# MOBSF

## ANDROID STATIC ANALYSIS REPORT



 Doctor On Demand (2024.51.3)

| | |
|---|---|
| File Name: | com.doctorondemand.android.patient_5406744.apk |
| Package Name: | com.doctorondemand.android.patient |
| Scan Date: | Aug. 29, 2025, 9:43 p.m. |
| App Security Score: | **46/100 (MEDIUM RISK)** |
| Grade: | B |
| Trackers Detection: | 5/432 |

# ⬤ FINDINGS SEVERITY

| 🐛 HIGH | ⚠ MEDIUM | ⓘ INFO | ✔ SECURE | 🔍 HOTSPOT |
|---------|----------|--------|----------|------------|
| 7 | 25 | 5 | 3 | 1 |

# 📦 FILE INFORMATION

**File Name:** com.doctorondemand.android.patient_5406744.apk
**Size:** 60.1MB
**MD5:** 063bbe58994597ef6caf71b2c871addc
**SHA1:** 2af92d88c59f52a9e869e41a9259bead3adec556
**SHA256:** 2a6a47097b36c1801ea0356a4abed0d18a05e5bb0dbb6ed52360c8430a4d0f2c

# ⓘ APP INFORMATION

**App Name:** Doctor On Demand
**Package Name:** com.doctorondemand.android.patient
**Main Activity:** com.grandroundshealth.grandrounds.presentation.splash.SplashActivity
**Target SDK:** 34
**Min SDK:** 24
**Max SDK:**
**Android Version Name:** 2024.51.3

**Android Version Code:** 5406744

# ▦ APP COMPONENTS

**Activities:** 133
**Services:** 22
**Receivers:** 16
**Providers:** 10
**Exported Activities:** 7
**Exported Services:** 1
**Exported Receivers:** 3
**Exported Providers:** 0

# ✾ CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=1, ST=CA, L=San Francisco, O=Doctor on Demand, OU=Android, CN=Adam Jackson
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-07-25 17:26:57+00:00
Valid To: 2513-03-26 17:26:57+00:00
Issuer: C=1, ST=CA, L=San Francisco, O=Doctor on Demand, OU=Android, CN=Adam Jackson
Serial Number: 0x51f15fe1
Hash Algorithm: sha1
md5: 3ed4381874db36d249556381e3779e00
sha1: c9dd830e31e07900df8a339c67be926391c49884
sha256: 084ca2861f5c1b3eed6b4c08b26e28a4fda4dd4b2e5c6ce98bfdeb005d721d04
sha512: cd729fb8bf56912dc9770232bd41a28576545bc8681dead06e4c8a16a88f9130646ac4713a67ab323c223867a6737cc1f2a2d48415b4ea7167da6fb978ac397e
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 38006d99e3f82923408b4126b87bed38d1ccaad389ca6fce64f88899eec4f653
Found 1 unique certificates

# ☰ APPLICATION PERMISSIONS

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|---|---|---|
| android.permission.INTERNET | normal | full Internet access | Allows an application to create network sockets. |
| android.permission.ACCESS_NETWORK_STATE | normal | view network status | Allows an application to view the status of all networks. |
| android.permission.USE_BIOMETRIC | normal | allows use of device-supported biometric modalities. | Allows an app to use device supported biometric modalities. |
| android.permission.WRITE_EXTERNAL_STORAGE | dangerous | read/modify/delete external storage contents | Allows an application to write to external storage. |
| 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. |

| 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.CAMERA | dangerous | take pictures and videos | Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time. |
| android.permission.RECORD_AUDIO | dangerous | record audio | Allows application to access the audio record path. |
| android.permission.WAKE_LOCK | normal | prevent phone from sleeping | Allows an application to prevent the phone from going to sleep. |
| android.permission.BLUETOOTH_CONNECT | dangerous | necessary for connecting to paired Bluetooth devices. | Required to be able to connect to paired Bluetooth devices. |
| android.permission.POST_NOTIFICATIONS | dangerous | allows an app to post notifications. | Allows an app to post notifications |
| android.permission.VIBRATE | normal | control vibrator | Allows the application to control the vibrator. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|---|---|---|
| android.permission.FOREGROUND_SERVICE | normal | enables regular apps to use Service.startForeground. | Allows a regular application to use Service.startForeground. |
| android.permission.FOREGROUND_SERVICE_REMOTE_MESSAGING | normal | allows foreground services for remote messaging. | Allows a regular application to use Service.startForeground with the type "remoteMessaging". |
| android.permission.READ_EXTERNAL_STORAGE | dangerous | read external storage contents | Allows an application to read from external storage. |
| android.permission.MODIFY_AUDIO_SETTINGS | normal | change your audio settings | Allows application to modify global audio settings, such as volume and routing. |
| 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.DETECT_SCREEN_CAPTURE | normal | notifies when a screen capture of the app's windows is attempted. | Allows an application to get notified when a screen capture of its windows is attempted. |
| android.permission.USE_FINGERPRINT | normal | allow use of fingerprint | This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|---|---|---|
| android.permission.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_SCAN | dangerous | required for discovering and pairing Bluetooth devices. | Required to be able to discover and pair nearby Bluetooth devices. |
| android.permission.BROADCAST_STICKY | normal | send sticky broadcast | Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|---|---|---|
| android.permission.SYSTEM_ALERT_WINDOW | dangerous | display system-level alerts | Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone. |
| android.permission.FOREGROUND_SERVICE_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". |
| android.permission.FOREGROUND_SERVICE_MEDIA_PROJECTION | normal | allows foreground services for media projection. | Allows a regular application to use Service.startForeground with the type "mediaProjection". |

| 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.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. |
| com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE | normal | permission defined by google | A custom permission defined by Google. |
| com.doctorondemand.android.patient.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION | unknown | Unknown permission | Unknown permission from android reference |
| 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. |

