

ANDROID STATIC ANALYSIS REPORT



Circle Medical (6.20.2)

| File Name: | co.circlemedical.patient_500.apk |
|---------------------|----------------------------------|
| Package Name: | co.circlemedical.patient |
| Scan Date: | Aug. 28, 2025, 10:26 p.m. |
| App Security Score: | 50/100 (MEDIUM RISK) |
| Grade: | |
| Trackers Detection: | 2/432 |
| | |

FINDINGS SEVERITY

| ॠ HIGH | ▲ MEDIUM | i INFO | ✓ SECURE | ◎ HOTSPOT |
|---------------|----------|--------|----------|------------------|
| 4 | 24 | 5 | 3 | 2 |

FILE INFORMATION

File Name: co.circlemedical.patient_500.apk

Size: 129.35MB

MD5: 768c0daa26a9fa7c7842f064053f63f1

SHA1: 515e3e6f1450fcf157a26f3164c00268f8165296

SHA256: 6af3c6955d11a2be4c4f1dbaced36d98bd4e719416d6091c3b8e9786072ae52e

i APP INFORMATION

App Name: Circle Medical

Package Name: co.circlemedical.patient

Main Activity: co.circlemedical.android.view.screens.guests.LoginActivity

Target SDK: 34 Min SDK: 23 Max SDK:

Android Version Name: 6.20.2

EE APP COMPONENTS

Activities: 123 Services: 17 Receivers: 17 Providers: 11

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

***** CERTIFICATE INFORMATION

Binary is signed v1 signature: True v2 signature: True v3 signature: True v4 signature: False

X.509 Subject: C=US, ST=California, L=San Francisco, O=Circle Medical Technologies, CN=Jean-Sebastien Boulanger

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2015-11-02 04:24:12+00:00 Valid To: 2040-10-26 04:24:12+00:00

Issuer: C=US, ST=California, L=San Francisco, O=Circle Medical Technologies, CN=Jean-Sebastien Boulanger

Serial Number: 0x4957c5c Hash Algorithm: sha256

md5: d4fe14b9107e0e866afa739dcfea7459

sha1: 1eeecdfcd14d07dd544f5dec22873014d2b5d481

sha256: 8d8989c729a777efb4fd471747cbdd60eda5a849b68e24af423bbc4b13329198

sha512; c2e003ee839531a025686bd406867ef7c56df894cd24d178827d7e5478f6932757691c986d8a6c8c54fe7e3024d52378156b2e3e1164a544b0a3103b9e031493

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 000e9d6a47d2fb4e9853f182bc202bc13cc0932e07ec722bbb85e2dcd1fc410d

Found 1 unique certificates

⋮ APPLICATION PERMISSIONS

| PERMISSION | STATUS | INFO | DESCRIPTION |
|--|-----------|---|--|
| android.permission.ACCESS_NETWORK_STATE | normal | view network status | Allows an application to view the status of all networks. |
| android.permission.INTERNET | normal | full Internet access | Allows an application to create network sockets. |
| 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_EXTERNAL_STORAGE | dangerous | read external storage contents | Allows an application to read from external storage. |
| 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.FLASHLIGHT | normal | control flashlight | Allows the application to control the flashlight. |
| android.permission.RECORD_AUDIO | dangerous | record audio | Allows application to access the audio record path. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|-----------|---|---|
| android.permission.ACCESS_FINE_LOCATION | dangerous | fine (GPS) location | Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power. |
| android.permission.ACCESS_COARSE_LOCATION | dangerous | coarse (network-based) location | Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are. |
| android.permission.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. |
| 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.WAKE_LOCK | normal | prevent phone from sleeping | Allows an application to prevent the phone from going to sleep. |
| co.circlemedical.patient.permission.C2D_MESSAGE | unknown | Unknown permission | Unknown permission from android reference |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|-----------|---|--|
| android.permission.WRITE_EXTERNAL_STORAGE | dangerous | read/modify/delete external storage contents | Allows an application to write to 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.ACCESS_WIFI_STATE | normal | view Wi-Fi status | Allows an application to view the information about the status of Wi-Fi. |
| 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.BLUETOOTH | normal | create Bluetooth connections | Allows applications to connect to paired bluetooth devices. |
| android.permission.BLUETOOTH_ADMIN | normal | bluetooth administration | Allows applications to discover and pair bluetooth devices. |
| 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_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.MODIFY_AUDIO_SETTINGS | normal | change your audio settings | Allows application to modify global audio settings, such as volume and routing. |
| 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. |
| 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 | normal | enables regular apps to use Service.startForeground. | Allows a regular application to use Service.startForeground. |
| 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_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". |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|--|-----------|--|--|
| 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". |
| 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. |
| 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.POST_NOTIFICATIONS | dangerous | allows an app to post notifications. | Allows an app to post notifications |
| 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. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|--|---------|--|--|
| co.circlemedical.patient.sdk.permission-group.ipc.sender | unknown | Unknown permission | Unknown permission from android reference |
| 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. |
| com.google.android.c2dm.permission.RECEIVE | normal | recieve push notifications | Allows an application to receive push notifications from cloud. |
| com.google.android.gms.permission.AD_ID | normal | application shows advertisements | This app uses a Google advertising ID and can possibly serve advertisements. |
| android.permission.ACCESS_ADSERVICES_ATTRIBUTION | normal | allow applications to access advertising service attribution | This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns. |
| android.permission.ACCESS_ADSERVICES_AD_ID | normal | allow app to access the device's advertising ID. | This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|--|---------|--------------------------------|---|
| 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. |
| com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE | normal | permission defined by google | A custom permission defined by Google. |
| co.circlemedical.patient.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION | unknown | Unknown permission | Unknown permission from android reference |

M APKID ANALYSIS

| FILE | DETAILS | | |
|--------------------------------------|--------------|-------------------|--|
| 768c0daa26a9fa7c7842f064053f63f1.apk | FINDINGS | DETAILS | |
| 700c0daa20a31a7C7042100403310311.apk | Anti-VM Code | possible VM check | |

| FILE | DETAILS | | |
|----------------|--------------|---|--|
| | FINDINGS | DETAILS | |
| | Anti-VM Code | Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check possible VM check | |
| classes.dex | Compiler | r8 without marker (suspicious) | |
| | | | |
| classes10.dex | FINDINGS | DETAILS | |
| Classes Folder | Compiler | r8 without marker (suspicious) | |

| FILE | DETAILS | | |
|---------------|--------------|---|--|
| | FINDINGS | DETAILS | |
| classes11.dex | Anti-VM Code | Build.MANUFACTURER check network operator name check | |
| | Compiler | r8 without marker (suspicious) | |
| classes12.dex | FINDINGS | DETAILS | |
| Classes12.uex | Compiler | r8 without marker (suspicious) | |
| | | | |
| | FINDINGS | DETAILS | |
| classes13.dex | Anti-VM Code | Build.FINGERPRINT check Build.MANUFACTURER check | |
| | Compiler | r8 without marker (suspicious) | |

| FILE | DETAILS | | | |
|---------------|-----------------|---|--|--|
| | FINDINGS | DETAILS | | |
| classes14.dex | Anti-VM Code | Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check possible ro.secure check possible VM check | | |
| | Anti Debug Code | Debug.isDebuggerConnected() check | | |
| | Compiler | r8 without marker (suspicious) | | |
| classes15.dex | FINDINGS | DETAILS | | |
| | Compiler | unknown (please file detection issue!) | | |

| FILE | DETAILS | | | |
|--------------|-----------------|--|--|--|
| | FINDINGS | DETAILS | | |
| classes2.dex | 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 | r8 without marker (suspicious) | | |
| | | | | |
| | FINDINGS | DETAILS | | |
| classes3.dex | Anti-VM Code | Build.MANUFACTURER check Build.BOARD check | | |
| | Compiler | r8 without marker (suspicious) | | |

| FILE | DETAILS | | | |
|--------------|--------------|--|--|--|
| | FINDINGS | DETAILS | | |
| classes4.dex | Anti-VM Code | Build.FINGERPRINT check Build.MANUFACTURER check | | |
| | Compiler | r8 without marker (suspicious) | | |
| | FINDINGS | DETAILS | | |
| classes5.dex | Anti-VM Code | Build.FINGERPRINT check Build.MANUFACTURER check Build.HARDWARE check Build.TAGS check | | |
| | Compiler | r8 without marker (suspicious) | | |

| FILE | DETAILS | | | |
|--------------|--------------|--|--|--|
| | FINDINGS | DETAILS | | |
| classes6.dex | Anti-VM Code | Build.FINGERPRINT check Build.MANUFACTURER check Build.BOARD check possible Build.SERIAL check Build.TAGS check network operator name check device ID check possible ro.secure check possible VM check | | |
| | Compiler | r8 without marker (suspicious) | | |
| | FINDINGS | DETAILS | | |
| classes7.dex | Anti-VM Code | Build.FINGERPRINT check Build.MANUFACTURER check Build.BOARD check | | |
| | Compiler | r8 without marker (suspicious) | | |

| FILE | DETAILS | | | |
|--------------|--------------|---|--|--|
| | FINDINGS | DETAILS | | |
| classes8.dex | Anti-VM Code | Build.MANUFACTURER check SIM operator check | | |
| | Compiler | r8 without marker (suspicious) | | |
| | FINDINGS | DETAILS | | |
| | | | | |
| classes9.dex | Anti-VM Code | Build.MANUFACTURER check | | |
| | Compiler | r8 without marker (suspicious) | | |

BROWSABLE ACTIVITIES

| ACTIVITY | INTENT |
|--|--|
| co.circlemedical.android.view.screens.guests.DeepLinksActivity | Schemes: @string/http://, @string/https://, Hosts: @string/host, @string/hostCom, @string/linkTrackingDomain, Path Prefixes: /appointments, /check-in, /messages, /directions, /users/sign_in, /users/id_verification, /users/verification, /invoices, /patients/immunity_passport_opt_in, /patients/controlled_substance_agreement, /patients/at_home_sleep_study_agreement, /patients/gender_identity, /patients/truepill_opt_in, /places, /lab_orders, /prescription_orders, /questionnaire_responses, /payment_cards/new, /help, /rx_support, /conversations, /lab_reports, /insurances/new, /home, /payment_methods/new, /sleep_study_device, /insurances/new/v2, /a, |

| ACTIVITY | INTENT |
|--|---|
| com.stripe.android.link.LinkRedirectHandlerActivity | Schemes: link-popup://, Hosts: complete, Paths: /co.circlemedical.patient, |
| com.stripe.android.payments.StripeBrowserProxyReturnActivity | Schemes: stripesdk://, Hosts: payment_return_url, Paths: /co.circlemedical.patient, |

△ NETWORK SECURITY

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

| NO | SCOPE | SEVERITY | DESCRIPTION |
|----|---|----------|--|
| 1 | ocsp.digicert.com crl3.digicert.com crl4.digicert.com crl.godaddy.com certificates.godaddy.com crl.starfieldtech.com certificates.starfieldtech.com ocsp.godaddy.com ocsp.starfieldtech.com | high | Domain config is insecurely configured to permit clear text traffic to these domains in scope. |

CERTIFICATE ANALYSIS

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

Q MANIFEST ANALYSIS

HIGH: 1 | WARNING: 11 | INFO: 0 | SUPPRESSED: 0

| NO | ISSUE | SEVERITY | DESCRIPTION |
|----|--|----------|--|
| 1 | App can be installed on a vulnerable unpatched Android version Android 6.0-6.0.1, [minSdk=23] | high | This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates. |
| 2 | App has a Network Security Configuration [android:networkSecurityConfig=@xml/circle_medical_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 (co.circlemedical.android.view.screens.guests.DeepLinksActivity) 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 |
|----|---|----------|--|
| 4 | Broadcast Receiver (co.circlemedical.android.utils.sms.SmsBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.phone.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. |
| 5 | 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. |
| 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. |
| 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 | TaskAffinity is set for activity (com.braze.push.NotificationTrampolineActivity) | 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. |

| NO | ISSUE | SEVERITY | DESCRIPTION |
|----|---|----------|--|
| 9 | 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. |
| 10 | 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] | | 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. |
| 11 | 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 |
|----|---|----------|--|
| 12 | 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. |
| 13 | Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true] | warning | A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission. |

</> CODE ANALYSIS

HIGH: 2 | WARNING: 10 | INFO: 4 | SECURE: 2 | SUPPRESSED: 0

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|-------|----------|-----------|--|
| | | | | butterknife/ButterKnife.java co/circlemedical/android/utils/sms/AppSignatur eHelper.java |

| | | | | com/anonome/come/commanonview.java |
|----|-------|----------|-----------|--|
| NO | ISSUE | SEVERITY | STANDARDS | FILESirbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java |
| | | | | com/braze/support/BrazeLogger.java |
| | | | | com/bumptech/glide/Glide.java |
| | | | | com/bumptech/glide/disklrucache/DiskLruCach |
| | | | | e.java |
| | | | | com/bumptech/glide/gifdecoder/GifHeaderPars er.java |
| | | | | com/bumptech/glide/gifdecoder/StandardGifDe |
| | | | | coder.java |
| | | | | com/bumptech/glide/load/data/AssetPathFetche |
| | | | | r.java |
| | | | | com/bumptech/glide/load/data/HttpUrlFetcher.j |
| | | | | ava |
| | | | | com/bumptech/glide/load/data/LocalUriFetcher. |
| | | | | java |
| | | | | com/bumptech/glide/load/data/mediastore/Thu |
| | | | | mbFetcher.java |
| | | | | com/bumptech/glide/load/data/mediastore/Thu |
| | | | | mbnailStreamOpener.java |
| | | | | com/bumptech/glide/load/engine/DecodeJob.ja |
| | | | | Va |
| | | | | com/bumptech/glide/load/engine/DecodePath.j |
| | | | | ava |
| | | | | com/bumptech/glide/load/engine/Engine.java |
| | | | | com/bumptech/glide/load/engine/GlideExceptio |
| | | | | n.java |
| | | | | com/bumptech/glide/load/engine/SourceGenera |
| | | | | tor.java |
| | | | | com/bumptech/glide/load/engine/bitmap_recycl |
| | | | | e/LruArrayPool.java |
| | | | | com/bumptech/glide/load/engine/bitmap_recycl |
| | | | | e/LruBitmapPool.java |
| | | | | com/bumptech/glide/load/engine/cache/DiskLr |
| | | | | uCacheWrapper.java |
| | | | | com/bumptech/glide/load/engine/cache/Memor |
| | | | | ySizeCalculator.java |
| | | | | com/bumptech/glide/load/engine/executor/Glid |
| | | | | eExecutor.java |
| | | | | com/bumptech/glide/load/engine/executor/Run |
| 1 | | | | |

| NO | ISSUE | SEVERITY | STANDARDS | ရောက်မွှာumptech/glide/load/engine/prefill/Bitma PreFillRunner.java |
|----|-------|----------|-----------|--|
| | | | | com/bumptech/glide/load/model/ByteBufferE |
| | | | | oder.java |
| | | | | com/bumptech/glide/load/model/ByteBufferFi |
| | | | | Loader.java |
| | | | | com/bumptech/glide/load/model/FileLoader.ja |
| | | | | a |
| | | | | com/bumptech/glide/load/model/ResourceLo |
| | | | | er.java |
| | | | | com/bumptech/glide/load/model/StreamEnco |
| | | | | r.java |
| | | | | com/bumptech/glide/load/resource/ImageDe |
| | | | | derResourceDecoder.java |
| | | | | com/bumptech/glide/load/resource/bitmap/B |
| | | | | mapEncoder.java |
| | | | | com/bumptech/glide/load/resource/bitmap/E |
| | | | | mapImageDecoderResourceDecoder.java |
| | | | | com/bumptech/glide/load/resource/bitmap/E |
| | | | | aultImageHeaderParser.java |
| | | | | com/bumptech/glide/load/resource/bitmap/E |
| | | | | wnsampler.java |
| | | | | com/bumptech/glide/load/resource/bitmap/E |
| | | | | wableToBitmapConverter.java |
| | | | | com/bumptech/glide/load/resource/bitmap/l |
| | | | | dwareConfigState.java |
| | | | | com/bumptech/glide/load/resource/bitmap/T |
| | | | | nsformationUtils.java |
| | | | | com/bumptech/glide/load/resource/bitmap/\ |
| | | | | eoDecoder.java |
| | | | | com/bumptech/glide/load/resource/gif/ByteB |
| | | | | erGifDecoder.java |
| | | | | com/bumptech/glide/load/resource/gif/GifDr |
| | | | | ableEncoder.java |
| | | | | com/bumptech/glide/load/resource/gif/Strea |
| | | | | ifDecoder.java |
| | | | | com/bumptech/glide/manager/DefaultConne |
| | | | | ityMonitor.java |
| | | | | com/bumptech/glide/manager/DefaultConne |
| | | | | ityMonitorFactory.java |

