814898909770759462613437669456364882730370838934791080835932647976778601915343474400961034231316672578686920482194932878633360203384797092684342247621055760235016132614780652761028509445403338652341

6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148

114ca50f7a8e2f3f657c1108d9d44cfd8

48439561293906451759052585252797914202762949526041747995844080717082404635286

04009D73616F35F4AB1407D73562C10F00A52830277958EE84D1315ED31886

DB7C2ABF62E35E7628DFAC6561C5

07A11B09A76B562144418FF3FF8C2570B8

1A827EF00DD6FC0E234CAF046C6A5D8A85395B236CC4AD2CF32A0CADBDC9DDF620B0EB9906D0957F6C6FEACD615468DF104DE296CD8F

MQVwithSHA384KDFAndSharedInfo

072546B5435234A422E0789675F432C89435DE5242

047B6AA5D85E572983E6FB32A7CDEBC14027B6916A894D3AEE7106FE805FC34B44

E2E31EDFC23DE7BDEBE241CE593EF5DE2295B7A9CBAEF021D385F7074CEA043AA27272A7AE602BF2A7B9033DB9ED3610C6FB85487EAE97AAC5BC7928C1950148

POSSIBLE SECRETS

0432C4AE2C1F1981195F9904466A39C9948FE30BBFF2660BE1715A4589334C74C7BC3736A2F4F6779C59BDCEE36B692153D0A9877CC62A474002DF32E52139F0A0

22123dc2395a05caa7423daeccc94760a7d462256bd56916

9DEF3CAFB939277AB1F12A8617A47BBBDBA51DF499AC4C80BEEEA9614B19CC4D5F4F5F556E27CBDE51C6A94BE4607A291558903BA0D0F84380B655BB9A22E8DCD
F028A7CEC67F0D08134B1C8B97989149B609E0BE3BAB63D47548381DBC5B1FC764E3F4B53DD9DA1158BFD3E2B9C8CF56EDF019539349627DB2FD53D24B7C48665
772E437D6C7F8CE442734AF7CCB7AE837C264AE3A9BEB87F8A2FE9B8B5292E5A021FFF5E91479E8CE7A28C2442C6F315180F93499A234DCF76E3FED135F9BB

04B70E0CBD6BB4BF7F321390B94A03C1D356C21122343280D6115C1D21BD376388B5F723FB4C22DFE6CD4375A05A07476444D5819985007E34

108576C80499DB2FC16EDDF6853BBB278F6B6FB437D9

0163F35A5137C2CE3EA6ED8667190B0BC43ECD69977702709B

03188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012

1854BEBDC31B21B7AEFC80AB0ECD10D5B1B3308E6DBF11C1

04640ECE5C12788717B9C1BA06CBC2A6FEBA85842458C56DDE9DB1758D39C0313D82BA51735CDB3EA499AA77A7D6943A64F7A3F25FE26F06B51BAA2696FA9035D
A5B534BD595F5AF0FA2C892376C84ACE1BB4E3019B71634C01131159CAE03CEE9D9932184BEEF216BD71DF2DADF86A627306ECFF96DBB8BACE198B61E00F8B332

04161FF7528B899B2D0C28607CA52C5B86CF5AC8395BAFEB13C02DA292DDED7A83

FFFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1
356D6D51C245E485B576625E7EC6F44C42E9A63A3620FFFFFFFFFFFFFFFFFF

DB7C2ABF62E35E668076BEAD208B

0401A57A6A7B26CA5EF52FCDB816479700B3ADC94ED1FE674C06E695BABA1D

12511cfe811d0f4e6bc688b4d

POSSIBLE SECRETS

002757A1114D696E6768756151755316C05E0BD4

C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86294

deca87e736574c5c83c07314051fd93a

100997906755055304772081815535925224869841082572053457874823515875577147990529272777244152852699298796483356699682842027972896052747173175480590485607134746852141928680912561502802222185647539190902656116367847270145019066794290930185446216399730872221732889830323194097355403213400972588322876850946740663962