# 🔍 APKID ANALYSIS

| FILE | DETAILS |
|------|---------|
| 063bbe58994597ef6caf71b2c871addc.apk | <table><tr><td>**FINDINGS**</td><td>**DETAILS**</td></tr><tr><td>Anti-VM Code</td><td>emulator file check</td></tr></table> |
| classes.dex | <table><tr><td>**FINDINGS**</td><td>**DETAILS**</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check<br>Build.MODEL check<br>Build.MANUFACTURER check<br>Build.PRODUCT check<br>device ID check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table> |

| FILE | DETAILS |
|---|---|
| classes2.dex | |

| FINDINGS | DETAILS |
|---|---|
| Anti-VM Code | Build.FINGERPRINT check<br>Build.MODEL check<br>Build.MANUFACTURER check<br>Build.PRODUCT check<br>Build.HARDWARE check<br>Build.BOARD check<br>possible Build.SERIAL check<br>Build.TAGS check<br>network operator name check<br>subscriber ID check<br>emulator file check |
| Anti Debug Code | Debug.isDebuggerConnected() check |
| Compiler | r8 without marker (suspicious) |

| FILE | DETAILS |
|------|---------|
| classes3.dex | **FINDINGS** / **DETAILS**<br><br>Anti-VM Code: Build.FINGERPRINT check, Build.MANUFACTURER check, SIM operator check<br><br>Compiler: r8 without marker (suspicious) |
| classes4.dex | **FINDINGS** / **DETAILS**<br><br>Anti-VM Code: Build.MODEL check, Build.MANUFACTURER check, Build.TAGS check, possible ro.secure check<br><br>Compiler: r8 without marker (suspicious) |

| FILE | DETAILS |
|------|---------|

**classes5.dex**

| FINDINGS | DETAILS |
|----------|---------|
| Anti-VM Code | Build.FINGERPRINT check<br>Build.MODEL check<br>Build.MANUFACTURER check<br>Build.PRODUCT check<br>Build.HARDWARE check<br>Build.BOARD check<br>Build.TAGS check<br>SIM operator check<br>network operator name check |
| Anti Debug Code | Debug.isDebuggerConnected() check |
| Compiler | r8 without marker (suspicious) |

**classes6.dex**

| FINDINGS | DETAILS |
|----------|---------|
| Compiler | r8 without marker (suspicious) |

# BROWSABLE ACTIVITIES

| ACTIVITY | INTENT |
|---|---|
| com.grandroundshealth.grandrounds.presentation.splash.SplashActivity | Schemes: doctorondemand://, http://, https://,<br>Hosts: doctorondemand.includedhealth.com, doctorondemand.uat.includedhealth.com, |
| com.auth0.android.provider.RedirectActivity | Schemes: @string/auth0_scheme://,<br>Hosts: @string/com_auth0_domain, @string/com_auth0_domain_uat,<br>@string/com_auth0_domain_prod, @string/included_health_com_auth0_domain_uat,<br>@string/included_health_com_auth0_domain_prod,<br>Path Prefixes: /android/com.doctorondemand.android.patient/callback, |
| com.braintreepayments.api.DropInActivity | Schemes: com.doctorondemand.android.patient.braintree://, |
| com.braintreepayments.api.BraintreeDeepLinkActivity | Schemes: com.doctorondemand.android.patient.braintree.deeplinkhandler://, |

# 🔒 NETWORK SECURITY

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

| NO | SCOPE | SEVERITY | DESCRIPTION |
|---|---|---|---|

# 📇 CERTIFICATE ANALYSIS

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

| TITLE | SEVERITY | DESCRIPTION |
|---|---|---|
| Signed Application | info | Application is signed with a code signing certificate |
| Certificate algorithm vulnerable to hash collision | high | Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. |

# 🔍 MANIFEST ANALYSIS

HIGH: **2** | WARNING: **13** | INFO: **0** | SUPPRESSED: **0**

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 1 | App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24] | high | This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates. |
| 2 | Clear text traffic is Enabled For App [android:usesCleartextTraffic=true] | high | The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected. |
| 3 | App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config] | info | The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app. |
| 4 | Activity (com.auth0.android.provider.RedirectActivity) 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. |
| 5 | Activity (com.braintreepayments.api.DropInActivity) 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 |
|---|---|---|---|
| 6 | TaskAffinity is set for activity (com.salesforce.marketingcloud.notifications.NotificationOpenActivity) | 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. |
| 7 | Activity (androidx.biometric.DeviceCredentialHandlerActivity) is not Protected. [android:exported=true] | warning | An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. |
| 8 | Activity (com.braintreepayments.api.BraintreeDeepLinkActivity) is not Protected. [android:exported=true] | warning | An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. |
| 9 | Service (androidx.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 |
|---|---|---|---|
| 10 | Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: android.permission.DUMP<br>[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. |
| 11 | Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: com.google.android.c2dm.permission.SEND<br>[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. |
| 12 | Activity (androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity) is not Protected.<br>[android:exported=true] | warning | An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. |
| 13 | Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity) is not Protected.<br>[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 |
|---|---|---|---|
| 14 | Activity (androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity) 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. |
| 15 | 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. |
| 16 | High Intent Priority (101) - {2} Hit(s) [android:priority] | warning | By setting an intent priority higher than another intent, the app effectively overrides other requests. |