| | | | | com/bumptech/glide/manager/RequestManager |
|----|---------------------------------------|----------|-----------------------------|---|
| NO | ISSUE logs information. Sensitive | SEVERITY | SWA:NY LANGE Sensitive | F112ECent.java |
| 1 | information should never be logged. | info | Information into Log File | com/bumptech/glide/manager/RequestManager |
| | intorritation should hever be logged. | | OWASP MASVS: MSTG-STORAGE-3 | Retriever.java |
| | | | | com/bumptech/glide/manager/RequestTracker.j |
| | | | | ava |
| | | | | com/bumptech/glide/manager/SupportRequest |
| | | | | ManagerFragment.java |
| | | | | com/bumptech/glide/module/ManifestParser.ja |
| | | | | va |
| | | | | com/bumptech/glide/request/SingleRequest.jav |
| | | | | a |
| | | | | com/bumptech/glide/request/target/CustomVie |
| | | | | wTarget.java |
| | | | | com/bumptech/glide/request/target/ViewTarget. |
| | | | | java |
| | | | | com/bumptech/glide/util/ContentLengthInputStr |
| | | | | eam.java |
| | | | | com/bumptech/glide/util/pool/FactoryPools.jav |
| | | | | a |
| | | | | com/caverock/androidsvg/SVGParser.java |
| | | | | com/caverock/androidsvg/SimpleAssetResolver.j |
| | | | | ava |
| | | | | com/coremedia/iso/boxes/sampleentry/AudioSa |
| | | | | mpleEntry.java |
| | | | | com/davemorrissey/labs/subscaleview/Subsam |
| | | | | plingScaleImageView.java |
| | | | | com/davemorrissey/labs/subscaleview/decoder |
| | | | | /SkiaPooledImageRegionDecoder.java |
| | | | | com/intercom/twig/Twig.java |
| | | | | com/jakewharton/disklrucache/DiskLruCache.ja |
| | | | | va |
| | | | | com/mp4parser/streaming/rawformats/H264Tr |
| | | | | ackAdapter.java |
| | | | | com/rudderstack/android/repository/EntityCont |
| | | | | entProvider.java |
| | | | | com/rudderstack/android/ruddermetricsreporte |
| | | | | randroid/internal/DebugLogger.java |
| | | | | com/rudderstack/android/ruddermetricsreporte |
| | | | | randroid/internal/error/ExceptionHandler.java |
| | | | | com/rudderstack/android/sdk/core/RudderLogg |

| NO | ISSUE | SEVERITY | STANDARDS | er.java ppregripe/android/core/Logger.java com/stripe/android/core/storage/SharedPrefere |
|----|-------|----------|-----------|---|
| NO | ISSUE | SEVERITY | STANDARDS | com/stripe/android/core/storage/SharedPrefere ncesStorage.java com/stripe/android/core/utils/PluginDetector.ja va com/stripe/android/stripe3ds2/transaction/Logg er.java com/stripe/hcaptcha/webview/HCaptchaDebugl nfo.java com/stripe/hcaptcha/webview/HCaptchaWebVie w.java com/stripe/hcaptcha/webview/HCaptchaWebVie w.java com/stripe/hcaptcha/webview/HCaptchaWebVie wHelper.java com/withpersona/sdk2/inquiry/internal/NfcErro rLog.java com/zipow/videobox/ZMFirebaseMessagingSer vice.java com/zipow/videobox/fragment/SettingAboutFra gment.java com/zipow/videobox/sip/server/CmmSIPNosMa nager.java io/ktor/http/parsing/DebugKt.java io/sentry/SystemOutLogger.java io/sentry/android/core/AndroidLogger.java io/sentry/android/core/SentryLogcatAdapter.jav a io/sentry/transport/StdoutTransport.java net/sqlcipher/database/SQLiteCompiledSql.java net/sqlcipher/database/SQLiteContentHelper.jav a net/sqlcipher/database/SQLiteContentHelper.jav |
| | | | | net/sqlcipher/database/SQLiteDebug.java net/sqlcipher/database/SQLiteProgram.java net/sqlcipher/database/SQLiteQuery.java net/sqlcipher/database/SQLiteQueryBuilder.java org/greenrobot/eventbus/Logger.java org/greenrobot/eventbus/util/ErrorDialogConfig. java org/greenrobot/eventbus/util/ErrorDialogManag |

| NO | ISSUE | SEVERITY | STANDARDS | er.java Fig/ESenrobot/eventbus/util/ExceptionToResou |
|----|-------|----------|-----------|---|
| | | | | rceMapping.java org/slf4j/helpers/Util.java |
| | | | | rx/internal/util/IndexedRingBuffer.java |
| | | | | rx/internal/util/RxRingBuffer.java |
| | | | | rx/plugins/RxJavaHooks.java |
| | | | | us/zoom/proguard/vh4.java |
| | | | | as zoom program arviviljava |
| | | | | co/circlemedical/android/Constants.java |
| | | | | co/circlemedical/android/model/domain/InputE rror.java |
| | | | | co/circlemedical/android/model/domain/pojo/S |
| | | | | ecrets.java |
| | | | | co/circlemedical/android/model/domain/pojo/S |
| | | | | tripeCustomerSecrets.java |
| | | | | co/circlemedical/android/model/domain/pojo/c |
| | | | | ontent/ContentAction.java |
| | | | | co/circlemedical/android/model/domain/pojo/f |
| | | | | eatureflag/FeatureFlagData.java |
| | | | | co/circlemedical/android/model/domain/pojo/i |
| | | | | n_app/payload/InAppPayloadType.java |
| | | | | co/circlemedical/android/model/domain/reposit |
| | | | | ory/network/circlemedical/request/UpdatePatie |
| | | | | ntRequestBody.java |
| | | | | co/circlemedical/android/model/domain/reposit |
| | | | | ory/network/circlemedical/request/UpdateUser |
| | | | | RequestBody.java |
| | | | | co/circlemedical/android/model/domain/reposit |
| | | | | ory/network/iterable/lterableApiInterceptor.java |
| | | | | co/circlemedical/android/view/control/calendar/ |
| | | | | WeekCalendarView.java |
| | | | | coil/decode/GifDecoder.java |
| | | | | coil/decode/SvgDecoder.java |
| | | | | coil/decode/VideoFrameDecoder.java |
| | | | | coil/memory/MemoryCache.java |
| | | | | coil/memory/MemoryCacheService.java |
| | | | | coil/request/Parameters.java |
| | | | | com/airbnb/lottie/compose/RememberLottieCo |
| | | | | mpositionKt.java |

| NO | ISSUE | SEVERITY | STANDARDS | com/braze/Constants.java Fdbf/6 raze/configuration/BrazeConfig.java com/braze/enums/CardKev.java |
|----|-------|----------|-----------|--|
| | | | | com/braze/images/DefaultBrazeImageLoader.ja va com/braze/models/inappmessage/InAppMessag eHtml.java com/braze/models/outgoing/AttributionData.jav a com/braze/push/BrazeNotificationUtils.java com/braze/push/BrazePushReceiver.java com/braze/support/StringUtils.java com/braze/ui/contentcards/ContentCardsFragm ent.java com/braze/ui/inappmessage/listeners/DefaultIn AppMessageWebViewClientListener.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKe y.java com/bumptech/glide/load/engine/EngineResour ce.java com/bumptech/glide/load/engine/ResourceCach eKey.java com/bumptech/glide/manager/RequestManager Retriever.java com/bumptech/glide/manager/RequestManager Retriever.java com/nimbusds/jose/HeaderParameterNames.ja va com/pubnub/api/models/consumer/PNStatus.ja va com/pubnub/api/models/consumer/PNStatus.ja va com/pubnub/api/models/consumer/PNStatus.ja va com/pubnub/api/models/server/SubscribeMess age.java com/pubnub/api/models/server/files/FormField .java com/rudderstack/android/integration/braze/Bra zeIntegrationFactory.java com/rudderstack/android/ruddermetricsreporte |

| NO | ISSUE | SEVERITY | STANDARDS | randroid/LibraryMetadata.java Hala S idderstack/android/ruddermetricsreporte randroid/internal/DefaultUploadMediator.java |
|----|-------|----------|-----------|--|
| | | | | com/rudderstack/android/ruddermetricsreporte randroid/internal/error/ExceptionHandler.java com/rudderstack/android/sdk/core/ReportMana ger.java |
| | | | | com/rudderstack/android/sdk/core/RudderFlus hWorkManager.java com/rudderstack/android/sdk/core/RudderNetw |
| | | | | orkManager.java com/rudderstack/android/sdk/core/RudderPrefe renceManager.java com/rudderstack/android/sdk/core/RudderTrait |
| | | | | s.java com/sdk/growthbook/Utils/Constants.java com/sdk/growthbook/Utils/GBVariationMeta.jav |
| | | | | a com/stripe/android/EphemeralKey.java com/stripe/android/PaymentConfiguration.java com/stripe/android/analytics/SessionSavedState Handler.java |
| | | | | com/stripe/android/auth/PaymentBrowserAuth Contract.java com/stripe/android/core/injection/InjectorKt.jav |
| | | | | a com/stripe/android/core/injection/NamedConst antsKt.java com/stripe/android/core/networking/AnalyticsFi |
| | | | | elds.java com/stripe/android/core/networking/AnalyticsFi elds.java t.java |
| | | | | com/stripe/android/core/networking/NetworkC onstantsKt.java com/stripe/android/core/networking/SendAnaly |
| | | | | ticsRequestV2WorkerKt.java com/stripe/android/customersheet/CustomerSh eetConfigViewModel.java com/stripe/android/customersheet/CustomerSh |
| | | | | eetContractKt.java |

| ОИ | ISSUE | SEVERITY | STANDARDS | com/stripe/android/googlepaylauncher/GoogleP |
|----|---------------------------------------|-----------|--|--|
| | <u> </u> | ' | | com/stripe/android/googlepaylauncher/GoogleP |
| l | 1 | 1 | | ayLauncherViewModel.java |
| ļ | 1 | 1 | | com/stripe/android/googlepaylauncher/GoogleP |
| I | 1 | 1 | | ayPaymentMethodLauncherContract.java |
| I | 1 | 1 | | com/stripe/android/googlepaylauncher/GoogleP |
| I | 1 | 1 | | ayPaymentMethodLauncherViewModel.java |
| I | 1 | 1 | | com/stripe/android/link/serialization/PopupPayl |
| | | | | oad.java |
| | | | | com/stripe/android/model/AttachConsumerToLi nkAccountSession.java |
| I | 1 | 1 | | com/stripe/android/model/ConfirmPaymentInte |
| I | 1 | 1 | | ntParams.java |
| I | 1 | 1 | | com/stripe/android/model/ConfirmSetupIntentP |
| I | 1 | 1 | | arams.java |
| I | 1 | 1 | | com/stripe/android/model/ConfirmStripeIntentP |
| I | 1 | 1 | | arams.java |
| I | 1 | 1 | | com/stripe/android/model/ConsumerSession.ja |
| I | 1 | 1 | | va |
| I | 1 | 1 | | com/stripe/android/model/ConsumerSessionLo |
| I | 1 | 1 | | okup.java |
| I | 1 | 1 | | com/stripe/android/model/ConsumerSessionSig |
| I | 1 | 1 | | nup.java |
| I | 1 | 1 | | com/stripe/android/model/CreateFinancialConn |
| I | 1 | 1 | | ectionsSessionParams.java |
| I | 1 | 1 | | com/stripe/android/model/ElementsSession.jav |
| I | 1 | 1 | | a |
| I | 1 | 1 | | com/stripe/android/model/ElementsSessionPar |
| I | 1 | 1 | | ams.java |
| l | 1 | 1 | | com/stripe/android/model/FinancialConnection |
| I | 1 | 1 | | sSession.java |
| I | 1 | 1 | | com/stripe/android/model/PaymentIntent.java |
| I | 1 | 1 | | com/stripe/android/model/PaymentMethodCre |
| I | 1 | 1 | | ateParams.java |
| I | 1 | 1 | | com/stripe/android/model/RadarSessionWithHC |
| I | 1 | 1 | CME: CME 212: Cleartest Storage of | aptcha.java |
| I | Files may contain hardcoded | 1 | CWE: CWE-312: Cleartext Storage of Sensitive Information | com/stripe/android/model/SetupIntent.java |
| 2 | sensitive information like usernames, | warning | | |
| I | <u>passwords, keys etc.</u> | 1 | OWASP MASVS: MSTC STORAGE 14 | com/stripe/android/model/Source.java |
| ļ | 1 | 1 | OWASP MASVS: MSTG-STORAGE-14 | com/stripe/android/model/SourceParams.java |

| NO | ISSUE | SEVERITY | STANDARDS | com/stripe/android/model/Stripe3ds2AuthPara |
|----|-------|----------|-----------|---|
| NO | ISSUE | SEVERITY | STANDARDS | · · |

| NO | ISSUE | SEVERITY | STANDARDS | mationDefinition.java For Stripe/android/paymentsheet/IntentConfir mationHandler.java |
|----|-------|----------|-----------|---|
| | | | | com/stripe/android/paymentsheet/IntentConfir mationInterceptor.java |
| | | | | com/stripe/android/paymentsheet/PaymentShe et.java |
| | | | | com/stripe/android/paymentsheet/PaymentShe etContract.java |
| | | | | com/stripe/android/paymentsheet/addresselem ent/AddressDetails.java |
| | | | | com/stripe/android/paymentsheet/addresselem |
| | | | | ent/AddressElementActivityContract.java com/stripe/android/paymentsheet/addresselem |
| | | | | ent/AddressElementNavigator.java com/stripe/android/paymentsheet/addresselem ent/AddressLauncher.java |
| | | | | com/stripe/android/paymentsheet/flowcontrolle r/DefaultFlowController.java |
| | | | | com/stripe/android/paymentsheet/flowcontrolle r/FlowControllerActivityResultCaller.java |
| | | | | com/stripe/android/paymentsheet/flowcontrolle |
| | | | | r/FlowControllerViewModel.java com/stripe/android/paymentsheet/paymentdata |
| | | | | collection/ach/USBankAccountFormViewModel.j ava |
| | | | | com/stripe/android/paymentsheet/paymentdata collection/polling/PollingContract.java |
| | | | | com/stripe/android/paymentsheet/paymentdata collection/polling/PollingViewModel.java |
| | | | | com/stripe/android/paymentsheet/repositories/ CustomerRepository.java |
| | | | | com/stripe/android/paymentsheet/state/Custo merState.java |
| | | | | com/stripe/android/polling/IntentStatusPoller.ja |
| | | | | com/stripe/android/stripe3ds2/observability/De faultSentryConfig.java |
| | | | | com/stripe/android/stripe3ds2/transaction/Acs Data.java |

| NO | ISSUE | SEVERITY | STANDARDS | com/stripe/android/stripe3ds2/transaction/Auth |
|----|-------|----------|-----------|--|
| | | | | com/stripe/android/stripe3ds2/transaction/Defa |
| | | 1 | | ultAcsDataParser.java |
| | | 1 | | com/stripe/android/stripe3ds2/transaction/Inte |
| | | 1 | | ntData.java |
| | | 1 | | com/stripe/android/uicore/elements/AddressTy |
| | | 1 | | pe.java |
| | | | | com/stripe/android/view/AddPaymentMethodVi ewModel.java |
| | | | | com/stripe/android/view/PaymentAuthWebView Client.java |
| | | 1 | | com/stripe/hcaptcha/config/HCaptchaConfig.jav |
| | | 1 | | a |
| | | | | com/withpersona/sdk2/inquiry/governmentid/G overnmentld.java |
| | | 1 | | com/withpersona/sdk2/inquiry/governmentid/G |
| | | 1 | | overnmentIdAnalyzeWorker.java |
| | | 1 | | com/withpersona/sdk2/inquiry/governmentid/l |
| | | 1 | | |
| | | 1 | | dConfig.java com/withpersona/sdk2/inquiry/internal/Inquiryl |
| | | 1 | | |
| | | 1 | | ntentKeys.java |
| | | 1 | | com/withpersona/sdk2/inquiry/internal/Inquiry |
| | | 1 | | State.java |
| | | | | com/withpersona/sdk2/inquiry/modal/ModalW orkflow.java |
| | | | | com/withpersona/sdk2/inquiry/network/ErrorR esponse.java |
| | | | | com/withpersona/sdk2/inquiry/nfc/PassportNfc ReaderConfig.java |
| | | | | com/withpersona/sdk2/inquiry/permissions/Per missionsUtilsKt.java |
| | | | | com/withpersona/sdk2/inquiry/shared/data_coll |
| | | 1 | | ection/RealDataCollector.java |
| | | 1 | | com/withpersona/sdk2/inquiry/types/ConstsKt.j |
| | | 1 | | ava |
| | | 1 | | com/withpersona/sdk2/inquiry/ui/UiState.java |
| | | 1 | | com/zipow/videobox/confapp/meeting/reaction |
| | | 1 | | /ZmBulletEmojiEmitter.java |
| | 1 | 1 | | com/zipow/videobox/login/model/UserAccount. |