7BC86E2102902EC4D5890E8B6B4981ff27E0482750FEFC03

31a92ee2029fd10d901b113e990710f0d21ac6b6

027d29778100c65a1da1783716588dce2b8b4aee8e228f1896

7BC382C63D8C150C3C72080ACE05AFA0C2BEA28E4FB22787139165EFBA91F90F8AA5814A503AD4EB04A8C7DD22CE2826

EE353FCA5428A9300D4ABA754A44C00FDFEC0C9AE4B1A1803075ED967B7BB73F

010090512DA9AF72B08349D98A5DD4C7B0532ECA51CE03E2D10F3B7AC579BD87E909AE40A6F131E9CFCE5BD967

B4050A850C04B3ABF54132565044B0B7D7BFD8BA270B39432355FFB4

29C41E568B77C617EFE5902F11DB96FA9613CD8D03DB08DA

DC9203E514A721875485A529D2C722FB187BC8980EB866644DE41C68E143064546E861C0E2C9EDD92ADE71F46FCF50FF2AD97F951FDA9F2A2EB6546F39689BD3

0236B3DAF8A23206F9C4F299D7B21A9C369137F2C84AE1AA0D

127971af8721782ecffa3

POSSIBLE SECRETS

036b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

68A5E62CA9CE6C1C299803A6C1530B514E182AD8B0042A59CAD29F43

04DB4FF10EC057E9AE26B07D0280B7F4341DA5D1B1EAE06C7D9B2F2F6D9C5628A7844163D015BE86344082AA88D95E2F9D

5037EA654196CFF0CD82B2C14A2FCF2E3FF8775285B545722F03EACDB74B

7B425ED097B425ED097B425ED097B425ED097B425ED097B4260B5E9C7710C864

11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

13D56FFAEC78681E68F9DEB43B35BEC2FB68542E27897B79

51DEF1815DB5ED74FCC34C85D709

b28ef557ba31dfcbdd21ac46e2a91e3c304f44cb87058ada2cb815151e610046

1f3bdba585295d9a1110d1df1f9430ef8442c5018976ff3437ef91b81dc0b8132c8d5c39c32d0e004a3092b7d327c0e7a4d26d2c7b69b58f9066652911e457779de

5DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2

B4C4EE28CEBC6C2C8AC12952CF37F16AC7EFB6A9F69F4B57FFDA2E4F0DE5ADE038CBC2FFF719D2C18DE0284B8BFEF3B52B8CC7A5F5BF0A3C8D2319A5312557E1

5FF6108462A2DC8210AB403925E638A19C1455D21

03375D4CE24FDE434489DE8746E71786015009E66E38A926DD

POSSIBLE SECRETS

0289FDFBE4ABE193DF9559ECF07AC0CE78554E2784EB8C1ED1A57A

D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E27

7ae96a2b657c07106e64479eac3434e99cf0497512f58995c1396c28719501ee

5506626302227734366957871889516853432625060345377759417550018736 0389116729240

003088250CA6E7C7FE649CE85820F7

FFFFFFFE0000000075A30D1B9038A115

040D9029AD2C7E5CF4340823B2A87DC68C9E4CE3174C1E6EFDEE12C07D58AA56F772C0726F24C6B89E4ECDAC24354B9E99CAA3F6D3761402CD

9ba48cba5ebcb9b6bd33b92830b2a2e0e192f10a

5EEEFCA380D02919DC2C6558BB6D8A5D

04017232BA853A7E731AF129F22FF4149563A419C26BF50A4C9D6EEFAD612601DB537DECE819B7F70F555A67C427A8CD9BF18AEB9B56E0C11056FAE6A3

04C0A0647EAAB6A48753B033C56CB0F0900A2F5C4853375FD614B690866ABD5BB88B5F4828C1490002E6773FA2FA299B8F

E8C2505DEDFC86DDC1BD0B2B6667F1DA34B82574761CB0E879BD081CFD0B6265EE3CB090F30D27614CB4574010DA90DD862EF9D4EBEE4761503190785A71C760

1157920892373161954235709850086879078528375642790749043826051631 41518161494337

394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731 12319

10D9B4A3D9047D8B154359ABFB1B7F5485B04CEB868237DDC9DEDA982A679A5A919B626D4E50A8DD731B107A9962381FB5D807BF2618

POSSIBLE SECRETS

04015D4860D088DDB3496B0C6064756260441CDE4AF1771D4DB01FFE5B34E59703DC255A868A1180515603AEAB60794E54BB7996A70061B1CFAB6BE5F32BBFA783 24ED106A7636B9C5A7BD198D0158AA4F5488D08F38514F1FDF4B4F40D2181B3681C364BA0273C706