# </> CODE ANALYSIS

HIGH: **3** | WARNING: **11** | INFO: **4** | SECURE: **2** | SUPPRESSED: **0**

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 1 | This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel. | secure | OWASP MASVS: MSTG-NETWORK-4 | com/braintreepayments/api/d3.java<br>d00/g.java<br>e80/e.java<br>e80/h.java<br>e80/m.java<br>e80/n.java<br>m30/e.java<br>m30/h.java<br>m30/m.java<br>m30/n.java<br>org/conscrypt/DefaultSSLContextImpl.java<br>org/conscrypt/SSLParametersImpl.java<br>r70/i.java<br>us/zoom/video_sdk/v0.java<br>v30/b.java |
|  |  |  |  | a0/d.java<br>a3/a.java<br>a3/d.java<br>af/b.java<br>av/c.java<br>ax/d.java<br>ay/b.java<br>b1/b0.java<br>b1/i.java<br>b1/n.java<br>b9/f.java<br>bo/c.java<br>c3/e.java<br>c3/g.java<br>com/auth0/android/provider/AuthenticationActivity.java<br>com/auth0/android/request/internal/JwksDeserializer.java<br>com/auth0/android/request/internal/a.java<br>com/braintreepayments/api/BraintreeDeepLinkActivity.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| | | | | com/braintreepayments/api/m1.java |
| | | | | com/braintreepayments/api/p0.java |
| | | | | com/braintreepayments/api/v1.java |
| | | | | com/bumptech/glide/GeneratedAppGlideModuleImpl.java |
| | | | | com/bumptech/glide/Glide.java |
| | | | | com/bumptech/glide/disklrucache/DiskLruCache.java |
| | | | | com/bumptech/glide/gifdecoder/GifHeaderParser.java |
| | | | | com/bumptech/glide/gifdecoder/StandardGifDecoder.java |
| | | | | com/bumptech/glide/load/data/AssetPathFetcher.java |
| | | | | com/bumptech/glide/load/data/HttpUrlFetcher.java |
| | | | | com/bumptech/glide/load/data/LocalUriFetcher.java |
| | | | | com/bumptech/glide/load/data/mediastore/ThumbFetcher.java |
| | | | | com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java |
| | | | | com/bumptech/glide/load/engine/DecodeJob.java |
| | | | | com/bumptech/glide/load/engine/DecodePath.java |
| | | | | com/bumptech/glide/load/engine/Engine.java |
| | | | | com/bumptech/glide/load/engine/GlideException.java |
| | | | | com/bumptech/glide/load/engine/SourceGenerator.java |
| | | | | com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java |
| | | | | com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java |
| | | | | com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java |
| | | | | com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java |
| | | | | com/bumptech/glide/load/engine/executor/GlideExecutor.java |
| | | | | com/bumptech/glide/load/engine/executor/RuntimeCompat.java |
| | | | | com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java |
| | | | | com/bumptech/glide/load/model/ByteBufferEncoder.java |
| | | | | com/bumptech/glide/load/model/ByteBufferFileLoader |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|-------|----------|-----------|-------|
| | | | | .java<br>com/bumptech/glide/load/model/FileLoader.java<br>com/bumptech/glide/load/model/ResourceLoader.java<br>com/bumptech/glide/load/model/ResourceUriLoader.java<br>com/bumptech/glide/load/model/StreamEncoder.java<br>com/bumptech/glide/load/resource/DefaultOnHeaderDecodedListener.java<br>com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java<br>com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java<br>com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java<br>com/bumptech/glide/load/resource/bitmap/Downsampler.java<br>com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java<br>com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java<br>com/bumptech/glide/load/resource/bitmap/TransformationUtils.java<br>com/bumptech/glide/load/resource/bitmap/VideoDecoder.java<br>com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java<br>com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java<br>com/bumptech/glide/load/resource/gif/StreamGifDecoder.java<br>com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java<br>com/bumptech/glide/manager/RequestTracker.java<br>com/bumptech/glide/manager/SingletonConnectivityReceiver.java<br>com/bumptech/glide/module/ManifestParser.java<br>com/bumptech/glide/request/SingleRequest.java<br>com/bumptech/glide/request/target/CustomViewTarget.java<br>com/bumptech/glide/request/target/ViewTarget.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|-------|----------|-----------|-------|
|    |       |          |           | com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/caverock/androidsvg/SVGImageView.java com/faltenreich/skeletonlayout/SkeletonLayout.java com/fasterxml/jackson/databind/ext/DOMSerializer.java com/fasterxml/jackson/databind/util/ClassUtil.java com/grandroundshealth/grandrounds/data/remote/RemoteRepoImpl.java com/grandroundshealth/grandrounds/di/modules/Auth0Module.java com/grandroundshealth/grandrounds/helpers/Stemmer.java com/grandroundshealth/grandrounds/initializers/AmplitudeInitializer.java com/grandroundshealth/grandrounds/presentation/universalLogin/UniversalWebAuthViewModel.java com/salesforce/marketingcloud/MCLogListener.java com/salesforce/marketingcloud/g.java com/salesforce/marketingcloud/legacycrypto/OldSdkHash.java com/salesforce/marketingcloud/sfmcsdk/components/encryption/EncryptedSharedPreferences.java com/salesforce/marketingcloud/sfmcsdk/components/encryption/Encryptor.java com/salesforce/marketingcloud/sfmcsdk/components/encryption/KeyStoreWrapper.java com/salesforce/marketingcloud/sfmcsdk/components/encryption/SalesforceKeyGenerator.java com/salesforce/marketingcloud/sfmcsdk/components/logging/LogListener.java com/salesforce/marketingcloud/sfmcsdk/components/logging/Logger.java com/salesforce/marketingcloud/tozny/AesCbcWithIntegrity$PrngFixes$LinuxPRNGSecureRandom.java com/sendbird/android/push/SendbirdFirebaseMessagingService.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| | | | | com/zipow/cmmlib/AppContext.java com/zipow/cmmlib/AppUtil.java com/zipow/cmmlib/CmmTimer.java |