| NO | ISSUE | SEVERITY | STANDARDS | java FdhFSpow/videobox/ptapp/ZmZRMgr.java com/zipow/videobox/sip/server/CmmSIPCallHis |
|----|---|----------|---|--|
| | | | | toryltemBean.java io/ktor/client/request/forms/FormPart.java io/ktor/http/auth/HttpAuthHeader.java io/ktor/util/PlatformUtilsJvmKt.java io/reactivex/internal/schedulers/SchedulerPoolF actory.java io/reactivex/rxjava3/internal/schedulers/Schedu lerPoolFactory.java io/sentry/Baggage.java io/sentry/SpanDataConvention.java io/sentry/TraceContext.java io/sentry/okhttp/SentryOkHttpEventKt.java io/sentry/protocol/User.java operations/array/Reduce.java rx/internal/schedulers/NewThreadWorker.java us/zoom/feature/pbo/ui/ZmPBOUI.java us/zoom/libtools/storage/PreferenceUtil.java us/zoom/libtools/storage/ZmSharePreferenceHe lper.java us/zoom/module/api/zcalendar/IZCalendarServi ce.java us/zoom/proguard/bh0.java us/zoom/proguard/cx4.java |
| 3 | 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 | US/7/2017/proguard/cx1-java US/7/2017/proguard/cx1-java US/7/2017/proguard/cx1-java/cs |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|--|----------|--|---|
| 4 | App can write to App Directory. Sensitive Information should be encrypted. | info | CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14 | bo/app/cg0.java bo/app/e50.java bo/app/fv.java bo/app/gy.java bo/app/jr.java bo/app/jr.java bo/app/jr.java bo/app/ju.java bo/app/la0.java bo/app/rc.java bo/app/re0.java bo/app/re0.java bo/app/xs.java bo/app/xs.java bo/app/xs.java com/braze/configuration/RuntimeAppConfigurat ionProvider.java com/braze/managers/BrazeGeofenceManager.ja va |
| 5 | The App uses an insecure Random Number Generator. | warning | CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6 | bo/app/w30.java com/braze/support/IntentUtils.java com/pubnub/api/vendor/Crypto.java com/zipow/videobox/conference/ui/controller/S ymbioticActivityController.java io/sentry/metrics/MetricsHelper.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|--|----------|---|--|
| 6 | This App may have root detection capabilities. | secure | OWASP MASVS: MSTG-RESILIENCE-1 | com/rudderstack/android/ruddermetricsreporte randroid/internal/error/RootDetector.java io/sentry/android/core/DeviceInfoUtil.java io/sentry/android/core/internal/util/RootChecke r.java us/zoom/proguard/ym4.java |
| 7 | This App may request root (Super User) privileges. | warning | CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1 | com/withpersona/sdk2/inquiry/shared/device/R ootedDeviceUtilsKt.java io/sentry/android/core/internal/util/RootChecke r.java |
| 8 | App can read/write to External Storage. Any App can read data written to External Storage. | warning | CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2 | com/withpersona/sdk2/inquiry/document/DocumentCameraWorker.java com/withpersona/sdk2/inquiry/launchers/DocumentSelectWorker.java com/withpersona/sdk2/inquiry/launchers/DocumentsSelectWorker\$run\$1.java com/zipow/annotate/AnnoUtil.java com/zipow/cmmlib/AppUtil.java io/sentry/android/core/DeviceInfoUtil.java us/zoom/libtools/utils/ZmDeviceUtils.java us/zoom/proguard/ez1.java us/zoom/proguard/k15.java us/zoom/proguard/kx0.java us/zoom/proguard/l93.java us/zoom/proguard/ph0.java us/zoom/proguard/ph0.java us/zoom/proguard/yh1.java us/zoom/proguard/wl1.java us/zoom/proguard/wl1.java us/zoom/videomeetings/richtext/ZMRichTextUti l.java us/zoom/zimmsg/chatlist/MMChatsListFragmen t.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|--|----------|--|---|
| 9 | 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 |
| 10 | 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/rudderstack/android/repository/Dao.java com/rudderstack/android/sdk/core/DBPersisten tManager.java com/rudderstack/android/sdk/core/persistence/ DefaultPersistence.java com/rudderstack/android/sdk/core/persistence/ DefaultPersistenceProvider.java com/rudderstack/android/sdk/core/persistence/ EncryptedPersistence.java io/sentry/android/sqlite/SentrySupportSQLiteDa tabase.java net/sqlcipher/DatabaseUtils.java net/sqlcipher/database/SQLiteDatabase.java |
| 11 | This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files. | info | OWASP MASVS: MSTG-CRYPTO-1 | com/rudderstack/android/sdk/core/persistence/ DefaultPersistenceProvider.java net/sqlcipher/database/SupportHelper.java |
| 12 | This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel. | secure | OWASP MASVS: MSTG-NETWORK-4 | co/circlemedical/android/di/PresentersModule.j ava co/circlemedical/android/model/api/ApiModule. java com/pubnub/api/managers/RetrofitManager.jav a com/withpersona/sdk2/inquiry/network/Networ kModule.java us/zoom/proguard/n32.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|--|----------|---|---|
| 13 | 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 | co/circlemedical/android/view/screens/guests/C heckAccountStatusFragment.java com/stripe/hcaptcha/webview/HCaptchaWebVie wHelper.java us/zoom/proguard/wl1.java |
| 14 | 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/ZmB aseLiveStreamDialog.java com/zipow/videobox/view/sip/coverview/Phone PBXListCoverSummaryView.java com/zipow/videobox/view/sip/voicemail/encryp tion/ui/b.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/zmsg/deeplink/DeepLinkViewHelper.ja va us/zoom/zmsg/richtext/CustomActionModeProv ider.java us/zoom/zmsg/view/mm/f.java |
| 15 | 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/pubnub/api/vendor/FileEncryptionUtil.java io/ktor/util/CryptoKtCryptoJvmKt.java io/ktor/util/NonceKt\$nonceGeneratorJob\$1.java io/sentry/util/StringUtils.java |
| 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/nimbusds/jose/crypto/impl/AESCBC.java com/nimbusds/jose/jca/JCASupport.java com/pubnub/api/vendor/Crypto.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|--|----------|---|--|
| 17 | 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 | coil/decode/SourceImageSource.java com/zipow/videobox/MMShareActivity.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/MMChatInputFragmen t.java us/zoom/zmsg/view/mm/VoiceRecordView.java us/zoom/zmsg/view/mm/VoiceTalkView.java |
| 18 | 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 |

■ NIAP ANALYSIS v1.3

| NO IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|---------------|-------------|---------|-------------|
|---------------|-------------|---------|-------------|

BEHAVIOUR ANALYSIS

| RULE ID | BEHAVIOUR | LABEL | FILES |
|------------|-----------|-------|---|
| | | | bo/app/bj0.java bo/app/ea.java bo/app/fa.java |

| | | | bo/app/gp.java |
|------|-----------|-------|--|
| RULE | BEHAVIOUR | LABEL | bo/app/yd0.java 50/app /zc.java |
| ID | | | co/circlemedical/android/app/insurance/scanner/InsuranceCardScannerActivity.java |
| | | | co/circlemedical/android/app/insurance/scanner/InsuranceCardScannerFragment.java |
| | | | co/circlemedical/android/components/messageinput/MessageInputView.java |
| | | | co/circlemedical/android/components/picker/ImagePickerProvider.java |
| | | | co/circlemedical/android/extensions/file/File_getExifOrientationKt.java |
| | | | co/circlemedical/android/extensions/file/File_loadToBitmapKt.java |
| | | | co/circlemedical/android/model/domain/pojo/Conversation.java |
| | | | co/circlemedical/android/model/domain/repository/network/circlemedical/NetworkD |
| | | | ataStoreImpl.java |
| | | | coil/disk/DiskCache.java |
| | | | com/airbnb/lottie/LottieCompositionFactory.java |
| | | | com/airbnb/lottie/network/NetworkCache.java |
| | | | com/airbnb/lottie/network/NetworkFetcher.java |
| | | | com/braze/e0.java |
| | | | com/braze/support/BrazeImageUtils.java |
| | | | com/braze/support/WebContentUtils.java |
| | | | com/fasterxml/jackson/databind/ser/std/FileSerializer.java |
| | | | com/rudderstack/android/sdk/core/persistence/DefaultPersistenceProvider.java |
| | | | com/withpersona/sdk2/camera/camera2/MediaRecorderWrapper.java |
| | | | com/withpersona/sdk2/inquiry/document/DocumentCameraWorker.java |
| | | | com/withpersona/sdk2/inquiry/document/DocumentTileAdapter.java |
| | | | com/withpersona/sdk2/inquiry/governmentid/CameraScreenRunner\$showRendering\$ 1\$7\$1.java |
| | | | com/withpersona/sdk2/inquiry/governmentid/CameraScreenRunner\$showRendering\$ 1\$9.java |
| | | | com/withpersona/sdk2/inquiry/governmentid/CountdownCameraWorker.java com/withpersona/sdk2/inquiry/governmentid/video_capture/LocalVideoCaptureRend |
| | | | erer.java |
| | | | com/withpersona/sdk2/inquiry/launchers/DocumentSelectWorker.java |
| | | | com/withpersona/sdk2/inquiry/launchers/DocumentsSelectWorker\$run\$1.java |
| | | | com/withpersona/sdk2/inquiry/selfie/CameraScreenRunner\$showRendering\$1\$takeP |
| | | | hoto\$1.java |
| | | | com/withpersona/sdk2/inquiry/selfie/SelfieKt.java |
| | | | com/withpersona/sdk2/inquiry/selfie/video_capture/LocalVideoCaptureRenderer.java |
| | | | com/withpersona/sdk2/inquiry/shared/image/ReallmageHelper.java |
| | | | com/zipow/annotate/AnnoUtil.java |
| | | | com/zipow/cmmlib/AppContext.java |
| | | | com/zipow/videobox/CameraActivity.java |
| l | I | I | constant and const |

| | | | com/zipow/videobox/VideoBoxApplication.java |
|-------|--------------------------------------|-------|---|
| RULE | DELLAVIOLID | LADEL | com/zipow/videobox/broadcast/ZmPtBroadCastReceiver.java |
| ID | BEHAVIOUR | LABEL | Eon/zipow/videobox/config/ConfigWriter.java |
| טו | | | com/zipow/videobox/stabilility/StabilityService.java |
| | | | com/zipow/videobox/utils/ZmUtils.java |
| | Open a file from given absolute path | | com/zipow/videobox/view/mm/a.java |
| 00022 | of the file | file | com/zipow/videobox/view/ptvideo/PBXVideoRecordActivity.java |
| | of the file | | 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/cache/CacheStrategy.java |
| | | | io/sentry/cache/CacheUtils.java |
| | | | io/sentry/cache/EnvelopeCache.java |
| | | | io/sentry/instrumentation/file/FileIOSpanManager.java |
| | | | us/zoom/apm/stats/ZMStats.java |
| | | | us/zoom/libtools/utils/ZmMimeTypeUtils.java |
| | | | 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 |

| RULE ID | BEHAVIOUR | LABEL | us/zoom/proguard/ql.java us/zoom/proguard/uf3.java LSZOOM/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/f.java |
| 00204 | Get the default ringtone | collection | us/zoom/proguard/ir3.java us/zoom/proguard/ns.java |
| | | | bo/app/pr.java bo/app/wc0.java co/circlemedical/android/model/domain/repository/network/circlemedical/request/Pr ogressAwareRequestBody.java coil/fetch/ContentUriFetcher.java com/airbnb/lottie/compose/RememberLottieCompositionKt.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/braze/support/BrazelmageUtils.java com/braze/support/WebContentUtils.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/fasterxml/jackson/core/TokenStreamFactory.java com/fasterxml/jackson/databind/ObjectReader.java com/fasterxml/jackson/dataformat/cbor/CBORFactory.java com/fasterxml/jackson/dataformat/cbor/CBORFactory.java com/jakewharton/disklrucache/DiskLruCache.java com/nimbusds/jose/util/IOUtils.java com/rudderstack/android/ruddermetricsreporterandroid/internal/error/RootDetector.j ava |

| | | | com/rudderstack/android/sdk/core/RudderFlushWorkManager.java |
|-------|------------------------------------|-------|--|
| RULE | DELLA MOLID | LADEL | com/rudderstack/android/sdk/core/RudderServerConfigManager.java |
| ID | BEHAVIOUR | LABEL | com/rudderstack/android/sdk/core/RudderServerConfigManager.java FILES com/sdk/growthbook/sandbox/CachingAndroid.java |
| 10 | | | com/soywiz/krypto/PRNGFixes.java |
| | | | com/stripe/android/core/networking/FileUploadRequest.java |
| | | | com/withpersona/sdk2/inquiry/document/network/ProgressRequestBody.java |
| | | | com/withpersona/sdk2/inquiry/error_reporting/ExceptionLogger.java |
| | | | com/withpersona/sdk2/inquiry/shared/image/RealImageHelper.java |
| | | | com/zipow/annotate/ImageUtil.java |
| | | | com/zipow/cmmlib/AppContext.java |
| | | | com/zipow/videobox/VideoBoxApplication.java |
| | | | com/zipow/zm2d/Zm2DImageUtil.java |
| | | | io/sentry/EnvelopeSender.java |
| | | | io/sentry/OutboxSender.java |
| | | | io/sentry/PreviousSessionFinalizer.java |
| 00013 | Read file and put it into a stream | file | io/sentry/android/core/SentryPerformanceProvider.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/OkioJvmOkioKt.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 |
| 1 | | I | |

| RULE ID | BEHAVIOUR | LABEL | 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 |
| 00125 | Check if the given file path exist | file | 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 us/zoom/proguard/b51.java us/zoom/proguard/b43.java us/zoom/proguard/de3.java us/zoom/proguard/gc1.java us/zoom/proguard/gh0.java us/zoom/proguard/jt1.java us/zoom/proguard/o00.java us/zoom/roguard/o00.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/fragment/a.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/MMContentFileViewerFragment.java us/zoom/zmsg/view/mm/MMContentFileViewerFragment.java us/zoom/zmsg/view/mm/b.java us/zoom/zmsg/view/mm/b.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|------------|------------------------------|------------|--|
| 00091 | Retrieve data from broadcast | collection | co/circlemedical/android/app/home/area_or_care/AreaOfCareActivity.java co/circlemedical/android/app/primary_care_provider_detail/PrimaryCareProviderDetai lActivity.java co/circlemedical/android/app/web/WebViewActivity.java co/circlemedical/android/inp/web/WebViewActivity.java com/braze/push/BrazeNotificationUtils.java com/stripe/android/link/LinkForegroundActivity.java com/stripe/android/link/LinkForegroundActivity.java com/withpersona/sdk2/inquiry/lnquiry.java com/zipow/videobox/IMActivity.java com/zipow/videobox/fragment/IMAddrBookListFragment.java com/zipow/videobox/fragment/SettingAboutFragment.java com/zipow/videobox/fragment/SettingAboutFragment.java us/zoom/proguard/e40.java us/zoom/proguard/ij1.java us/zoom/proguard/k72.java us/zoom/proguard/rn0.java us/zoom/proguard/u03.java us/zoom/rproguard/u03.java us/zoom/zimmsg/filecontent/MMSessionFilesFragment.java us/zoom/zimmsg/filecontent/a.java us/zoom/zimmsg/fragment/MMChatInputFragment.java us/zoom/zmsg/fragment/MMChatInputFragment.java us/zoom/zmsg/fragment/a.java us/zoom/zmsg/fragment/a.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|------------|---|---------|--|
| 00012 | Read data and put it into a buffer stream | file | io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/cache/CacheStrategy.java io/sentry/cache/EnvelopeCache.java io/sentry/config/FilesystemPropertiesLoader.java io/sentry/util/FileUtils.java 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 |
| 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 |
| | | | co/circlemedical/android/extensions/context/Context_callPhoneNumberKt.java co/circlemedical/android/extensions/context/Context_openEmailIntentKt.java co/circlemedical/android/extensions/context/Context_openGoogleMapsDirectionsKt.ja va co/circlemedical/android/extensions/context/Context_openInGooglePlayKt.java co/circlemedical/android/extensions/context/Context_openUrlInBrowserKt.java co/circlemedical/android/view/screens/IntentFactory.java com/braze/Braze.java com/braze/braze.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/inappmessage/views/InAppMessageHtmlBaseView.java com/braze/ui/support/UriUtils.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 |