5F49EB26781C0EC6B8909156D98ED435E45FD59918

C2173F1513981673AF4892C23035A27CE25E2013BF95AA33B22C656F277E7335

c49d360886e704936a6678e1139d26b7819f7e90

71169be7330b3038edb025f1d0f9

10B51CC12849B234C75E6DD2028BF7FF5C1CE0D991A1

3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CADC083E67984050B75EBAE5DD2809BD638016F723

fe0e87005b4e83761908c5131d552a850b3f58b749c37cf5b84d6768

8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B31F166E6CAC0425A7CF3AB6AF6B7FC3103B883202E9046565

7167EFC92BB2E3CE7C8AAAFF34E12A9C557003D7C73A6FAF003F99F6CC8482E540F7

8325710961489029985546751289520108179287853048861315594709205902480503199884419224438643760392947333078086511627871

023809B2B7CC1B28CC5A87926AAD83FD28789E81E2C9E3BF10

687D1B459DC841457E3E06CF6F5E2517B97C7D614AF138BCBF85DC806C4B289F3E965D2DB1416D217F8B276FAD1AB69C50F78BEE1FA3106EFB8CCBC7C5140116

1243ae1b4d71613bc9f780a03690e

02197B07845E9BE2D96ADB0F5F3C7F2CFFBD7A3EB8B6FEC35C7FD67F26DDF6285A644F740A2614

POSSIBLE SECRETS

8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC50

4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

044BA30AB5E892B4E1649DD0928643ADCD46F5882E3747DEF36E956E97

04BED5AF16EA3F6A4F62938C4631EB5AF7BDBCDBC31667CB477A1A8EC338F94741669C976316DA6321

6EE3CEEB230811759F20518A0930F1A4315A827DAC

9162fbe73984472a0a9d0590

393C7F7D53666B5054B5E6C6D3DE94F4296C0C599E2E2E241050DF18B6090BDC90186904968BB

324A6EDDD512F08C49A99AE0D3F961197A76413E7BE81A400CA681E09639B5FE12E59A109F78BF4A373541B3B9A1

02F40E7E2221F295DE297117B7F3D62F5C6A97FFCB8CEFF1CD6BA8CE4A9A18AD84FFABBD8EFA59332BE7AD6756A66E294AFD185A78FF12AA520E4DE739BACA0C7FFEFF7F2955727A

004D696E67687561517512D8F03431FCE63B88F4

f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a

e8b4011604095303ca3b8099982be09fcb9ae616

B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF

033C258EF3047767E7EDE0F1FDAA79DAEE3841366A132E163ACED4ED2401DF9C6BDCDE98E8E707C07A2239B1B097

POSSIBLE SECRETS

0400C6858E06B70404E9CD9E3ECB662395B4429C648139053FB521F828AF606B4D3DBAA14B5E77EFE75928FE1DC127A2FFA8DE3348B3C1856A429BF97E7E31C2E5B
D66011839296A789A3BC0045C8A5FB42C7D1BD998F54449579B446817AFBD17273E662C97EE72995EF42640C550B9013FAD0761353C7086A272C24088BE94769FD1
6650

2E45EF571F00786F67B0081B9495A3D95462F5DE0AA185EC

BDB6F4FE3E8B1D9E0DA8C0D40FC962195DFAE76F56564677

046B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C2964FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5