| 2 | [The App logs information. Sensitive information should never be logged.](#) | info | CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3 | com/zipow/nydus/DeviceFilter.java com/zipow/nydus/NydusUtil.java com/zipow/nydus/UVCDevice.java com/zipow/nydus/VideoCapDevicesNotifier.java com/zipow/nydus/VideoCapturer.java com/zipow/nydus/camera/AbsCameraCapture.java com/zipow/nydus/camera/CameraCaptureImplV1.java com/zipow/nydus/camera/CameraCaptureImplV2.java com/zipow/nydus/camera/CameraHandleZoomV1.java com/zipow/nydus/camera/CameraHandleZoomV2.java com/zipow/nydus/camera/CameraMgrV1.java com/zipow/nydus/camera/CameraMgrV2.java com/zipow/nydus/camera/CameraV1ListEntity.java com/zipow/nydus/camera/CameraV2ListEntity.java com/zipow/nydus/camera/ZMCameraMgr.java com/zipow/videobox/ptapp/SystemInfoHelper.java com/zipow/videobox/view/video/VideoRenderer.java e80/n.java f2/c1.java f2/h0.java f2/i0.java f2/m.java f30/b.java f80/c.java g40/a.java h3/d.java h3/g.java h90/a.java hm/a.java hp/b.java i10/g.java il/a.java ir/c.java is/e.java j0/e.java m30/n.java mg/a.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|-------|----------|-----------|-------|
| | | | | mj/a.java |
| | | | | thb.java |
| | | | | net/sqlcipher/AbstractCursor.java |
| | | | | net/sqlcipher/BulkCursorToCursorAdaptor.java |
| | | | | net/sqlcipher/DatabaseUtils.java |
| | | | | net/sqlcipher/DefaultDatabaseErrorHandler.java |
| | | | | net/sqlcipher/database/SQLiteCompiledSql.java |
| | | | | net/sqlcipher/database/SQLiteContentHelper.java |
| | | | | net/sqlcipher/database/SQLiteDatabase.java |
| | | | | net/sqlcipher/database/SQLiteDebug.java |
| | | | | net/sqlcipher/database/SQLiteOpenHelper.java |
| | | | | net/sqlcipher/database/SQLiteProgram.java |
| | | | | net/sqlcipher/database/SQLiteQuery.java |
| | | | | net/sqlcipher/database/SQLiteQueryBuilder.java |
| | | | | net/sqlcipher/database/SqliteWrapper.java |
| | | | | o70/a.java |
| | | | | org/beyka/tiffbitmapfactory/TiffBitmapFactory.java |
| | | | | org/conscrypt/Platform.java |
| | | | | org/conscrypt/ct/CTVerifier.java |
| | | | | org/webrtc/voiceengine/AudioDeviceAndroid.java |
| | | | | org/webrtc/voiceengine/AudioDeviceAndroidAAudio.java |
| | | | | org/webrtc/voiceengine/AudioDeviceAndroidOpenSLESHelper.java |
| | | | | org/webrtc/voiceengine/AudioPlaybackCaptureAndroid.java |
| | | | | org/webrtc/voiceengine/VoiceEngineCompat.java |
| | | | | p00/l.java |
| | | | | p000do/c.java |
| | | | | p5/b.java |
| | | | | p70/a.java |
| | | | | pw/b.java |
| | | | | pw/c.java |
| | | | | q0/a.java |
| | | | | q70/d.java |
| | | | | qw/a.java |
| | | | | r0/a.java |
| | | | | r1/f.java |
| | | | | r1/q.java |
| | | | | r70/d.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|-------|----------|-----------|-------|
| | | | | ry/d.java |
| | | | | s1/f.java |
| | | | | s2/c2.java |
| | | | | s2/m2.java |
| | | | | s2/o.java |
| | | | | s2/t1.java |
| | | | | s2/y1.java |
| | | | | s2/z1.java |
| | | | | sn/a.java |
| | | | | t3/c.java |
| | | | | tj/b.java |
| | | | | tx/e.java |
| | | | | u1/c.java |
| | | | | u2/b.java |
| | | | | u3/b.java |
| | | | | u5/b.java |
| | | | | us/zoom/androidlib/util/HeadsetUtil.java |
| | | | | us/zoom/internal/SDKApplication.java |
| | | | | us/zoom/internal/UtilWrapper.java |
| | | | | us/zoom/internal/ZoomVideoSDKDelegateHelper.java |
| | | | | us/zoom/internal/ZoomVideoSDKRawDataPipeProxy.java |
| | | | | us/zoom/internal/ZoomVideoSDKShareHelperImpl.java |
| | | | | us/zoom/internal/ZoomVideoSDKTestAudioDeviceHelperImpl.java |
| | | | | us/zoom/internal/ZoomVideoSDKVideoHelperImpl.java |
| | | | | us/zoom/internal/audio/AudioSessionMgr.java |
| | | | | us/zoom/internal/share/ScreenShareServer.java |
| | | | | us/zoom/internal/share/ShareServer.java |
| | | | | us/zoom/internal/share/ShareSessionMgr.java |
| | | | | us/zoom/internal/uvc/USBMonitor.java |
| | | | | us/zoom/internal/video/SDKShareUnit.java |
| | | | | us/zoom/internal/video/SDKVideoRender.java |
| | | | | us/zoom/internal/video/SDKVideoSurfaceView.java |
| | | | | us/zoom/internal/video/SDKVideoTextureView.java |
| | | | | us/zoom/internal/video/SDKVideoUnit.java |
| | | | | us/zoom/internal/video/SDKVideoUnitMgr.java |
| | | | | us/zoom/internal/video/VideoSessionMgr.java |
| | | | | us/zoom/libtools/lifecycle/ZmMutableLiveData.java |