| RULE ID | BEHAVIOUR | LABEL | com/stripe/android/view/PaymentAuthWebViewClient.java com/withpersona/sdk2/inquiry/launchers/CustomTabsLauncherModuleKt.java FILES com/zlpow/videobox/JoinByURLActivity.java |
|------------|---|---------|---|
| 00063 | Implicit intent(view a web page, make a phone call, etc.) | control | com/zipow/videobox/LauncherActivity, java com/zipow/videobox/MMShareActivity, java com/zipow/videobox/framainServiceImpl.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/wiget/MeetingsWidget.java io/noties/markwon/LinkResolverDef.java us/zoom/internal/impl/b.java us/zoom/proguard/bn0.java us/zoom/proguard/bq3.java us/zoom/proguard/ch.java us/zoom/proguard/ch.java us/zoom/proguard/e21.java us/zoom/proguard/e40.java us/zoom/proguard/fk1.java us/zoom/proguard/fk1.java us/zoom/proguard/fk1.java us/zoom/proguard/fk1.java us/zoom/proguard/fk1.java us/zoom/proguard/fk1.java us/zoom/proguard/fk1.java us/zoom/proguard/fk1.java us/zoom/proguard/kl55.java us/zoom/proguard/lc4.java |

| RULE ID | BEHAVIOUR | LABEL | us/zoom/proguard/u03.java us/zoom/proguard/v74.java F1LFS 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/zclips/viewer/entrance/a.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/a.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/MMContentFileViewerFragment.java us/zoom/zmsg/view/mm/MMContentFileViewerFragment.java us/zoom/zmsg/view/mm/message/MessageRemoveHistoryView.java us/zoom/zmsg/view/mm/message/MessageRemoveHistoryView.java |
| 00208 | Capture the contents of the device screen | collection screen | us/zoom/proguard/gm1.java us/zoom/proguard/ho4.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 |
| 00112 | Get the date of the calendar event | collection calendar | com/fasterxml/jackson/databind/ser/std/StdKeySerializers.java com/fasterxml/jackson/databind/util/StdDateFormat.java com/zipow/videobox/view/schedule/ZmScheduleTimeAndRecurringLayout.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/rudderstack/android/sdk/core/RudderNetworkManager.java com/rudderstack/web/internal/WebServiceImpl.java com/stripe/android/core/networking/ConnectionFactory.java com/stripe/android/stripe3ds2/transaction/StripeHttpClient.java io/ktor/client/engine/android/AndroidClientEngine.java io/sentry/transport/HttpConnection.java |
| 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/rudderstack/android/sdk/core/RudderNetworkManager.java com/rudderstack/web/internal/WebServiceImpl.java com/stripe/android/stripe3ds2/transaction/StripeHttpClient.java io/sentry/transport/HttpConnection.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|------------|---|------------|---|
| 00036 | Get resource file from res/raw directory | reflection | coil/map/ResourceIntMapper.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/support/UriUtils.java com/braze/ui/support/UriUtils.java com/davemorrissey/labs/subscaleview/SubsamplingScaleImageView.java com/rudderstack/android/repository/EntityContentProvider.java com/zipow/videobox/confapp/meeting/confhelper/ZoomRateHelper.java com/zipow/videobox/utill/NotificationMgr.java com/zipow/videobox/utils/ZmUtils.java com/zipow/videobox/widget/MeetingsWidget.java io/noties/markwon/LinkResolverDef.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/bn0.java us/zoom/proguard/di4.java us/zoom/proguard/h2.java us/zoom/proguard/h2.java us/zoom/proguard/h2.java us/zoom/proguard/k15.java us/zoom/proguard/l5.java us/zoom/proguard/l5.java us/zoom/proguard/l64.java us/zoom/proguard/l64.java us/zoom/proguard/l64.java us/zoom/proguard/l64.java us/zoom/proguard/l64.java us/zoom/proguard/l64.java us/zoom/proguard/l64.java us/zoom/proguard/l64.java us/zoom/proguard/l64.java |
| 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 |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|------------|---|------------|--|
| 00051 | Implicit intent(view a web page, make a phone call, etc.) via setData | control | co/circlemedical/android/extensions/context/Context_openEmailIntentKt.java co/circlemedical/android/view/screens/IntentFactory.java com/stripe/android/link/LinkForegroundActivity.java com/stripe/android/payments/StripeBrowserLauncherViewModel.java com/stripe/android/uicore/text/HtmlKt.java com/stripe/android/uicore/text/HtmlKt.java com/stripe/android/uicore/text/HtmlKt.java com/stripe/android/uicore/text/HtmlKt.java com/stripe/android/uicore/text/HtmlKt.java com/stripe/android/uicore/text/HtmlKt.java com/zipow/videobox/ZmMainServiceImpl.java com/zipow/videobox/ZmMainServiceImpl.java com/zipow/videobox/fragment/AddrBookItemDetailSFragment.java com/zipow/videobox/fragment/MyProfileFragment.java com/zipow/videobox/fragment/MyProfileFragment.java com/zipow/videobox/view/sip/sms/PbxSmsTextItemView.java com/zipow/videobox/widget/MeetingsWidget.java us/zoom/ilibtools/utils/ZmMimeTypeUtils.java us/zoom/ilibtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/h1.java us/zoom/proguard/k15.java us/zoom/proguard/k15.java us/zoom/proguard/n1.java us/zoom/proguard/n3.java us/zoom/proguard/n3.java us/zoom/zapp/fragment/ZappUIComponent.java us/zoom/zapp/fragment/ZappUIComponent.java us/zoom/zapp/misc/BasicModeUIMgr.java us/zoom/zimmsg/comtacts/ShowMyQrCodeFragment.java us/zoom/zimmsg/comtacts/ShowMyQrCodeFragment.java us/zoom/zimmsg/fragment/IMShareInviteDialog.java us/zoom/zmsg/fragment/Java us/zoom/zmsg/fragment/Java us/zoom/zmsg/fragment/Java us/zoom/zmsg/fragment/Jiava us/zoom/zmsg/fragment/Java us/zoom/zmsg/fragment/Java us/zoom/zmsg/fragment/Java us/zoom/zmsg/fragment/Java us/zoom/zmsg/view/mm/f.java us/zoom/zmsg/view/mm/f.java us/zoom/zmsg/view/mm/f.java |
| 00038 | Query the phone number | collection | com/zipow/videobox/sip/server/CmmSIPCallManager.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|------------|---|-----------------|--|
| 00033 | Query the IMEI number | collection | com/zipow/videobox/sip/server/CmmSIPCallManager.java us/zoom/libtools/utils/ZmDeviceUtils.java |
| 00192 | Get messages in the SMS inbox | sms | us/zoom/proguard/f93.java us/zoom/proguard/l93.java us/zoom/videomeetings/richtext/ZMRichTextUtil.java |
| 00089 | Connect to a URL and receive input stream from the server | command network | com/bumptech/glide/load/data/HttpUrlFetcher.java com/nimbusds/jose/util/DefaultResourceRetriever.java com/rudderstack/android/sdk/core/RudderNetworkManager.java com/rudderstack/web/internal/WebServiceImpl.java com/stripe/android/stripe3ds2/transaction/StripeHttpClient.java io/sentry/transport/HttpConnection.java |
| 00109 | Connect to a URL and get the response code | network command | com/bumptech/glide/load/data/HttpUrlFetcher.java com/nimbusds/jose/util/DefaultResourceRetriever.java com/rudderstack/android/sdk/core/RudderNetworkManager.java com/rudderstack/web/internal/WebServiceImpl.java com/stripe/android/payments/core/authentication/RealRedirectResolver.java com/stripe/android/stripe3ds2/transaction/StripeHttpClient.java io/ktor/client/engine/android/AndroidClientEngine.java io/sentry/transport/HttpConnection.java |
| 00043 | Calculate WiFi signal strength | collection wifi | us/zoom/proguard/ny2.java |
| 00130 | Get the current WIFI information | wifi collection | us/zoom/proguard/l34.java us/zoom/proguard/ny2.java |
| 00175 | Get notification manager and cancel notifications | notification | com/zipow/videobox/util/NotificationMgr.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|------------|---|---------------------|---|
| 00121 | Create a directory | file command | com/zipow/videobox/view/mm/a.java us/zoom/zapp/jni/common/ZappCallBackUllmpl.java us/zoom/zimmsg/chatlist/MMChatsListFragment.java us/zoom/zmsg/fragment/MMChatInputFragment.java |
| 00016 | Get location info of the device and put it to JSON object | location collection | com/braze/models/outgoing/BrazeLocation.java |
| 00064 | Monitor incoming call status | control | com/zipow/videobox/sip/server/n.java us/zoom/proguard/oo2.java |
| 00189 | Get the content of a SMS message | sms | co/circlemedical/android/components/calendar/CalendarProvider.java co/circlemedical/android/presenter/usecases/appointments/AddAppointmentToCalen darUseCase.java us/zoom/core/data/preference/a.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/l93.java us/zoom/proguard/o23.java |
| 00202 | Make a phone call | control | us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/qh3.java |
| 00203 | Put a phone number into an intent | control | us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/qh3.java |
| 00188 | Get the address of a SMS message | sms | co/circlemedical/android/components/calendar/CalendarProvider.java co/circlemedical/android/presenter/usecases/appointments/AddAppointmentToCalen darUseCase.java us/zoom/core/data/preference/a.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/l93.java us/zoom/proguard/o23.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|------------|---|------------------------------------|---|
| 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 |
| 00011 | Query data from URI (SMS, CALLLOGS) | sms calllog collection | com/rudderstack/android/repository/EntityContentProvider.java us/zoom/core/data/preference/a.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/l93.java |
| 00191 | Get messages in the SMS inbox | sms | us/zoom/core/data/preference/a.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/i81.java us/zoom/proguard/l93.java |
| 00200 | Query data from the contact list | collection contact | co/circlemedical/android/components/calendar/CalendarProvider.java co/circlemedical/android/presenter/usecases/appointments/AddAppointmentToCalen darUseCase.java us/zoom/core/data/preference/a.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/l93.java us/zoom/proguard/o23.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 |
|------------|---|------------------------------------|--|
| 00201 | Query data from the call log | collection calllog | co/circlemedical/android/components/calendar/CalendarProvider.java co/circlemedical/android/presenter/usecases/appointments/AddAppointmentToCalen darUseCase.java us/zoom/core/data/preference/a.java us/zoom/libtools/utils/ZmMimeTypeUtils.java us/zoom/proguard/l93.java us/zoom/proguard/o23.java |
| 00077 | Read sensitive data(SMS, CALLLOG, etc) | collection sms calllog calendar | com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/rudderstack/android/repository/EntityContentProvider.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 |
| 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 | com/withpersona/sdk2/inquiry/shared/inquiry_session/GpsUtilsKt.java us/zoom/proguard/aw4.java |
| 00163 | Create new Socket and connecting to it | socket | com/rudderstack/android/sdk/core/RudderNetworkManager.java |
| 00094 | Connect to a URL and read data from it | command network | com/rudderstack/android/sdk/core/RudderNetworkManager.java us/zoom/core/model/a.java |
| 00108 | Read the input stream from given URL | network command | com/rudderstack/android/sdk/core/RudderNetworkManager.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|------------|--|----------------------|--|
| 00199 | Stop recording and release recording resources | record | com/withpersona/sdk2/camera/camera2/MediaRecorderWrapper\$stopRecording\$2.ja va com/withpersona/sdk2/camera/camera2/MediaRecorderWrapper.java us/zoom/proguard/u12.java |
| 00001 | Initialize bitmap object and compress data (e.g. JPEG) into bitmap object | camera | com/zipow/annotate/ImageUtil.java com/zipow/videobox/CameraActivity.java com/zipow/zm2d/Zm2DImageUtil.java us/zoom/proguard/ph0.java |
| 00005 | Get absolute path of file and put it to JSON object | file | com/airbnb/lottie/LottieCompositionFactory.java us/zoom/apm/stats/ZMStats.java us/zoom/proguard/ol2.java |
| 00024 | Write file after Base64 decoding | reflection file | com/airbnb/lottie/LottieCompositionFactory.java us/zoom/proguard/wl1.java |
| 00004 | Get filename and put it to JSON object | file collection | co/circlemedical/android/model/api/Api.java com/airbnb/lottie/LottieCompositionFactory.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 |
| 00083 | Query the IMEI number | collection telephony | us/zoom/libtools/utils/ZmDeviceUtils.java |
| 00137 | Get last known location of the device | location collection | us/zoom/proguard/aw4.java |
| 00195 | Set the output path of the recorded file | record file | com/withpersona/sdk2/camera/camera2/MediaRecorderWrapper.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|------------|---|----------------------|--|
| 00194 | Set the audio source (MIC) and recorded file format | record | com/withpersona/sdk2/camera/camera2/MediaRecorderWrapper.java us/zoom/proguard/u12.java |
| 00197 | Set the audio encoder and initialize the recorder | record | com/withpersona/sdk2/camera/camera2/MediaRecorderWrapper.java us/zoom/proguard/u12.java |
| 00007 | Use absolute path of directory for the output media file path | file | com/withpersona/sdk2/camera/camera2/MediaRecorderWrapper.java |
| 00196 | Set the recorded file format and output path | record file | com/withpersona/sdk2/camera/camera2/MediaRecorderWrapper.java us/zoom/proguard/u12.java |
| 00062 | Query WiFi information and WiFi Mac Address | wifi collection | us/zoom/proguard/l34.java |
| 00134 | Get the current WiFi IP address | wifi collection | us/zoom/proguard/l34.java |
| 00082 | Get the current WiFi MAC address | collection wifi | us/zoom/proguard/l34.java |
| 00028 | Read file from assets directory | file | com/caverock/androidsvg/SimpleAssetResolver.java us/zoom/proguard/k72.java |
| 00104 | Check if the given path is directory | file | com/zipow/videobox/VideoBoxApplication.java com/zipow/videobox/fragment/SettingAboutFragment.java us/zoom/zimmsg/chatlist/MMChatsListFragment.java |
| 00078 | Get the network operator name | collection telephony | bo/app/hr.java |
| 00046 | Method reflection | reflection | org/mp4parser/aspectj/lang/Aspects14.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|------------|--|--------------------|--|
| 00023 | Start another application from current application | reflection control | com/zipow/videobox/auto/ZmAutoMeetingScreen\$onClickMeet\$1.java |
| 00092 | Send broadcast | command | us/zoom/proguard/qh3.java |
| 00002 | Open the camera and take picture | camera | com/zipow/nydus/camera/CameraCaptureImplV1.java |
| 00198 | Initialize the recorder and start recording | record | us/zoom/proguard/u12.java |

FIREBASE DATABASES ANALYSIS

| TITLE | SEVERITY | DESCRIPTION |
|--|----------|---|
| App talks to a Firebase database | info | The app talks to Firebase database at https://circle-medical-app-prod-48e03.firebaseio.com |
| Firebase Remote Config disabled | secure | Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/562966950786/namespaces/firebase:fetch? key=AlzaSyCfFdDLEnyuf2lmdkLdfKozsSPduZFUj0Q. This is indicated by the response: {'state': 'NO_TEMPLATE'} |

SECOND SECOND PERMISSIONS

| TYPE | MATCHES | PERMISSIONS |
|--------------------------------|---------|---|
| Malware Permissions | 13/25 | android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.READ_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_WIFI_STATE, android.permission.READ_PHONE_STATE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.RECEIVE_BOOT_COMPLETED |
| Other Common Permissions | 10/44 | android.permission.FLASHLIGHT, android.permission.READ_CALENDAR, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.BROADCAST_STICKY, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE |

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

• OFAC SANCTIONED COUNTRIES

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

| DOMAIN | COUNTRY/REGION |
|--------|----------------|
|--------|----------------|

Q DOMAIN MALWARE CHECK

| DOMAIN | STATUS | GEOLOCATION |
|----------------------------|--------|---|
| merchant-ui-api.stripe.com | ok | IP: 44.236.89.158 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map |
| maps.googleapis.com | ok | IP: 142.251.40.234 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map |
| link.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 |
| docs.withpersona.com | ok | IP: 64.239.109.1 Country: Canada Region: Ontario City: Etobicoke Latitude: 43.623768 Longitude: -79.559723 View: Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|--------------------|--------|---|
| withpersona.com | ok | IP: 172.66.1.36 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map |
| api.stripe.com | ok | IP: 54.149.153.72 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map |
| support.google.com | ok | IP: 142.251.40.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map |
| 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 |
|----------------------|--------|---|
| www.zetetic.net | ok | IP: 18.238.96.30 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map |
| sdk.iad-01.braze.com | ok | IP: 104.18.39.68 Country: United States of America Region: Texas City: Dallas Latitude: 32.783058 Longitude: -96.806671 View: Google Map |
| xml.org | ok | IP: 104.239.142.8 Country: United States of America Region: Texas City: Windcrest Latitude: 29.499678 Longitude: -98.399246 View: Google Map |
| play.google.com | ok | IP: 142.250.81.238 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: 104.18.23.19 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map |
| app.circlemedical.co | ok | IP: 44.193.158.102 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map |
| github.com | ok | IP: 140.82.114.4 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map |
| sdk-metrics.dev-rudder.rudderlabs.com | ok | IP: 54.204.10.2 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 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 |
| android.asset | ok | No Geolocation information available. |
| errors.stripe.com | ok | IP: 198.137.150.41 Country: United States of America Region: Ohio City: Miamisburg Latitude: 39.630859 Longitude: -84.262108 View: Google Map |
| booking-v2.circlemedical.com | ok | IP: 104.21.96.1 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map |
| www.smpte-ra.org | ok | IP: 52.20.185.129 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---|--------|--|
| circlemedical-production.s3.us-west-1.amazonaws.com | ok | IP: 16.15.4.108 Country: United States of America Region: California City: Palo Alto Latitude: 37.409912 Longitude: -122.160400 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 |
| www.google.com | ok | IP: 142.250.176.196 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 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 |

| DOMAIN | STATUS | GEOLOCATION |
|--|--------|---|
| 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 |
| www.slf4j.org | ok | IP: 31.97.181.89 Country: United Kingdom of Great Britain and Northern Ireland Region: England City: Bowness-on-Windermere Latitude: 54.363312 Longitude: -2.918590 View: Google Map |
| circle-medical-app-prod-48e03.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.braze.com | ok | IP: 104.17.227.60 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|----------------------------------|--------|---|
| zoomus.zendesk.com | ok | IP: 216.198.53.2 Country: United States of America Region: California City: San Francisco Latitude: 37.773968 Longitude: -122.410446 View: Google Map |
| files.stripe.com | ok | IP: 44.236.89.158 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map |
| inquiry-fallback.withpersona.com | ok | IP: 34.111.150.223 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map |
| ppm.stripe.com | ok | IP: 35.167.54.49 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---------------------------------|--------|--|
| sondheim.braze.com | ok | IP: 172.64.144.252 Country: United States of America Region: Texas City: Dallas Latitude: 32.783058 Longitude: -96.806671 View: Google Map |
| assets-global.website-files.com | ok | IP: 104.18.34.201 Country: United States of America Region: Texas City: Dallas Latitude: 32.783058 Longitude: -96.806671 View: Google Map |
| m.stripe.com | ok | IP: 35.162.234.202 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map |
| api.rudderlabs.com | ok | IP: 18.238.96.121 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|-------------------|--------|---|
| link.co | ok | IP: 13.224.53.31 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map |
| docs.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 |
| www.example.com | ok | IP: 23.204.146.201 Country: United States of America Region: California City: Los Angeles Latitude: 34.052231 Longitude: -118.243683 View: Google Map |
| cdn.growthbook.io | ok | IP: 151.101.1.91 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|------------------------|--------|---|
| 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 |
| checkout.link.com | ok | IP: 18.238.96.126 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map |
| javax.xml.xmlconstants | ok | No Geolocation information available. |
| 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 |
| xml.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 |
|-------------------------------------|--------|---|
| app.circlemedical.com | ok | IP: 34.192.45.56 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map |
| www.circlemedical.com | ok | IP: 104.21.112.1 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map |
| iamcache.braze | ok | No Geolocation information available. |
| support.stripe.com | ok | IP: 198.202.176.161 Country: United States of America Region: New York City: New York City Latitude: 40.797550 Longitude: -73.946190 View: Google Map |
| dust.k8s.test-001.d-usw-2.braze.com | ok | No Geolocation information available. |

| DOMAIN | STATUS | GEOLOCATION |
|-------------------|--------|--|
| circlemedical.com | ok | IP: 104.21.80.1 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map |
| hooks.stripe.com | ok | IP: 54.187.175.68 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map |
| api.iterable.com | ok | IP: 54.236.93.246 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map |
| docs.bugsnag.com | ok | IP: 18.155.173.70 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map |

Т

| DOMAIN | STATUS | GEOLOCATION |
|---------------------------------|--------|--|
| 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 |
| q.stripe.com | ok | IP: 54.186.23.98 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map |
| ktor.io | ok | IP: 13.224.53.49 Country: United States of America Region: Arizona City: Phoenix Latitude: 33.448380 Longitude: -112.074043 View: Google Map |
| webrtc-consumer.withpersona.com | ok | IP: 172.66.1.36 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map |

Т

| DOMAIN | STATUS | GEOLOCATION |
|-----------------------|--------|---|
| 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 |
| www.zoomgov.com | ok | IP: 160.1.56.156 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 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 |
| hosted.rudderlabs.com | ok | IP: 52.6.8.140 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map |

Т

| 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 |
| 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 |
| sdk-metrics.rudderstack.com | ok | IP: 3.229.143.19 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map |
| r.stripe.com | ok | IP: 54.186.23.98 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 View: Google Map |



| EMAIL | FILE |
|--|---|
| support@circlemedical.com | co/circlemedical/android/view/screens/guests/AccountVerificationFragment.java |
| this@copy.slice | io/ktor/util/NIOKt.java |
| 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/networking/FraudDetectionDataRequest.java |
| support@stripe.com | com/stripe/android/core/exception/APIConnectionException.java |
| support@stripe.com | com/stripe/android/core/networking/ApiRequest.java |
| email@email.com | com/stripe/android/paymentsheet/paymentdatacollection/bacs/ComposableSingletons\$BacsMandateConfirmationFormKt.ja va |
| 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 |
| zdc.pr@zoom.us no-reply@zoom.us support@stripe.com user@example.com | Android String Resource |



| 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 |
|---|
| "biometric_auth_failed_logout_cta" : "Logout" |
| "biometric_auth_failed_unlock_cta" : "Unlock" |
| "biometric_auth_negative_button" : "Cancel" |
| "com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key" |
| "com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key" |
| "com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key" |
| "firebase_database_url" : "https://circle-medical-app-prod-48e03.firebaseio.com" |
| "google_api_key" : "AlzaSyCfFdDLEnyuf2lmdkLdfKozsSPduZFUj0Q" |

| POSSIBLE SECRETS |
|---|
| "google_crash_reporting_api_key" : "AlzaSyCfFdDLEnyuf2lmdkLdfKozsSPduZFUj0Q" |
| "google_geo_api_key" : "AlzaSyDqWTGLLrgtERP1Q-yyE2GYL-8bsZ-C54U" |
| "library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/" |
| "sign_up_password" : "Password" |
| "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"

DB7C2ABF62E35E668076BEAD2088

0400FAC9DFCBAC8313BB2139F1BB755FEF65BC391F8B36F8F8EB7371FD558B01006A08A41903350678E58528BEBF8A0BEFF867A7CA36716F7E01F81052

41058363725152142129326129780047268409114441015993725554835256314039467401291

0400D9B67D192E0367C803F39E1A7E82CA14A651350AAE617E8F01CE94335607C304AC29E7DEFBD9CA01F596F927224CDECF6C

3FA8124359F96680B83D1C3EB2C070E5C545C9858D03ECFB744BF8D717717EFC

E95E4A5F737059DC60DFC7AD95B3D8139515620F

0620048D28BCBD03B6249C99182B7C8CD19700C362C46A01

2580F63CCFE44138870713B1A92369E33E2135D266DBB372386C400B

74D59FF07F6B413D0FA14B344B20A2DB049B50C3

26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6

0370F6E9D04D289C4E89913CE3530BFDE903977D42B146D539BF1BDE4E9C92

046AB1E344CE25FF3896424E7FFE14762ECB49F8928AC0C76029B4D5800374E9F5143E568CD23F3F4D7C0D4B1E41C8CC0D1C6ABD5F1A46DB4C

04AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25DBF55296C3A545E3872760AB73617DE4A96262C6F5D9E98BF9292DC29F 8F41DBD289A147CE9DA3113B5F0B8C00A60B1CE1D7E819D7A431D7C90EA0E5F

FFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3D F1FD5D5FD65612433F51F5F066FD0856365553DFD1AF3B557135F7F57C935984F0C70F0F68B77F2A689DAF3FFF8721DF158A136ADF73530ACCA4F483A797ABC0AB1 82B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9C E98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99 C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF6 9EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B 6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1 A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23 BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855 322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C 1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C 6272B045B3B71F9DC6B80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CCFF46AAA36AD004CF600C8381E425A31D951AE64FDB23FCEC 9509D43687FEB69EDD1CC5E0B8CC3BDF64B10EF86B63142A3AB8829555B2F747C932665CB2C0F1CC01BD70229388839D2AF05E454504AC78B7582822846C0BA35C 35F5C59160CC046FD8251541FC68C9C86B022BB7099876A460E7451A8A93109703FEE1C217E6C3826E52C51AA691E0E423CFC99E9E31650C1217B624816CDAD9A95 F9D5B8019488D9C0A0A1FE3075A577E23183F81D4A3F2FA4571EFC8CE0BA8A4FE8B6855DFE72B0A66EDED2FBABFBE58A30FAFABE1C5D71A87E2F741EF8C1FE86FEA

1E589A8595423412134FAA2DBDEC95C8D8675E58

| POSSIBLE SECRETS |
|---|
| 04A1455B334DF099DF30FC28A169A467E9E47075A90F7E650EB6B7A45C7E089FED7FBA344282CAFBD6F7E319F7C0B0BD59E2CA4BDB556D61A5 |
| A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377 |
| MQVwithSHA512KDFAndSharedInfo |
| 000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F |
| 26617408020502170632287687167233609607298591687569731477066713684188029449964278084915450806277719023520942412250655586621571135455709 16814161637315895999846 |
| 04B8266A46C55657AC734CE38F018F2192 |
| F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C03 |
| 883423532389192164791648750360308885314476597252960362792450860609699839 |
| 9cdbd84c9f1ac2f38d0f80f42ab952e7338bf511 |
| 115792089210356248762697446949407573529996955224135760342422259061068512044369 |
| 2866537B676752636A68F56554E12640276B649EF7526267 |
| FC1217D4320A90452C760A58EDCD30C8DD069B3C34453837A34ED50CB54917E1C2112D84D164F444F8F74786046A |

91A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C40094DBACDB586FB20

3FCDA526B6CDF83BA1118DF35B3C31761D3545F32728D003EEB25EFE96

3045AE6FC8422F64ED579528D38120EAE12196D5

AC6BDB41324A9A9BF166DE5E1389582FAF72B6651987EE07FC3192943DB56050A37329CBB4A099ED8193E0757767A13DD52312AB4B03310DCD7F48A9DA04FD50E 8083969EDB767B0CF6095179A163AB3661A05FBD5FAAAE82918A9962F0B93B855F97993EC975EEAA80D740ADBF4FF747359D041D5C33EA71D281E446B14773BCA9 7B43A23FB801676BD207A436C6481F1D2B9078717461A5B9D32E688F87748544523B524B0D57D5EA77A2775D2ECFA032CFBDBF52FB3786160279004E57AE6AF874E 7303CE53299CCC041C7BC308D82A5698F3A8D0C38271AE35F8E9DBFBB694B5C803D89F7AE435DE236D525F54759B65E372FCD68EF20FA7111F9E4AFF73

04188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF101207192B95FFC8DA78631011ED6B24CDD573F977A11E794811

10938490380737342745111123907668055699362075989516837489945863944959531161507350160137087375737596232485921322967063133094384525315910 12912142327488478985984

04A8C7DD22CE28268B39B55416F0447C2FB77DE107DCD2A62E880EA53EEB62D57CB4390295DBC9943AB78696FA504C11

64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1

0101D556572AABAC800101D556572AABAC8001022D5C91DD173F8FB561DA6899164443051D

39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643

F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C00

5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B

07A526C63D3E25A256A007699F5447E32AE456B50E

7503CFE87A836AE3A61B8816E25450E6CE5E1C93ACF1ABC1778064FDCBEFA921DF1626BE4FD036E93D75E6A50E3A41E98028FE5FC235F5B889A589CB5215F2A4

0307AF69989546103D79329FCC3D74880F33BBE803CB

04A3E8EB3CC1CFE7B7732213B23A656149AFA142C47AAFBC2B79A191562E1305F42D996C823439C56D7F7B22E14644417E69BCB6DE39D027001DABE8F35B25C9BE

790408F2EEDAF392B012EDEFB3392F30F4327C0CA3F31FC383C422AA8C16

3045AE6FC8422f64ED579528D38120EAE12196D5

10686D41FF744D4449FCCF6D8EEA03102E6812C93A9D60B978B702CF156D814EF

64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1

0257927098FA932E7C0A96D3FD5B706EF7E5F5C156E16B7E7C86038552E91D

0238af09d98727705120c921bb5e9e26296a3cdcf2f35757a0eafd87b830e7

FFFFFFF00000000FFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551

fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17

27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575

0479BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B

00F50B028E4D696E676875615175290472783FB1

fffffff00000000fffffffffffffbce6faada7179e84f3b9cac2fc632551

678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4

662C61C430D84EA4FE66A7733D0B76B7BF93EBC4AF2F49256AE58101FEE92B04

POSSIBLE SECRETS B4E134D3FB59EB8BAB57274904664D5AF50388BA 02A29EF207D0E9B6C55CD260B306C7E007AC491CA1B10C62334A9E8DCD8D20FB7 040369979697AB43897789566789567F787A7876A65400435EDB42EFAFB2989D51FEFCE3C80988F41FF883 42debb9da5b3d88cc956e08787ec3f3a09bba5f48b889a74aaf53174aa0fbe7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76 137e792f3f0db859d095e4a5b932024f079ecf2ef09c797452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94cccf1449ac43d586 d0beee43251b0b2287349d68de0d144403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1b27d0639f695e347d8d1cf9ac819a26ca9b04cb0eb9b7b 035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffbc97134025fe8ce04c4399ad96569be91a546f4978693c7a 2AA058F73A0E33AB486B0F610410C53A7F132310 4099B5A457F9D69F79213D094C4BCD4D4262210B 040081BAF91FDF9833C40F9C181343638399078C6E7EA38C001F73C8134B1B4EF9E150 91E38443A5E82C0D880923425712B2BB658B9196932E02C78B2582FE742DAA28 A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5374 7d7374168ffe3471b60a857686a19475d3bfa2ff 3826F008A8C51D7B95284D9D03FF0F00CF2CD723A 6db14acc9e21c820ff28b1d5ef5de2b0 985BD3ADBAD4D696F676875615175A21B43A97F3 048BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F04699

| POSSIBLE SECRETS |
|--|
| 3086d221a7d46bcde86c90e49284eb15 |
| b8adf1378a6eb73409fa6c9c637ba7f5 |
| 9760508f15230bccb292b982a2eb840bf0581cf5 |
| AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F0 |
| 010092537397ECA4F6145799D62B0A19CE06FE26AD |
| 714114B762F2FF4A7912A6D2AC58B9B5C2FCFE76DAEB7129 |
| 68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166 43812574028291115057151 |
| FD0D693149A118F651E6DCE6802085377E5F882D1B510B44160074C1288078365A0396C8E681 |
| E95E4A5F737059DC60DF5991D45029409E60FC09 |
| 10E723AB14D696E6768756151756FEBF8FCB49A9 |
| 041D1C64F068CF45FFA2A63A81B7C13F6B8847A3E77EF14FE3DB7FCAFE0CBD10E8E826E03436D646AAEF87B2E247D4AF1E8ABE1D7520F9C2A45CB1EB8E95CFD5526 2B70B29FEEC5864E19C054FF99129280E4646217791811142820341263C5315 |
| 044AD5F7048DE709AD51236DE65E4D4B482C836DC6E410664002BB3A02D4AAADACAE24817A4CA3A1B014B5270432DB27D2 |
| 020ffa963cdca8816ccc33b8642bedf905c3d358573d3f27fbbd3b3cb9aaaf |
| 6b8cf07d4ca75c88957d9d670591 |
| 71FE1AF926CF847989EFEF8DB459F66394D90F32AD3F15E8 |