6127C24C05F38A0AAAF65C0EF02C

0667ACEB38AF4E488C407433FFAE4F1C811638DF20

038D16C2866798B600F9F08BB4A8E860F3298CE04A5798

07B6882CAAEFA84F9554FF8428BD88E246D2782AE2

BD71344799D5C7FCDC45B59FA3B9AB8F6A948BC5

6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

4E13CA542744D696E67687561517552F279A8C84

16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a

C302F41D932A36CDA7A3462F9E9E916B5BE8F1029AC4ACC1

70B5E1E14031C1F70BBEFE96BDDE66F451754B4CA5F48DA241F331AA396B8D1839A855C1769B1EA14BA53308B5E2723724E090E02DB9

027B680AC8B8596DA5A4AF8A19A0303FCA97FD7645309FA2A581485AF6263E313B79A2F5

POSSIBLE SECRETS

10C0FB15760860DEF1EEF4D696E676875615175D

103FAEC74D696E676875615175777FC5B191EF30

c97445f45cdef9f0d3e05e1e585fc297235b82b5be8ff3efca67c59852018192

c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

4B337D934104CD7BEF271BF60CED1ED20DA14C08B3BB64F18A60888D

3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316

1053CDE42C14D696E67687561517533BF3F83345

b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae466748d9b5a536

C49D360886E704936A6678E1139D26B7819F7E90

b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FC

D7C134AA264366862A18302575D0FB98D116BC4B6DDEBCA3A5A7939F

e4437ed6010e88286f547fa90abfe4c42212

POSSIBLE SECRETS

02120FC05D3C67A99DE161D2F4092622FECA701BE4F50F4758714E8A87BBF2A658EF8C21E7C5EFE965361F6C2999C0C247B0DBD70CE6B7

0108B39E77C4B108BED981ED0E890E117C511CF072

0405F939258DB7DD90E1934F8C70B0DFEC2EED25B8557EAC9C80E2E198F8CDBECD86B1205303676854FE24141CB98FE6D4B20D02B4516FF702350EDDB0826779C813F0DF45BE8112F4

BDDB97E555A50A908E43B01C798EA5DAA6788F1EA2794EFCF57166B8C14039601E55827340BE

026108BABB2CEEBCF787058A056CBE0CFE622D7723A289E08A07AE13EF0D10D171DD8D

e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf

36134250956749795798585127919587881956611106672985015071877198253568414405109

0403F0EBA16286A2D57EA0991168D4994637E8343E3600D51FBC6C71A0094FA2CDD545B11C5C0C797324F1

E87579C11079F43DD824993C2CEE5ED3

dcb428fea25c40e7b99f81ae5981ee6a

36DF0AAFD8B8D7597CA10520D04B

127021248288932417465907042777176443525787653508916535812817507265705031260985098497423188333483401180925999995120988934130659205614996724254121049274349357074920312769561451689224110579311248812610229678534638401693520013288995000362260684222750813532307004517341633685004541062586971416883686778842537820383

13945487119911582560140965510769071310704170705992803179775800145437576535772298409412436852228823983303911468164807668823692122073732267216074074777170091113455043205380464769490468612011308781624074018480047704715733666292624942357124882396854222175366014339148568084052033685945849480318734128858048952516

POSSIBLE SECRETS

00689918DBEC7E5A0DD6DFC0AA55C7

036768ae8e18bb92cfcf005c949aa2c6d94853d0e660bbf854b1c9505fe95a

f8183668ba5fc5bb06b5981e6d8b795d30b8978d43ca0ec572e37e09939a9773

8D91E471E0989CDA27DF505A453F2B7635294F2DDF23E3B122ACC99C9E9F1E14

6A941977BA9F6A435199ACFC51067ED587F519C5ECB541B8E44111DE1D40

A7F561E038EB1ED560B3D147DB782013064C19F27ED27C6780AAF77FB8A547CEB5B4FEF422340353

04925BE9FB01AFC6FB4D3E7D4990010F813408AB106C4F09CB7EE07868CC136FFF3357F624A21BED5263BA3A7A27483EBF6671DBEF7ABB30EBEE084E58A0B077AD42A5A0989D1EE71B1B9BC0455FB0D2C3

60dcd2104c4cbc0be6eeefc2bdd610739ec34e317f9b33046c9e4788

1C97BEFC54BD7A8B65ACF89F81D4D4ADC565FA45

2472E2D0197C49363F1FE7F5B6DB075D52B6947D135D8CA445805D39BC345626089687742B6329E70680231988

E95E4A5F737059DC60DFC7AD95B3D8139515620C

617fab6832576cbbfed50d99f0249c3fee58b94ba0038c7ae84c8c832f2c

0100FAF51354E0E39E4892DF6E319C72C8161603FA45AA7B998A167B8F1E629521

POSSIBLE SECRETS

FFFFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DBE115974A3926F12FEE5E438777CB6A932DF8CD8BEC4D073B931BA3BC832B68D9DD300741FA7BF8AFC47ED2576F6936BA424663AAB639C5AE4F5683423B4742BF1C978238F16CBE39D652DE3FDB8BEFC848AD922222E04A4037C0713EB57A81A23F0C73473FC646CEA306B4BCBC8862F8385DDFA9D4B7FA2C087E879683303ED5BDD3A062B3CF5B3A278A66D2A13F83F44F82DDF310EE074AB6A364597E899A0255DC164F31CC50846851DF9AB48195DED7EA1B1D510BD7EE74D73FAF36BC31ECFA268359046F4EB879F924009438B481C6CD7889A002ED5EE382BC9190DA6FC026E479558E4475677E9AA9E3050E2765694DFC81F56E880B96E7160C980DD98EDD3DFFFFFFFFFFFFFFFFFFF