| | | | | us/zoom/libtools/lifecycle/viewmodel/ZmBaseViewMod |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| | | | | el.java<br>us/zoom/libtools/lifecycle/viewmodel/a.java<br>us/zoom/libtools/screenshot/ScreenShotInst.java<br>us/zoom/libtools/screenshot/a.java<br>us/zoom/libtools/storage/ZMEncryptedSharedPreferences.java<br>us/zoom/libtools/storage/ZmSharePreferenceHelper.java<br>us/zoom/libtools/utils/ZmAppUtils.java<br>us/zoom/libtools/utils/ZmCollectionsUtils.java<br>us/zoom/libtools/utils/ZmDeviceUtils.java<br>us/zoom/libtools/utils/ZmExceptionDumpUtils.java<br>us/zoom/libtools/utils/ZmMimeTypeUtils.java<br>us/zoom/libtools/utils/ZmStringUtils.java<br>us/zoom/libtools/utils/ZmUIUtils.java<br>us/zoom/net/AndroidNetworkLibrary.java<br>us/zoom/net/ZmX509Helper.java<br>us/zoom/net/dns/AndroidDnsQuery.java<br>us/zoom/net/dns/DnsResponse.java<br>us/zoom/net/dns/DnsUdpResolver.java<br>us/zoom/reflection/helper/MachInfoHelper.java<br>us/zoom/reflection/utils/AppUtilsReflection.java<br>us/zoom/reflection/utils/AssistantAppHelperReflection.java<br>us/zoom/reflection/utils/CommonReflection.java<br>us/zoom/reflection/utils/DeviceReflection.java<br>us/zoom/reflection/utils/MachInfoHelperReflection.java<br>us/zoom/reflection/utils/NetworkReflection.java<br>us/zoom/reflection/utils/PreferenceReflection.java<br>us/zoom/reflection/utils/PropertiesReflection.java<br>us/zoom/reflection/utils/SystemApiReflection.java<br>us/zoom/video_sdk/a.java<br>us/zoom/video_sdk/a2.java<br>us/zoom/video_sdk/b2.java<br>us/zoom/video_sdk/c2.java<br>us/zoom/video_sdk/e1.java<br>us/zoom/video_sdk/e2.java<br>us/zoom/video_sdk/f1.java<br>us/zoom/video_sdk/g1.java<br>us/zoom/video_sdk/h0.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|-------|----------|-----------|-------|
| | | | | us/zoom/video_sdk/h1.java us/zoom/video_sdk/i1.java us/zoom/video_sdk/j0.java |
| | | | | us/zoom/video_sdk/j1.java us/zoom/video_sdk/k.java us/zoom/video_sdk/m.java us/zoom/video_sdk/m0.java us/zoom/video_sdk/n.java us/zoom/video_sdk/n1.java us/zoom/video_sdk/o.java us/zoom/video_sdk/o0.java us/zoom/video_sdk/q0.java us/zoom/video_sdk/q1.java us/zoom/video_sdk/r1.java us/zoom/video_sdk/s1.java us/zoom/video_sdk/t1.java us/zoom/video_sdk/u1.java us/zoom/video_sdk/v0.java us/zoom/video_sdk/x1.java us/zoom/video_sdk/y0.java us/zoom/video_sdk/y1.java v1/c.java v1/f.java v3/c.java x1/i.java |
| | | | | x1/v.java y1/b.java z20/a.java z3/n.java z7/g.java zo/n.java com/amplitude/android/sessionreplay/config/RemoteC onfigServer.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.ja va com/grandroundshealth/core/network/interceptors/Gr aphqlInterceptor.java com/grandroundshealth/core/network/type/Complete HubTaskTuple.java com/grandroundshealth/core/network/type/CostShare |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|-------|----------|-----------|-------|
| | | | | TagDataInput.java com/grandroundshealth/core/network/type/CreateAccountInput.java |
| | | | | com/grandroundshealth/core/network/type/CreateMemberUserRecordInput.java |
| | | | | com/grandroundshealth/core/network/type/CreateOrUpdateMockMemberInput.java |
| | | | | com/grandroundshealth/core/network/type/DeleteConversationMetadataKeyInput.java |
| | | | | com/grandroundshealth/core/network/type/EmailAttribute.java |
| | | | | com/grandroundshealth/core/network/type/FeatureFlag.java |
| | | | | com/grandroundshealth/core/network/type/ListGroupChannelsByMetadataInput.java |
| | | | | com/grandroundshealth/core/network/type/NotificationAttribute.java |
| | | | | com/grandroundshealth/core/network/type/RawPIIFieldInput.java |
| | | | | com/grandroundshealth/core/network/type/SettingInput.java |
| | | | | com/grandroundshealth/core/network/type/TriggerNotificationJourneyRequest.java |
| | | | | com/grandroundshealth/core/network/type/UpdateUserCaseDashboardSettingInput.java |
| | | | | com/grandroundshealth/core/network/type/UpdateUserMessageDismissedSettingInput.java |
| | | | | com/grandroundshealth/grandrounds/BuildConfig.java |
| | | | | com/grandroundshealth/grandrounds/CareDeliveryReleaseAppointmentMutation.java |
| | | | | com/grandroundshealth/grandrounds/CreateClinicalVisitMutation.java |
| | | | | com/grandroundshealth/grandrounds/CreateHoldMutation.java |
| | | | | com/grandroundshealth/grandrounds/InsurancePlanInfoQuery.java |
| | | | | com/grandroundshealth/grandrounds/InsurancePlanInfoV2Query.java |
| | | | | com/grandroundshealth/grandrounds/MemberCasesListQuery.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 3 | [Files may contain hardcoded sensitive information like usernames, passwords, keys etc.](#) | warning | CWE: CWE-312: Cleartext Storage of Sensitive Information<br>OWASP Top 10: M9: Reverse Engineering<br>OWASP MASVS: MSTG-STORAGE-14 | com/grandroundshealth/grandrounds/ProvisionLinkedAccountEmployerMutation.java<br>com/grandroundshealth/grandrounds/PusherInfoQuery.java<br>com/grandroundshealth/grandrounds/UpdateUserSettingMutation.java<br>com/grandroundshealth/grandrounds/UserSettingFetchQuery.java<br>com/grandroundshealth/grandrounds/care/domain/model/ClinicalVisit.java<br>com/grandroundshealth/grandrounds/chat/data/models/ChatFeatureTag.java<br>com/grandroundshealth/grandrounds/chat/presentation/ChatUiData.java<br>com/grandroundshealth/grandrounds/data/model/CoverageCategory.java<br>com/grandroundshealth/grandrounds/data/model/claims/RouteParam.java<br>com/grandroundshealth/grandrounds/data/model/unifiedEligibility/EmployerVerificationField.java<br>com/grandroundshealth/grandrounds/data/sp/SPHelper.java<br>com/grandroundshealth/grandrounds/fragment/ClaimsAction.java<br>com/grandroundshealth/grandrounds/helpers/Constants.java<br>com/grandroundshealth/grandrounds/helpers/DeeplinkHelper.java<br>com/grandroundshealth/grandrounds/insurance/domain/model/CoverageCategory.java<br>com/grandroundshealth/grandrounds/insurance/domain/model/InsuranceCardInfo.java<br>com/grandroundshealth/grandrounds/presentation/claimsSupport/screens/caseLanding/ClaimsSupportDocuSignBottomSheetFragment.java<br>com/grandroundshealth/grandrounds/presentation/claimsSupport/screens/uploadDocuments/ClaimsSupportDeleteDocumentBottomSheetFragment.java<br>com/grandroundshealth/grandrounds/presentation/document/upload/UploadDocumentSourceSelector.