043AE9E58C82F63C30282E1FE7BBF43FA72C446AF6F4618129097E2C5667C2223A902AB5CA449D0084B7E5B3DE7CCC01C9 5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b 216EE8B189D291A0224984C1E92F1D16BF75CCD825A087A239B276D3167743C52C02D6E7232AA 3086d221a7d46bcde86c90e49284eb153dab A2B55680-6F43-11E0-9A3F-0002A5D5C51B 3E1AF419A269A5F866A7D3C25C3DF80AE979259373FF2B182F49D4CE7E1BBC8B 0021A5C2C8EE9FEB5C4B9A753B7B476B7FD6422EF1F3DD674761FA99D6AC27C8A9A197B272822F6CD57A55AA4F50AE317B13545F 0402FE13C0537BBC11ACAA07D793DE4E6D5E5C94EEE80289070FB05D38FF58321F2E800536D538CCDAA3D9 26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087 5667676A654B20754F356EA92017D946567C46675556F19556A04616B567D223A5E05656FB549016A96656A557 C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86297 4D696E676875615175985BD3ADBADA21B43A97E2 A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7 0429A0B6A887A983E9730988A68727A8B2D126C44CC2CC7B2A6555193035DC76310804F12E549BDB011C103089E73510ACB275FC312A5DC6B76553F0CA

D35E472036BC4FB7E13C785ED201E065F98FCFA5B68F12A32D482EC7EE8658E98691555B44C59311

020A601907B8C953CA1481EB10512F78744A3205FD

1A8F7EDA389B094C2C071E3647A8940F3C123B697578C213BE6DD9E6C8EC7335DCB228FD1EDF4A39152CBCAAF8C0398828041055F94CEEEC7E21340780FE41BD

32879423AB1A0375895786C4BB46E9565FDE0B5344766740AF268ADB32322E5C

A59A749A11242C58C894E9E5A91804E8FA0AC64B56288F8D47D51B1EDC4D65444FECA0111D78F35FC9FDD4CB1F1B79A3BA9CBEE83A3F811012503C8117F98E5048 B089E387AF6949BF8784EBD9EF45876F2E6A5A495BE64B6E770409494B7FEE1DBB1E4B2BC2A53D4F893D418B7159592E4FFFDF6969E91D770DAEBD0B5CB14C00AD 68EC7DC1E5745EA55C706C4A1C5C88964E34D09DEB753AD418C1AD0F4FDFD049A955E5D78491C0B7A2F1575A008CCD727AB376DB6E695515B05BD412F5B8C2F4C 77EE10DA48ABD53F5DD498927EE7B692BBBCDA2FB23A516C5B4533D73980B2A3B60E384ED200AE21B40D273651AD6060C13D97FD69AA13C5611A51B9085

71169be7330b3038edb025f1

5E5CBA992E0A680D885EB903AEA78E4A45A469103D448EDE3B7ACCC54D521E37F84A4BDD5B06B0970CC2D2BBB715F7B82846F9A0C393914C792E6A923E2117AB8 05276A975AADB5261D91673EA9AAFFEECBFA6183DFCB5D3B7332AA19275AFA1F8EC0B60FB6F66CC23AE4870791D5982AAD1AA9485FD8F4A60126FEB2CF05DB8A7F 0F09B3397F3937F2E90B9E5B9C9B6EFEF642BC48351C46FB171B9BFA9EF17A961CE96C7E7A7CC3D3D03DFAD1078BA21DA425198F07D2481622BCE45969D9C4D606 3D72AB7A0F08B2F49A7CC6AF335E08C4720E31476B67299E231F8BD90B39AC3AE3BE0C6B6CACEF8289A2E2873D58E51E029CAFBD55E6841489AB66B5B4B9BA6E2F 784660896AFF387D92844CCB8B69475496DE19DA2E58259B090489AC8E62363CDF82CFD8EF2A427ABCD65750B506F56DDE3B988567A88126B914D7828E2B63A6D7 ED0747EC59E0E0A23CE7D8A74C1D2C2A7AFB6A29799620F00E11C33787F7DED3B30E1A22D09F1FBDA1ABBBFBF25CAE05A13F812E34563F99410E73B

040503213F78CA44883F1A3B8162F188E553CD265F23C1567A16876913B0C2AC245849283601CCDA380F1C9E318D90F95D07E5426FE87E45C0E8184698E45962364E 34116177DD2259

37a6259cc0c1dae299a7866489dff0bd

00E8BEE4D3E2260744188BE0E9C723

 $13353181327272067343385951994831900121794237596784748689948235959936964252873471246159040332773182141032801252925387191478859899310331\\05677441361963648030647213778266568986864684632777101508094011826087702016153249904683329312949209127762411378780302243557466062839716\\59376426832674269780880061631528163475887$

B99B99B099B323E02709A4D696E6768756151751

90066455B5CFC38F9CAA4A48B4281F292C260FEEF01FD61037E56258A7795A1C7AD46076982CE6BB956936C6AB4DCFE05E6784586940CA544B9B2140E1EB523F009
D20A7E7880E4E5BFA690F1B9004A27811CD9904AF70420EEFD6EA11EF7DA129F58835FF56B89FAA637BC9AC2EFAAB903402229F491D8D3485261CD068699B6BA58A
1DDBBEF6DB51E8FE34E8A78E542D7BA351C21EA8D8F1D29F5D5D15939487E27F4416B0CA632C59EFD1B1EB66511A5A0FBF615B766C5862D0BD8A3FE7A0E0DA0FB
2FE1FCB19E8F9996A8EA0FCCDE538175238FC8B0EE6F29AF7F642773EBE8CD5402415A01451A840476B2FCEB0E388D30D4B376C37FE401C2A2C2F941DAD179C540C
1C8CE030D460C4D983BE9AB0B20F69144C1AE13F9383EA1C08504FB0BF321503EFE43488310DD8DC77EC5B8349B8BFE97C2C560EA878DE87C11E3D597F1FEA742D
73EEC7F37BE43949EF1A0D15C3F3E3FC0A8335617055AC91328EC22B50FC15B941D3D1624CD88BC25F3E941FDDC6200689581BFEC416B4B2CB73

03CE10490F6A708FC26DFE8C3D27C4F94E690134D5BFF988D8D28AAEAEDE975936C66BAC536B18AE2DC312CA493117DAA469C640CAF3

9B9F605F5A858107AB1EC85E6B41C8AACF846E86789051D37998F7B9022D759B

7d73d21f1bd82c9e5268b6dcf9fde2cb

AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F3

043B4C382CE37AA192A4019E763036F4F5DD4D7EBB938CF935318FDCED6BC28286531733C3F03C4FEE

79885141663410976897627118935756323747307951916507639758300472692338873533959

90EAF4D1AF0708B1B612FF35E0A2997EB9E9D263C9CE659528945C0D

8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a9 78d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f

00C9BB9E8927D4D64C377E2AB2856A5B16E3EFB7F61D4316AE

| POSSIBLE SECRETS |
|---|
| 8e722de3125bddb05580164bfe20b8b432216a62926c57502ceede31c47816edd1e89769124179d0b695106428815065 |
| D6031998D1B3BBFEBF59CC9BBFF9AEE1 |
| 2762c874eafb8e94376855402628e842 |
| b3fb3400dec5c4adceb8655d4c94 |
| 0401F481BC5F0FF84A74AD6CDF6FDEF4BF6179625372D8C0C5E10025E399F2903712CCF3EA9E3A1AD17FB0B3201B6AF7CE1B05 |
| 24B7B137C8A14D696E6768756151756FD0DA2E5C |
| F1FD178C0B3AD58F10126DE8CE42435B53DC67E140D2BF941FFDD459C6D655E1 |
| 030024266E4EB5106D0A964D92C4860E2671DB9B6CC5 |
| 10B7B4D696E676875615175137C8A16FD0DA2211 |
| 3EE30B568FBAB0F883CCEBD46D3F3BB8A2A73513F5EB79DA66190EB085FFA9F492F375A97D860EB4 |
| 9CA8B57A934C54DEEDA9E54A7BBAD95E3B2E91C54D32BE0B9DF96D8D35 |
| D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E24 |
| 37571800257700204635455072244911836035944551347697624866945677796155444774405563166912344050129455395621444445372894285225856667291965 80810124344277578376784 |
| 03F7061798EB99E238FD6F1BF95B48FEEB4854252B |
| 6b8cf07d4ca75c88957d9d67059037a4 |

| POSSIBLE SECRETS |
|---|
| AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA70330870553E5C414CA92619418661197FAC10471DB1D381085DDADDB58796829CA90069 |
| 5f6b901aaf8b0978eef1c05e18a8a2e1 |
| 962eddcc369cba8ebb260ee6b6a126d9346e38c5 |
| E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B |
| 051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00 |
| 0202F9F87B7C574D0BDECF8A22E6524775F98CDEBDCB |
| E0D2EE25095206F5E2A4F9ED229F1F256E79A0E2B455970D8D0D865BD94778C576D62F0AB7519CCD2A1A906AE30D |
| bb85691939b869c1d087f601554b96b80cb4f55b35f433c2 |
| 06973B15095675534C7CF7E64A21BD54EF5DD3B8A0326AA936ECE454D2C |
| 115792089210356248762697446949407573530086143415290314195533631308867097853948 |
| cc22d6dfb95c6b25e49c0d6364a4e5980c393aa21668d953 |
| 401028774D7777C7B7666D1366EA432071274F89FF01E718 |
| FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF |

| POSSIBLE SECRETS |
|--|
| 0481AEE4BDD82ED9645A21322E9C4C6A9385ED9F70B5D916C1B43B62EEF4D0098EFF3B1F78E2D0D48D50D1687B93B97D5F7C6D5047406A5E688B352209BCB9F82 27DDE385D566332ECC0EABFA9CF7822FDF209F70024A57B1AA000C55B881F8111B2DCDE494A5F485E5BCA4BD88A2763AED1CA2B2FA8F0540678CD1E0F3AD80892 |
| 044A96B5688EF573284664698968C38BB913CBFC8223A628553168947D59DCC912042351377AC5FB32 |
| db92371d2126e9700324977504e8c90e |
| b869c82b35d70e1b1ff91b28e37a62ecdc34409b |
| 659EF8BA043916EEDE8911702B22 |
| 0452DCB034293A117E1F4FF11B30F7199D3144CE6DFEAFFEF2E331F296E071FA0DF9982CFEA7D43F2E |
| 03E5A88919D7CAFCBF415F07C2176573B2 |
| edef8ba9-79d6-4ace-a3c8-27dcd51d21ed |
| 04026EB7A859923FBC82189631F8103FE4AC9CA2970012D5D46024804801841CA44370958493B205E647DA304DB4CEB08CBBD1BA39494776FB988B47174DCA88C7 E2945283A01C89720349DC807F4FBF374F4AEADE3BCA95314DD58CEC9F307A54FFC61EFC006D8A2C9D4979C0AC44AEA74FBEBBB9F772AEDCB620B01A7BA7AF1B32 0430C8591984F601CD4C143EF1C7A3 |
| D2C0FB15760860DEF1EEF4D696E6768756151754 |
| 255705fa2a306654b1f4cb03d6a750a30c250102d4988717d9ba15ab6d3e |
| 32010857077C5431123A46B808906756F543423E8D27877578125778AC76 |
| 4D41A619BCC6EADF0448FA22FAD567A9181D37389CA |
| 0017858FEB7A98975169E171F77B4087DE098AC8A911DF7B01 |

| POSSIBLE SECRETS | | |
|--|--|--|
| MQVwithSHA256KDFAndSharedInfo | | |
| CFA0478A54717B08CE64805B76E5B14249A77A4838469DF7F7DC987EFCCFB11D | | |
| 469A28EF7C28CCA3DC721D044F4496BCCA7EF4146FBF25C9 | | |
| aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7 | | |
| 01AF286BCA1AF286BCA1AF286BCA1AF286BC9FB8F6B85C556892C20A7EB964FE7719E74F490758D3B | | |
| 41ECE55743711A8C3CBF3783CD08C0EE4D4DC440D4641A8F366E550DFDB3BB67 | | |
| 85E25BFE5C86226CDB12016F7553F9D0E693A268 | | |
| 77E2B07370EB0F832A6DD5B62DFC88CD06BB84BE | | |
| 0713612DCDDCB40AAB946BDA29CA91F73AF958AFD9 | | |
| 77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399 | | |
| 04B199B13B9B34EFC1397E64BAEB05ACC265FF2378ADD6718B7C7C1961F0991B842443772152C9E0AD | | |
| BB8E5E8FBC115E139FE6A814FE48AAA6F0ADA1AA5DF91985 | | |
| D09E8800291CB85396CC6717393284AAA0DA64BA | | |
| ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n | | |
| 6BA06FE51464B2BD26DC57F48819BA9954667022C7D03 | | |

POSSIBLE SECRETS 8d5155894229d5e689ee01e6018a237e2cae64cd 520883949DFDBC42D3AD198640688A6FE13F41349554B49ACC31DCCD884539816F5EB4AC8FB1F1A6 e43bb460f0b80cc0c0b075798e948060f8321b7d 7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9 0418DE98B02DB9A306F2AFCD7235F72A819B80AB12EBD653172476FECD462AABFFC4FF191B946A5F54D8D0AA2F418808CC25AB056962D30651A114AFD2755AD33 6747F93475B7A1FCA3B88F2B6A208CCFE469408584DC2B2912675BF5B9E582928 C196BA05AC29E1F9C3C72D56DFFC6154A033F1477AC88EC37F09BE6C5BB95F51C296DD20D1A28A067CCC4D4316A4BD1DCA55ED1066D438C35AEBAABF57E7DAE4 28782A95ECA1C143DB701FD48533A3C18F0FE23557EA7AE619ECACC7E0B51652A8776D02A425567DED36EABD90CA33A1E8D988F0BBB92D02D1D20290113BB562C E1FC856EEB7CDD92D33EEA6F410859B179E7E789A8F75F645FAE2E136D252BFFAFF89528945C1ABE705A38DBC2D364AADE99BE0D0AAD82E5320121496DC65B3930 E38047294FF877831A16D5228418DE8AB275D7D75651CEFED65F78AFC3EA7FE4D79B35F62A0402A1117599ADAC7B269A59F353CF450E6982D3B1702D9CA83 6132838810ceebe08d96644a 65e73ee0bcfb089df0e1adbe 0443BD7E9AFB53D8B85289BCC48EE5BFE6F20137D10A087EB6E7871E2A10A599C710AF8D0D39E2061114FDD05545EC1CC8AB4093247F77275E0743FFED117182EAA 9C77877AAAC6AC7D35245D1692E8EE1 00FDFB49BFE6C3A89FACADAA7A1E5BBC7CC1C2E5D831478814 00C9517D06D5240D3CFF38C74B20B6CD4D6F9DD4D9 023b1660dd701d0839fd45eec36f9ee7b32e13b315dc02610aa1b636e346df671f790f84c5e09b05674dbb7e45c803dd 517cc1b727220a94fe13abe8fa9a6ee0

7A1F6653786A68192803910A3D30B2A2018B21CD54

1CEF494720115657E18F938D7A7942394FF9425C1458C57861F9EEA6ADBE3BE10

fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7

32670510020758816978083085130507043184471273380659243275938904335757337482424

95475cf5d93e596c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bbdd84c9836be1f31c0777725aeb6c2fc38b85f48076fa76bcd8146cc89a6fb2f706 dd719898c2083dc8d896f84062e2c9c94d137b054a8d8096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9eb60eee8b030376b236bc 73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520086746175c8885925ebc64c6147906773496990cb714ec 667304e261faee33b3cbdf008e0c3fa90650d97d3909c9275bf4ac86ffcb3d03e6dfc8ada5934242dd6d3bcca2a406cb0b