8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC53

4230017757A767FAE42398569B746325D45313AF0766266479B75654E65F

c39c6c3b3a36d7701b9c71a1f5804ae5d0003f4

040356DCD8F2F95031AD652D23951BB366A80648F06D867940A5366D9E265DE9EB240F

▶ PLAYSTORE INFORMATION

Title: Froedtert & MCW

Score: 4.24 **Installs:** 100,000+ **Price:** 0 **Android Version Support: Category:** Medical **Play Store URL:** com.froedtert.care

Developer Details: Froedtert and Medical College of Wisconsin, Froedtert+and+Medical+College+of+Wisconsin, None, https://www.froedtert.com/virtual-clinic, DigitalSupportTeam@froedtert.com,

Release Date: Mar 23, 2020 **Privacy Policy:** [Privacy link](#)

Description:

Froedtert & the Medical College of Wisconsin app is a digital engagement platform designed to offer easy and same day care access to high quality health services for in person and on-demand visits from Froedtert & Medical College of Wisconsin. With Froedtert & MCW app you can: - Connect with a board certified clinician instantly through video and chat - Book an appointment at any of our FastCare and Ortho Now locations - Connect to your medical records all within the same app using MyChart. - Message and schedule an appointment with your care team. - Review medications, immunization history, and other health information. - Review your COVID-19 vaccination status. - And many other features.

≔ SCAN LOGS

Timestamp	Event	Error
2025-08-29 22:34:52	Generating Hashes	OK
2025-08-29 22:34:53	Extracting APK	OK
2025-08-29 22:34:53	Unzipping	OK
2025-08-29 22:34:59	Parsing APK with androguard	OK
2025-08-29 22:35:00	Extracting APK features using aapt/aapt2	OK
2025-08-29 22:35:01	Getting Hardcoded Certificates/Keystores	OK

2025-08-29 22:35:07	Parsing AndroidManifest.xml	OK
2025-08-29 22:35:07	Extracting Manifest Data	OK
2025-08-29 22:35:07	Manifest Analysis Started	OK
2025-08-29 22:35:07	Reading Network Security config from wp_network_security_config.xml	OK
2025-08-29 22:35:07	Parsing Network Security config	OK
2025-08-29 22:35:07	Performing Static Analysis on: Froedtert&MCW (com.froedtert.care)	OK
2025-08-29 22:35:08	Fetching Details from Play Store: com.froedtert.care	OK
2025-08-29 22:35:09	Checking for Malware Permissions	OK
2025-08-29 22:35:09	Fetching icon path	OK
2025-08-29 22:35:09	Library Binary Analysis Started	OK
2025-08-29 22:35:09	Reading Code Signing Certificate	OK

2025-08-29 22:35:09	Running APKiD 2.1.5	OK
2025-08-29 22:35:14	Detecting Trackers	OK
2025-08-29 22:35:28	Decompiling APK to Java with JADX	OK
2025-08-29 22:36:38	Converting DEX to Smali	OK
2025-08-29 22:36:38	Code Analysis Started on - java_source	OK
2025-08-29 22:36:56	Android SBOM Analysis Completed	OK
2025-08-29 22:40:00	Android SAST Completed	OK
2025-08-29 22:40:00	Android API Analysis Started	OK
2025-08-29 22:43:24	Android API Analysis Completed	OK
2025-08-29 22:43:25	Android Permission Mapping Started	OK
2025-08-29 22:46:33	Android Permission Mapping Completed	OK

2025-08-29 22:46:34	Android Behaviour Analysis Started	OK
2025-08-29 22:49:50	Android Behaviour Analysis Completed	OK
2025-08-29 22:49:50	Extracting Emails and URLs from Source Code	OK
2025-08-29 22:50:31	Email and URL Extraction Completed	OK
2025-08-29 22:50:32	Extracting String data from APK	OK
2025-08-29 22:50:32	Extracting String data from Code	OK
2025-08-29 22:50:32	Extracting String values and entropies from Code	OK
2025-08-29 22:52:49	Performing Malware check on extracted domains	OK
2025-08-29 22:53:00	Saving to Database	OK

Report Generated by - MobSF v4.4.0

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.