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| | | | | com/grandroundshealth/grandrounds/presentation/findcareRecommendation/FindCareRecommendationVM.java |
| | | | | com/grandroundshealth/grandrounds/presentation/findcare/adapters/SearchFiltersAdapter.java |
| | | | | com/grandroundshealth/grandrounds/presentation/findcare/results/FindCareResultsViewModel.java |
| | | | | com/grandroundshealth/grandrounds/presentation/findcare/results/InsuranceStatusDialogFragment.java |
| | | | | com/grandroundshealth/grandrounds/presentation/healthProfile/ReviewProfileFragment.java |
| | | | | com/grandroundshealth/grandrounds/presentation/insurance/InsuranceCardActivity.java |
| | | | | com/grandroundshealth/grandrounds/presentation/signup/accountmerge/AccountMergingActivity.java |
| | | | | com/grandroundshealth/grandrounds/presentation/telemedicine/intake/IntakeConfirmationActivity.java |
| | | | | com/grandroundshealth/grandrounds/presentation/telemedicine/twilio/PusherInformation.java |
| | | | | com/grandroundshealth/grandrounds/presentation/unifiedIntake/selectPatient/dependents/DependentPatientBottomSheetFragment.java |
| | | | | com/grandroundshealth/grandrounds/presentation/virtualcare/location/LocationConfirmationBottomSheetFragment.java |
| | | | | com/grandroundshealth/grandrounds/views/ContinueToWebBottomSheetFragment.java |
| | | | | com/launchdarkly/sdk/LDContext.java |
| | | | | com/salesforce/marketingcloud/events/g.java |
| | | | | com/salesforce/marketingcloud/events/h.java |
| | | | | com/sendbird/android/internal/stats/NotificationStat.java |
| | | | | eg/a0.java |
| | | | | o20/g0.java |
| | | | | o20/m.java |
| | | | | o20/t.java |
| | | | | org/conscrypt/OpenSSLECKeyFactory.java |
| | | | | org/conscrypt/OpenSSLRSAKeyFactory.java |
| | | | | r00/m0.java |
| | | | | us/zoom/libtools/storage/PreferenceUtil.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| | | | | us/zoom/libtools/storage/ZmSharePreferenceHelper.ja va |
| | | | | a20/d0.java |
| | | | | us/zoom/libtools/utils/ZmDeviceUtils.java |
| | | | | arrow/core/c.java |
| | | | | 2070.java |
| | | | | av/c.java |
| | | | | com/salesforce/marketingcloud/storage/db/a.java |
| | | | | com/salesforce/marketingcloud/storage/db/b.java |
| | | | | com/salesforce/marketingcloud/storage/db/c.java |
| | | | | com/salesforce/marketingcloud/storage/db/e.java |
| | | | | com/salesforce/marketingcloud/storage/db/f.java |
| | | | | com/salesforce/marketingcloud/storage/db/g.java |
| | | | | com/salesforce/marketingcloud/storage/db/h.java |
| | | | | com/salesforce/marketingcloud/storage/db/i.java |
| | | | | com/salesforce/marketingcloud/storage/db/j.java |
| | | | | com/salesforce/marketingcloud/storage/db/k.java |
| | | | | com/salesforce/marketingcloud/storage/db/l.java |
| | | | | com/salesforce/marketingcloud/storage/db/m.java |
| | | | | com/salesforce/marketingcloud/storage/db/upgrades/a .java |
| | | | | com/salesforce/marketingcloud/storage/db/upgrades/b .java |
| | | | | com/salesforce/marketingcloud/storage/db/upgrades/c .java |
| | | | | com/salesforce/marketingcloud/storage/db/upgrades/d .java |
| | | | | com/salesforce/marketingcloud/storage/db/upgrades/e .java |
| 4 | App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database. | warning | CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality | com/salesforce/marketingcloud/storage/db/upgrades/f. java com/salesforce/marketingcloud/storage/db/upgrades/g .java com/salesforce/marketingcloud/storage/db/upgrades/h .java com/salesforce/marketingcloud/storage/db/upgrades/i. java com/salesforce/marketingcloud/storage/db/upgrades/j. java com/salesforce/marketingcloud/storage/db/upgrades/k .java e80/d.java e80/l.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| | | | | ev/b.java<br>ev/f.java<br>ev/m.java |
| | | | | ev/p.java<br>ev/q.java<br>f2/g0.java<br>f2/v.java<br>go/a.java<br>k10/m.java<br>kr/a.java<br>n70/p.java<br>net/sqlcipher/database/SQLiteDatabase.java<br>oq/a.java<br>q3/d.java<br>tx/a.java<br>uk/f.java<br>z00/s.java<br>zu/g.java |
| 5 | SHA-1 is a weak hash known to have hash collisions. | warning | CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | com/salesforce/marketingcloud/sfmcsdk/components/encryption/Encryptor.java<br>com/salesforce/marketingcloud/sfmcsdk/components/encryption/SalesforceKeyGenerator.java<br>qw/a.java<br>u3/b.java |