0217C05610884B63B9C6C7291678F9D341

6C01074756099122221056911C77D77E77A777E7E7E77FCB

021085F2755381DCCCF3C1557AFA10C2F0C0C2825646C5B34A394CBCFA8BC16B22F7F789F927BF216F02F1FB136A5F

115792089210356248762697446949407573530086143415290314195533631308867097853951

D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FF

04B6B3D4C356C139EB31183D4749D423958C27D2DCAF98B70164C97A2DD98F5CFF6142E0F7C8B204911F9271F0F3ECEF8C2701C307E8E4C9E183115A1554062CFB

| POSSIBLE SECRETS |
|--|
| 68647976601306097149819007990813932172694353001433054093944634591855431833976553942450577463332171975329639963713633211138647686124403 80340372808892707005449 |
| 4A6E0856526436F2F88DD07A341E32D04184572BEB710 |
| 03eea2bae7e1497842f2de7769cfe9c989c072ad696f48034a |
| 7F519EADA7BDA81BD826DBA647910F8C4B9346ED8CCDC64E4B1ABD11756DCE1D2074AA263B88805CED70355A33B471EE |
| 7fffffffffffffffffffff800000cfa7e8594377d414c03821bc582063 |
| C8619ED45A62E6212E1160349E2BFA844439FAFC2A3FD1638F9E |
| 30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d2029d83c1c1585 47f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346d3f529252 |
| 0051953EB9618E1C9A1F929A21A0B68540EEA2DA725B99B315F3B8B489918EF109E156193951EC7E937B1652C0BD3BB1BF073573DF883D2C34F1EF451FD46B503F0 |
| BDB6F4FE3E8B1D9E0DA8C0D46F4C318CEFE4AFE3B6B8551F |
| 258EAFA5-E914-47DA-95CA-C5AB0DC85B11 |
| 0066647EDE6C332C7F8C0923BB58213B333B20E9CE4281FE115F7D8F90AD |
| 295F9BAE7428ED9CCC20E7C359A9D41A22FCCD9108E17BF7BA9337A6F8AE9513 |
| |

5D9306BACD22B7FAEB09D2E049C6E2866C5D1677762A8F2F2DC9A11C7F7BE8340AB2237C7F2A0

040303001D34B856296C16C0D40D3CD7750A93D1D2955FA80AA5F40FC8DB7B2ABDBDE53950F4C0D293CDD711A35B67FB1499AE60038614F1394ABFA3B4C850D9 27E1E7769C8EEC2D19037BF27342DA639B6DCCFFFEB73D69D78C6C27A6009CBBCA1980F8533921E8A684423E43BAB08A576291AF8F461BB2A8B3531D2F0485C19B 16E2F1516E23DD3C1A4827AF1B8AC15B

1b9fa3e518d683c6b65763694ac8efbaec6fab44f2276171a42726507dd08add4c3b3f4c1ebc5b1222ddba077f722943b24c3edfa0f85fe24d0c8c01591f0be6f63

0095E9A9EC9B297BD4BF36E059184F

1A62BA79D98133A16BBAE7ED9A8E03C32E0824D57AEF72F88986874E5AAE49C27BED49A2A95058068426C2171E99FD3B43C5947C857D

9A04F079-9840-4286-AB92-E65BE0885F95

7A556B6DAE535B7B51ED2C4D7DAA7A0B5C55F380

28E9FA9E9D9F5E344D5A9E4BCF6509A7F39789F515AB8F92DDBCBD414D940E93

25FBC363582DCEC065080CA8287AAFF09788A66DC3A9E

43FC8AD242B0B7A6F3D1627AD5654447556B47BF6AA4A64B0C2AFE42CADAB8F93D92394C79A79755437B56995136

5363ad4cc05c30e0a5261c028812645a122e22ea20816678df02967c1b23bd72

EEAF0AB9ADB38DD69C33F80AFA8FC5E86072618775FF3C0B9EA2314C9C256576D674DF7496EA81D3383B4813D692C6E0E0D5D8E250B98BE48E495C1D6089DAD15 DC7D7B46154D6B6CE8EF4AD69B15D4982559B297BCF1885C529F566660E57EC68EDBC3C05726CC02FD4CBF4976EAA9AFD5138FE8376435B9FC61D2FC0EB06E3

0101BAF95C9723C57B6C21DA2EFF2D5ED588BDD5717E212F9D

9B9F605F5A858107AB1FC85F6B41C8AACF846F86789051D37998F7B9022D7598

9B9F605F5A858107AB1FC85F6B41C8AA582CA3511FDDFB74F02F3A6598980BB9

91771529896554605945588149018382750217296858393520724172743325725474374979801

96341f1138933bc2f503fd44

 $14201174159756348119636828602231808974327613839524373876287257344192745939351271897363116607846760036084894662356762579528277471921224\\19290710461342083806363940845126918288940005715246254452957693493567527289568315417754417631393844571917550968471078465956625479423122\\93338483924514339614727760681880609734239$

A335926AA319A27A1D00896A6773A4827ACDAC73

1AB597A5B4477F59E39539007C7F977D1A567B92B043A49C6B61984C3FE3481AAF454CD41BA1F051626442B3C10

0409487239995A5EE76B55F9C2F098A89CE5AF8724C0A23E0E0FF77500

6b016c3bdcf18941d0d654921475ca71a9db2fb27d1d37796185c2942c0a

c469684435deb378c4b65ca9591e2a5763059a2e

340E7BE2A280EB74E2BE61BADA745D97E8F7C300

308201e53082014ea00302010202044faa0a6b300d06092a864886f70d01010505003036310b300906035504061302555331273025060355040a131e5a6f6f6d20566964 656f20436f6d6d756e69636174696f6e7320496e632e3020170d3132303530393036313035315a180f32303632303432373036313035315a3036310b3009060355040613 02555331273025060355040a131e5a6f6f6d20566964656f20436f6d6d756e69636174696f6e7320496e632e30819f300d06092a864886f70d010101050003818d0030818 9028181009b463f2d26827dcd115aecc70e5124b9d68cd78e401489c9eae4cd19bc4ca0576ad28168a81f71e8d8b5a7cdc956d937510df3cfa956c28d55668894c33ce080 52946ae4af1455becfd2243897f1731fd17a547260c5a52daaebf8ab8a9aad1ad18f99ff696dcf7d713f6540f102c274fbfbc895045f25af67d0fe8dedc536510203010001300 d06092a864886f70d0101050500038181000db7990467b840f362bad88c35874abe4d10d3a872356e57581f06fcbac79ebf6d82bb380d14461eded133d9630d77a6b7bcc 9953f1ab02437c6317646218b6a37f3c75e833096fa24a473a9b53b1cca4269f0c753ec33239c9a293ea87c27121f424cb9ec1d7765c7fc0c51b7ee2ec4ab9d15a896eeb150 ac06fe67086f1c70

e423f053-51f6-430f-a04b-f2bff92b389b

68363196144955700784444165611827252895102170888761442055095051287550314083023

7CBBBCF9441CFAB76E1890E46884EAE321F70C0BCB4981527897504BEC3E36A62BCDFA2304976540F6450085F2DAE145C22553B465763689180EA2571867423E

0228F9D04E900069C8DC47A08534FE76D2B900B7D7EF31F5709F200C4CA205

040060F05F658F49C1AD3AB1890F7184210EFD0987E307C84C27ACCFB8F9F67CC2C460189EB5AAAA62EE222EB1B35540CFE902374601E369050B7C4E42ACBA1DACB F04299C3460782F918EA427E6325165E9EA10E3DA5F6C42E9C55215AA9CA27A5863EC48D8E0286B

000E0D4D696E6768756151750CC03A4473D03679

F5CE40D95B5EB899ABBCCFF5911CB8577939804D6527378B8C108C3D2090FF9BE18E2D33E3021ED2EF32D85822423B6304F726AA854BAE07D0396E9A9ADDC40F

7830A3318B603B89E2327145AC234CC594CBDD8D3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CA

3d84f26c12238d7b4f3d516613c1759033b1a5800175d0b1

2E2F85F5DD74CE983A5C4237229DAF8A3F35823BE

6A91174076B1E0E19C39C031FE8685C1CAE040E5C69A28EF

42941826148615804143873447737955502392672345968607143066798112994089471231420027060385216699563848719957657284814898909770759462613437 66945636488273037083893479108083593264797677860191534347440096103423131667257868692048219493287863336020338479709268434224762105576023 5016132614780652761028509445403338652341

 $68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166\\43812574028291115057148$

114ca50f7a8e2f3f657c1108d9d44cfd8

48439561293906451759052585252797914202762949526041747995844080717082404635286

04009D73616F35F4AB1407D73562C10F00A52830277958EE84D1315ED31886

| POSSIBLE SECRETS |
|--|
| DB7C2ABF62E35E7628DFAC6561C5 |
| 07A11B09A76B562144418FF3FF8C2570B8 |
| 1A827EF00DD6FC0E234CAF046C6A5D8A85395B236CC4AD2CF32A0CADBDC9DDF620B0EB9906D0957F6C6FEACD615468DF104DE296CD8F |
| MQVwithSHA384KDFAndSharedInfo |
| 072546B5435234A422E0789675F432C89435DE5242 |
| 047B6AA5D85E572983E6FB32A7CDEBC14027B6916A894D3AEE7106FE805FC34B44 |
| E2E31EDFC23DE7BDEBE241CE593EF5DE2295B7A9CBAEF021D385F7074CEA043AA27272A7AE602BF2A7B9033DB9ED3610C6FB85487EAE97AAC5BC7928C1950148 |
| 0432C4AE2C1F1981195F9904466A39C9948FE30BBFF2660BE1715A4589334C74C7BC3736A2F4F6779C59BDCEE36B692153D0A9877CC62A474002DF32E52139F0A0 |
| 22123dc2395a05caa7423daeccc94760a7d462256bd56916 |
| 9DEF3CAFB939277AB1F12A8617A47BBBDBA51DF499AC4C80BEEEA9614B19CC4D5F4F5F556E27CBDE51C6A94BE4607A291558903BA0D0F84380B655BB9A22E8DCD F028A7CEC67F0D08134B1C8B97989149B609E0BE3BAB63D47548381DBC5B1FC764E3F4B53DD9DA1158BFD3E2B9C8CF56EDF019539349627DB2FD53D24B7C48665 772E437D6C7F8CE442734AF7CCB7AE837C264AE3A9BEB87F8A2FE9B8B5292E5A021FFF5E91479E8CE7A28C2442C6F315180F93499A234DCF76E3FED135F9BB |
| 04B70E0CBD6BB4BF7F321390B94A03C1D356C21122343280D6115C1D21BD376388B5F723FB4C22DFE6CD4375A05A07476444D5819985007E34 |
| 108576C80499DB2FC16EDDF6853BBB278F6B6FB437D9 |
| 0163F35A5137C2CE3EA6ED8667190B0BC43ECD69977702709B |
| 23456789abcdefghjkmnpqrstvwxyz |
| 03188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012 |

1854BEBDC31B21B7AEFC80AB0ECD10D5B1B3308E6DBF11C1

04640ECE5C12788717B9C1BA06CBC2A6FEBA85842458C56DDE9DB1758D39C0313D82BA51735CDB3EA499AA77A7D6943A64F7A3F25FE26F06B51BAA2696FA9035D A5B534BD595F5AF0FA2C892376C84ACE1BB4E3019B71634C01131159CAE03CEE9D9932184BEEF216BD71DF2DADF86A627306ECFF96DBB8BACE198B61E00F8B332

04161FF7528B899B2D0C28607CA52C5B86CF5AC8395BAFFB13C02DA292DDFD7A83

DB7C2ABF62E35E668076BEAD208B

0401A57A6A7B26CA5EF52FCDB816479700B3ADC94ED1FE674C06E695BABA1D

12511cfe811d0f4e6bc688b4d

002757A1114D696E6768756151755316C05E0BD4

C302F41D932A36CDA7A3463093D18DB78FCF476DF1A86294

deca87e736574c5c83c07314051fd93a

10099790675505530477208181553592522486984108257205345787482351587557714799052927277724415285269929879648335669968284202797289605274717 31754805904856071347468521419286809125615028022221856475391909026561163678472701450190667942909301854462163997308722217328898303231940 97355403213400972588322876850946740663962

7BC86E2102902EC4D5890E8B6B4981ff27E0482750FEFC03

31a92ee2029fd10d901b113e990710f0d21ac6b6

| POSSIBLE SECRETS | | | |
|---|--|--|--|
| 027d29778100c65a1da1783716588dce2b8b4aee8e228f1896 | | | |
| 7BC382C63D8C150C3C72080ACE05AFA0C2BEA28E4FB22787139165EFBA91F90F8AA5814A503AD4EB04A8C7DD22CE2826 | | | |
| EE353FCA5428A9300D4ABA754A44C00FDFEC0C9AE4B1A1803075ED967B7BB73F | | | |
| 010090512DA9AF72B08349D98A5DD4C7B0532ECA51CE03E2D10F3B7AC579BD87E909AE40A6F131E9CFCE5BD967 | | | |
| B4050A850C04B3ABF54132565044B0B7D7BFD8BA270B39432355FFB4 | | | |
| 29C41E568B77C617EFE5902F11DB96FA9613CD8D03DB08DA | | | |
| DC9203E514A721875485A529D2C722FB187BC8980EB866644DE41C68E143064546E861C0E2C9EDD92ADE71F46FCF50FF2AD97F951FDA9F2A2EB6546F39689BD3 | | | |
| 0236B3DAF8A23206F9C4F299D7B21A9C369137F2C84AE1AA0D | | | |
| 127971af8721782ecffa3 | | | |
| 036b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296 | | | |
| 68A5E62CA9CE6C1C299803A6C1530B514E182AD8B0042A59CAD29F43 | | | |
| 04DB4FF10EC057E9AE26B07D0280B7F4341DA5D1B1EAE06C7D9B2F2F6D9C5628A7844163D015BE86344082AA88D95E2F9D | | | |
| 5037EA654196CFF0CD82B2C14A2FCF2E3FF8775285B545722F03EACDB74B | | | |
| 7B425ED097B425ED097B425ED097B425ED097B4260B5E9C7710C864 | | | |
| 11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650 | | | |

| POSSIBLE SECRETS | | |
|---|--|--|
| 65bd6c1d9b1ad3061601a51e | | |
| 13D56FFAEC78681E68F9DEB43B35BEC2FB68542E27897B79 | | |
| 51DEF1815DB5ED74FCC34C85D709 | | |
| b28ef557ba31dfcbdd21ac46e2a91e3c304f44cb87058ada2cb815151e610046 | | |
| 1f3bdba585295d9a1110d1df1f9430ef8442c5018976ff3437ef91b81dc0b8132c8d5c39c32d0e004a3092b7d327c0e7a4d26d2c7b69b58f9066652911e457779de | | |
| 5DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2 | | |
| B4C4EE28CEBC6C2C8AC12952CF37F16AC7EFB6A9F69F4B57FFDA2E4F0DE5ADE038CBC2FFF719D2C18DE0284B8BFEF3B52B8CC7A5F5BF0A3C8D2319A5312557E1 | | |
| 5FF6108462A2DC8210AB403925E638A19C1455D21 | | |
| 03375D4CE24FDE434489DE8746E71786015009E66E38A926DD | | |
| 0289FDFBE4ABE193DF9559ECF07AC0CE78554E2784EB8C1ED1A57A | | |
| 128-c20968b22ed168a498a4bf28ebadc7e883bd4b8c2dba719cb4c661a2c15147f5 | | |
| D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E27 | | |
| 7ae96a2b657c07106e64479eac3434e99cf0497512f58995c1396c28719501ee | | |
| 55066263022277343669578718895168534326250603453777594175500187360389116729240 | | |
| 003088250CA6E7C7FE649CE85820F7 | | |