| 6 | Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole. | warning | CWE: CWE-749: Exposed Dangerous Method or Function<br>OWASP Top 10: M1: Improper Platform Usage<br>OWASP MASVS: MSTG-PLATFORM-7 | com/grandroundshealth/grandrounds/views/CustomWebView.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 7 | App can read/write to External Storage. Any App can read data written to External Storage. | warning | CWE: CWE-276: Incorrect Default Permissions<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | com/grandroundshealth/grandrounds/chat/presentation/dialogs/l.java<br>com/grandroundshealth/grandrounds/chat/presentation/dialogs/n.java<br>com/grandroundshealth/grandrounds/chat/presentation/dialogs/r.java<br>com/grandroundshealth/grandrounds/chat/presentation/y.java<br>com/grandroundshealth/grandrounds/helpers/CameraHelper.java<br>com/grandroundshealth/grandrounds/helpers/r3.java<br>m30/l.java<br>n70/k.java<br>n70/l.java<br>n70/n.java<br>us/zoom/libtools/utils/ZmAppUtils.java<br>us/zoom/libtools/utils/ZmDeviceUtils.java<br>us/zoom/libtools/utils/ZmUIUtils.java<br>us/zoom/video_sdk/r1.java<br>us/zoom/video_sdk/s1.java<br>yu/a.java<br>yu/b.java<br>zu/c.java |
| 8 | 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/grandroundshealth/grandrounds/chat/presentation/p2.java<br>com/grandroundshealth/grandrounds/presentation/developerMenu/b1.java<br>com/grandroundshealth/grandrounds/presentation/developerMenu/e1.java<br>com/grandroundshealth/grandrounds/presentation/insurance/InsuranceCardActivity.java<br>com/grandroundshealth/grandrounds/presentation/onboardingNWelcome/OnboardingActivity.java<br>us/zoom/libtools/utils/ZmMimeTypeUtils.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 9 | MD5 is a weak hash known to have hash collisions. | warning | CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-4 | com/salesforce/marketingcloud/legacycrypto/OldSdkHash.java<br>j1/f.java<br>uk/f.java<br>us/zoom/video_sdk/r1.java<br>us/zoom/video_sdk/v0.java<br>vy/b.java<br>x/e.java |
| 10 | The file or SharedPreference is World Readable. Any App can read from the file | high | CWE: CWE-276: Incorrect Default Permissions<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | us/zoom/video_sdk/d1.java<br>us/zoom/video_sdk/k.java |
| 11 | The App uses an insecure Random Number Generator. | warning | CWE: CWE-330: Use of Insufficiently Random Values<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-6 | a0/m.java<br>ai/e.java<br>b2/a.java<br>com/grandroundshealth/core/network/data/rpc/RpcRequest.java<br>com/grandroundshealth/grandrounds/helpers/notifications/SalesforceCloudMessagingHelper.java<br>d30/t.java<br>gx/c.java<br>hw/b.java<br>j80/f.java<br>j80/j.java<br>kr/a.java<br>m60/a.java<br>m60/b.java<br>n60/a.java<br>r30/e.java<br>x0/j.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 12 | This App may have root detection capabilities. | secure | OWASP MASVS: MSTG-RESILIENCE-1 | com/grandroundshealth/grandrounds/presentation/splash/a0.java<br>f2/x0.java<br>n70/k.java<br>pq/a.java |
| 13 | IP Address disclosure | warning | CWE: CWE-200: Information Exposure<br>OWASP MASVS: MSTG-CODE-2 | com/grandroundshealth/grandrounds/analytics/SnowplowHelper.java<br>n70/k.java<br>org/beyka/tiffbitmapfactory/BuildConfig.java<br>org/conscrypt/CertificatePriorityComparator.java<br>org/conscrypt/ChainStrengthAnalyzer.java<br>org/conscrypt/EvpMdRef.java<br>org/conscrypt/OAEPParameters.java<br>org/conscrypt/OidData.java<br>org/conscrypt/OpenSSLCipherRSA.java<br>org/conscrypt/OpenSSLProvider.java<br>org/conscrypt/OpenSSLSignature.java<br>org/conscrypt/TrustManagerImpl.java<br>org/conscrypt/ct/CTConstants.java<br>us/zoom/video_sdk/o.java<br>us/zoom/video_sdk/v0.java<br>us/zoom/video_sdk/x1.java |
| 14 | Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks | high | CWE: CWE-295: Improper Certificate Validation<br>OWASP Top 10: M3: Insecure Communication<br>OWASP MASVS: MSTG-NETWORK-3 | org/conscrypt/Conscrypt.java |
| 15 | App can write to App Directory. Sensitive Information should be encrypted. | info | CWE: CWE-276: Incorrect Default Permissions<br>OWASP MASVS: MSTG-STORAGE-14 | com/grandroundshealth/grandrounds/di/modules/Auth0Module.java<br>e1/e.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 16 | [This App may request root (Super User) privileges.](#) | warning | CWE: CWE-250: Execution with Unnecessary Privileges<br>OWASP MASVS: MSTG-RESILIENCE-1 | n00/a.java<br>n70/e.java |
| 17 | App creates temp file. Sensitive information should never be written into a temp file. | warning | CWE: CWE-276: Incorrect Default Permissions<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | bo/c.java<br>com/grandroundshealth/grandrounds/helpers/CameraHelper.java |
| 18 | This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files. | info | OWASP MASVS: MSTG-CRYPTO-1 | net/sqlcipher/database/SupportHelper.java |
| 19 | [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<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-3 | l10/a.java |
| 20 | [Ensure that user controlled URLs never reaches the Webview. Enabling file access from URLs in WebView can leak sensitive information from the file system.](#) | warning | CWE: CWE-200: Information Exposure<br>OWASP Top 10: M1: Improper Platform Usage<br>OWASP MASVS: MSTG-PLATFORM-7 | com/grandroundshealth/grandrounds/presentation/document/DocumentDetailViewActivity.java |