| POSSIBLE SECRETS | | | |
|--|--|--|--|
| FFFFFFE0000000075A30D1B9038A115 | | | |
| 040D9029AD2C7E5CF4340823B2A87DC68C9E4CE3174C1E6EFDEE12C07D58AA56F772C0726F24C6B89E4ECDAC24354B9E99CAA3F6D3761402CD | | | |
| 9ba48cba5ebcb9b6bd33b92830b2a2e0e192f10a | | | |
| 5EEEFCA380D02919DC2C6558BB6D8A5D | | | |
| 04017232BA853A7E731AF129F22FF4149563A419C26BF50A4C9D6EEFAD612601DB537DECE819B7F70F555A67C427A8CD9BF18AEB9B56E0C11056FAE6A3 | | | |
| 04C0A0647EAAB6A48753B033C56CB0F0900A2F5C4853375FD614B690866ABD5BB88B5F4828C1490002E6773FA2FA299B8F | | | |
| E8C2505DEDFC86DDC1BD0B2B6667F1DA34B82574761CB0E879BD081CFD0B6265EE3CB090F30D27614CB4574010DA90DD862EF9D4EBEE4761503190785A71C760 | | | |
| 115792089237316195423570985008687907852837564279074904382605163141518161494337 | | | |
| 39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319 | | | |
| 10D9B4A3D9047D8B154359ABFB1B7F5485B04CEB868237DDC9DEDA982A679A5A919B626D4E50A8DD731B107A9962381FB5D807BF2618 | | | |
| 04015D4860D088DDB3496B0C6064756260441CDE4AF1771D4DB01FFE5B34E59703DC255A868A1180515603AEAB60794E54BB7996A70061B1CFAB6BE5F32BBFA783 24ED106A7636B9C5A7BD198D0158AA4F5488D08F38514F1FDF4B4F40D2181B3681C364BA0273C706 | | | |
| 5F49EB26781C0EC6B8909156D98ED435E45FD59918 | | | |
| C2173F1513981673AF4892C23035A27CE25E2013BF95AA33B22C656F277E7335 | | | |
| c49d360886e704936a6678e1139d26b7819f7e90 | | | |
| 71169be7330b3038edb025f1d0f9 | | | |

| POSSIBLE SECRETS | | | | |
|--|--|--|--|--|
| 10B51CC12849B234C75E6DD2028BF7FF5C1CE0D991A1 | | | | |
| 3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CADC083E67984050B75EBAE5DD2809BD638016F3 | | | | |
| fe0e87005b4e83761908c5131d552a850b3f58b749c37cf5b84d6768 | | | | |
| 8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B31F166E6CAC0425A7CF3AB6AF6B7FC3103B883202E9046565 | | | | |
| 7167EFC92BB2E3CE7C8AAAFF34E12A9C557003D7C73A6FAF003F99F6CC8482E540F7 | | | | |
| 8325710961489029985546751289520108179287853048861315594709205902480503199884419224438643760392947333078086511627871 | | | | |
| 023809B2B7CC1B28CC5A87926AAD83FD28789E81E2C9E3BF10 | | | | |
| 687D1B459DC841457E3E06CF6F5E2517B97C7D614AF138BCBF85DC806C4B289F3E965D2DB1416D217F8B276FAD1AB69C50F78BEE1FA3106EFB8CCBC7C5140116 | | | | |
| 1243ae1b4d71613bc9f780a03690e | | | | |
| 02197B07845E9BE2D96ADB0F5F3C7F2CFFBD7A3EB8B6FEC35C7FD67F26DDF6285A644F740A2614 | | | | |
| 8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC50 | | | | |
| 4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5 | | | | |
| 044BA30AB5E892B4E1649DD0928643ADCD46F5882E3747DEF36E956E97 | | | | |
| 04BED5AF16EA3F6A4F62938C4631EB5AF7BDBCDBC31667CB477A1A8EC338F94741669C976316DA6321 | | | | |
| 6EE3CEEB230811759F20518A0930F1A4315A827DAC | | | | |

| POSSIBLE SECRETS | | | |
|--|--|--|--|
| 9162fbe73984472a0a9d0590 | | | |
| 393C7F7D53666B5054B5E6C6D3DE94F4296C0C599E2E2E241050DF18B6090BDC90186904968BB | | | |
| 324A6EDDD512F08C49A99AE0D3F961197A76413E7BE81A400CA681E09639B5FE12E59A109F78BF4A373541B3B9A1 | | | |
| 02F40E7E2221F295DE297117B7F3D62F5C6A97FFCB8CEFF1CD6BA8CE4A9A18AD84FFABBD8EFA59332BE7AD6756A66E294AFD185A78FF12AA520E4DE739BACA00 FEFF7F2955727A | | | |
| 004D696E67687561517512D8F03431FCE63B88F4 | | | |
| f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b5 47c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a | | | |
| e8b4011604095303ca3b8099982be09fcb9ae616 | | | |
| B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF | | | |
| 033C258EF3047767E7EDE0F1FDAA79DAEE3841366A132E163ACED4ED2401DF9C6BDCDE98E8E707C07A2239B1B097 | | | |
| 0400C6858E06B70404E9CD9E3ECB662395B4429C648139053FB521F828AF606B4D3DBAA14B5E77EFE75928FE1DC127A2FFA8DE3348B3C1856A429BF97E7E31C2E5B D66011839296A789A3BC0045C8A5FB42C7D1BD998F54449579B446817AFBD17273E662C97EE72995EF42640C550B9013FAD0761353C7086A272C24088BE94769FD1 6650 | | | |
| 2E45EF571F00786F67B0081B9495A3D95462F5DE0AA185EC | | | |
| BDB6F4FE3E8B1D9E0DA8C0D40FC962195DFAE76F56564677 | | | |
| 046B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C2964FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5 | | | |
| 6127C24C05F38A0AAAF65C0EF02C | | | |

| POSSIBLE SECRETS | | |
|--|--|--|
| 0667ACEB38AF4E488C407433FFAE4F1C811638DF20 | | |
| 038D16C2866798B600F9F08BB4A8E860F3298CE04A5798 | | |
| 07B6882CAAEFA84F9554FF8428BD88E246D2782AE2 | | |
| BD71344799D5C7FCDC45B59FA3B9AB8F6A948BC5 | | |
| 6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296 | | |
| 4E13CA542744D696E67687561517552F279A8C84 | | |
| 16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a | | |
| C302F41D932A36CDA7A3462F9E9E916B5BE8F1029AC4ACC1 | | |
| 70B5E1E14031C1F70BBEFE96BDDE66F451754B4CA5F48DA241F331AA396B8D1839A855C1769B1EA14BA53308B5E2723724E090E02DB9 | | |
| 027B680AC8B8596DA5A4AF8A19A0303FCA97FD7645309FA2A581485AF6263E313B79A2F5 | | |
| 10C0FB15760860DEF1EEF4D696E676875615175D | | |
| 103FAEC74D696E676875615175777FC5B191EF30 | | |
| c97445f45cdef9f0d3e05e1e585fc297235b82b5be8ff3efca67c59852018192 | | |
| c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66 | | |
| 4B337D934104CD7BEF271BF60CED1ED20DA14C08B3BB64F18A60888D | | |

| POSSIBLE SECRETS | | | |
|--|--|--|--|
| 3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f | | | |
| 39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316 | | | |
| 1053CDE42C14D696E67687561517533BF3F83345 | | | |
| b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae466748d9b5a536 | | | |
| C49D360886E704936A6678E1139D26B7819F7E90 | | | |
| b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef | | | |
| D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FC | | | |
| D7C134AA264366862A18302575D0FB98D116BC4B6DDEBCA3A5A7939F | | | |
| e4437ed6010e88286f547fa90abfe4c42212 | | | |
| 02120FC05D3C67A99DE161D2F4092622FECA701BE4F50F4758714E8A87BBF2A658EF8C21E7C5EFE965361F6C2999C0C247B0DBD70CE6B7 | | | |
| 0108B39E77C4B108BED981ED0E890E117C511CF072 | | | |
| 0405F939258DB7DD90E1934F8C70B0DFEC2EED25B8557EAC9C80E2E198F8CDBECD86B1205303676854FE24141CB98FE6D4B20D02B4516FF702350EDDB0826779C8 13F0DF45BE8112F4 | | | |
| BDDB97E555A50A908E43B01C798EA5DAA6788F1EA2794EFCF57166B8C14039601E55827340BE | | | |
| 3071c8717539de5d5353f4c8cd59a032 | | | |
| 026108BABB2CEEBCF787058A056CBE0CFE622D7723A289E08A07AE13EF0D10D171DD8D | | | |

e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe 9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf

36134250956749795798585127919587881956611106672985015071877198253568414405109

0403F0EBA16286A2D57EA0991168D4994637E8343E3600D51FBC6C71A0094FA2CDD545B11C5C0C797324F1

E87579C11079F43DD824993C2CEE5ED3

dcb428fea25c40e7b99f81ae5981ee6a

36DF0AAFD8B8D7597CA10520D04B

 $12702124828893241746590704277717644352578765350891653581281750726570503126098509849742318833348340118092599999512098893413065920561499\\ 67242541210492743493570749203127695614516892241105793112488126102296785346384016935200132889950003622606842227508135323070045173416336\\ 85004541062586971416883686778842537820383$

 $13945487119911582560140965510769071310704170705992803179775800145437576535772298409412436852228823983303911468164807668823692122073732\\26721607407477717009111345504320538046476949046861201130878162407401848004770471573366629262494235712488239685422217536601433914856808\\40520336859458494803187341288580489525163$

00689918DBEC7E5A0DD6DFC0AA55C7

036768ae8e18bb92cfcf005c949aa2c6d94853d0e660bbf854b1c9505fe95a

f8183668ba5fc5bb06b5981e6d8b795d30b8978d43ca0ec572e37e09939a9773

8D91E471E0989CDA27DF505A453F2B7635294F2DDF23E3B122ACC99C9E9F1E14

6A941977BA9F6A435199ACFC51067FD587F519C5FCB541B8F44111DF1D40

A7F561E038EB1ED560B3D147DB782013064C19F27ED27C6780AAF77FB8A547CEB5B4FEF422340353

04925BE9FB01AFC6FB4D3E7D4990010F813408AB106C4F09CB7EE07868CC136FFF3357F624A21BED5263BA3A7A27483EBF6671DBEF7ABB30EBEE084E58A0B077AD4 2A5A0989D1EE71B1B9BC0455FB0D2C3

60dcd2104c4cbc0be6eeefc2bdd610739ec34e317f9b33046c9e4788

1C97BEFC54BD7A8B65ACF89F81D4D4ADC565FA45

2472E2D0197C49363F1FE7F5B6DB075D52B6947D135D8CA445805D39BC345626089687742B6329E70680231988

E95E4A5F737059DC60DFC7AD95B3D8139515620C

617fab6832576cbbfed50d99f0249c3fee58b94ba0038c7ae84c8c832f2c

0100FAF51354E0E39E4892DF6E319C72C8161603FA45AA7B998A167B8F1E629521

FFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1 356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA483 61C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C18 0E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1C BA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86 A64521F2B18177B200CBBF117577A615D6C770988C0BAD946F208F24FA074F5AB3143DB5BFCF0FD108F4B82D120A92108011A723C12A787F6D788719A10BDBA5B2 699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED 1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DE C9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B3 32051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A9 7A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CC B1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DBE115974A3926F12FEE5E438777CB6A932DF8CD8BEC4D07 3B931BA3BC832B68D9DD300741FA7BF8AFC47ED2576F6936BA424663AAB639C5AE4F5683423B4742BF1C978238F16CBE39D652DE3FDB8BEFC848AD922222E04A40 37C0713FB57A81A23F0C73473FC646CFA306B4BCBC8862F8385DDFA9D4B7FA2C087F879683303FD5BDD3A062B3CF5B3A278A66D2A13F83F44F82DDF310FF074AB6 A364597E899A0255DC164F31CC50846851DF9AB48195DED7EA1B1D510BD7EE74D73FAF36BC31ECFA268359046F4EB879F924009438B481C6CD7889A002ED5EE382

8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC53

4230017757A767FAE42398569B746325D45313AF0766266479B75654E65F

c39c6c3b3a36d7701b9c71a1f5804ae5d0003f4

040356DCD8F2F95031AD652D23951BB366A80648F06D867940A5366D9E265DE9EB240F



> PLAYSTORE INFORMATION

Title: Circle Medical - See a Doctor

Score: 4.5663366 Installs: 100,000+ Price: 0 Android Version Support: Category: Health & Fitness Play Store URL: co.circlemedical.patient

Developer Details: Circle Medical Technologies, Circle+Medical+Technologies, None, https://www.circlemedical.com/, hello@circlemedical.com/,

Release Date: Nov 3, 2015 Privacy Policy: Privacy link

Description:

Circle Medical is a primary care clinic that connects you with a board-certified provider for same-day or next-day appointments. More than 50,000 patients per month use Circle to establish an ongoing relationship with a trusted primary care provider for their general physical and mental health, preventive care, referrals, and treatment of chronic conditions, as well as urgent issues. Currently available for video appointments in 30 states and Washington D.C. Circle Medical accepts most PPO plans from major insurances. No membership fees. Self pay also accepted. In-person appointments are available at our clinics in CA and NY, with more locations coming soon. What we offer: • Full-service primary care • Annual physicals/wellness exams • ADHD / ADD assessments and treatment • Anxiety and depression treatment • Sleep assessments and at-home sleep studies • Gender-affirming hormone therapy • Chronic disease management • Sexual health consultations and screenings • Sickness or injury visits • Nutrition and Weight Management • Blood tests • Referrals • PrEP Disclaimer: All medical services are provided by an independent physician group.



| Timestamp | Event | Error |
|---------------------|---|-------|
| 2025-08-28 22:26:49 | Generating Hashes | ОК |
| 2025-08-28 22:26:49 | Extracting APK | ОК |
| 2025-08-28 22:26:49 | Unzipping | ОК |
| 2025-08-28 22:26:51 | Parsing APK with androguard | ОК |
| 2025-08-28 22:26:51 | Extracting APK features using aapt/aapt2 | ОК |
| 2025-08-28 22:26:52 | Getting Hardcoded Certificates/Keystores | OK |
| 2025-08-28 22:26:57 | Parsing AndroidManifest.xml | ОК |
| 2025-08-28 22:26:57 | Extracting Manifest Data | ОК |
| 2025-08-28 22:26:57 | Manifest Analysis Started | ОК |
| 2025-08-28 22:26:57 | Reading Network Security config from circle_medical_network_security_config.xml | ОК |

| 2025-08-28 22:26:57 | Parsing Network Security config | ОК |
|---------------------|--|----|
| 2025-08-28 22:26:57 | Performing Static Analysis on: Circle Medical (co.circlemedical.patient) | ОК |
| 2025-08-28 22:26:58 | Fetching Details from Play Store: co.circlemedical.patient | ОК |
| 2025-08-28 22:26:58 | Checking for Malware Permissions | ОК |
| 2025-08-28 22:26:58 | Fetching icon path | ОК |
| 2025-08-28 22:26:58 | Library Binary Analysis Started | ОК |
| 2025-08-28 22:26:58 | Reading Code Signing Certificate | ОК |
| 2025-08-28 22:27:00 | Running APKiD 2.1.5 | ОК |
| 2025-08-28 22:27:18 | Detecting Trackers | ОК |
| 2025-08-28 22:27:33 | Decompiling APK to Java with JADX | ОК |
| 2025-08-28 22:28:50 | Converting DEX to Smali | OK |

| 2025-08-28 22:28:50 | Code Analysis Started on - java_source | ОК |
|---------------------|---|----|
| 2025-08-28 22:29:11 | Android SBOM Analysis Completed | ОК |
| 2025-08-28 22:30:08 | Android SAST Completed | ОК |
| 2025-08-28 22:30:08 | Android API Analysis Started | ОК |
| 2025-08-28 22:31:25 | Android API Analysis Completed | ОК |
| 2025-08-28 22:31:25 | Android Permission Mapping Started | ОК |
| 2025-08-28 22:33:20 | Android Permission Mapping Completed | ОК |
| 2025-08-28 22:33:22 | Android Behaviour Analysis Started | ОК |
| 2025-08-28 22:34:31 | Android Behaviour Analysis Completed | ОК |
| 2025-08-28 22:34:31 | Extracting Emails and URLs from Source Code | ОК |
| 2025-08-28 22:35:11 | Email and URL Extraction Completed | ОК |

| 2025-08-28 22:35:11 | Extracting String data from APK | ОК |
|---------------------|--|----|
| 2025-08-28 22:35:11 | Extracting String data from Code | ОК |
| 2025-08-28 22:35:11 | Extracting String values and entropies from Code | ОК |
| 2025-08-28 22:35:31 | Performing Malware check on extracted domains | OK |
| 2025-08-28 22:35:41 | Saving to Database | ОК |

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.

© 2025 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.