# 📇 NIAP ANALYSIS v1.3

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

# 🖧 BEHAVIOUR ANALYSIS

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---------|-----------|-------|-------|
| 00022 | Open a file from given absolute path of the file | file | ay/p.java<br>b00/e.java<br>com/airbnb/lottie/k.java<br>com/airbnb/lottie/n.java<br>com/braintreepayments/api/m.java<br>com/braintreepayments/api/m1.java<br>com/fasterxml/jackson/databind/ser/std/FileSerializer.java<br>com/grandroundshealth/grandrounds/chat/presentation/dialogs/l.java<br>com/grandroundshealth/grandrounds/chat/presentation/dialogs/m.java<br>com/grandroundshealth/grandrounds/chat/presentation/dialogs/n.java<br>com/grandroundshealth/grandrounds/chat/presentation/dialogs/r.java<br>com/grandroundshealth/grandrounds/chat/presentation/y.java<br>com/grandroundshealth/grandrounds/data/remote/RemoteRepoImpl.java<br>com/grandroundshealth/grandrounds/helpers/CameraHelper.java<br>com/grandroundshealth/grandrounds/helpers/r3.java<br>com/grandroundshealth/grandrounds/presentation/document/h.java<br>com/grandroundshealth/grandrounds/presentation/insurance/InsuranceCardActivity.java<br>com/launchdarkly/sdk/android/k0.java<br>com/launchdarkly/sdk/android/x.java<br>com/salesforce/marketingcloud/storage/d.java<br>com/salesforce/marketingcloud/util/c.java<br>com/zipow/cmmlib/AppContext.java<br>cv/a.java<br>dq/b.java<br>ds/c.java<br>gn/d.java<br>gn/q.java<br>io/realm/e.java<br>io/realm/e0.java<br>io/realm/internal/OsSharedRealm.java<br>io/realm/internal/Util.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| | | | ip/b.java<br>ix/e.java<br>j0/e.java<br>k10/u.java |
| | | | m30/d.java<br>n0/e.java<br>n70/h.java<br>nr/h.java<br>nx/k.java<br>org/beyka/tiffbitmapfactory/TiffBitmapFactory.java<br>org/beyka/tiffbitmapfactory/TiffConverter.java<br>org/beyka/tiffbitmapfactory/TiffSaver.java<br>p80/b.java<br>qw/b.java<br>us/zoom/libtools/utils/ZmAppUtils.java<br>us/zoom/libtools/utils/ZmMimeTypeUtils.java<br>us/zoom/libtools/utils/ZmUIUtils.java<br>us/zoom/video_sdk/h0.java<br>us/zoom/video_sdk/j0.java<br>us/zoom/video_sdk/m.java<br>us/zoom/video_sdk/r1.java<br>us/zoom/video_sdk/s1.java<br>vz/e.java<br>vz/h.java<br>wy/a.java<br>x/f.java<br>yu/a.java<br>yu/b.java<br>zu/c.java<br>zu/j.java |
| | | | a5/a.java<br>ay/i.java<br>ay/p.java<br>b00/e.java<br>bo/c.java<br>com/airbnb/lottie/k.java<br>com/bumptech/glide/disklrucache/DiskLruCache.java<br>com/bumptech/glide/load/ImageHeaderParserUtils.java<br>com/bumptech/glide/load/model/FileLoader.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| | | | com/bumptech/glide/load/resource/bitmap/ImageReader.java |
| | | | com/fasterxml/jackson/core/TokenStreamFactory.java |
| | | | com/fasterxml/jackson/databind/ObjectReader.java |
| | | | com/grandroundshealth/grandrounds/helpers/SecurityHelper.java |
| 00013 | Read file and put it into a stream | file | com/grandroundshealth/grandrounds/helpers/w3.java |
| | | | com/salesforce/marketingcloud/storage/d.java |
| | | | com/salesforce/marketingcloud/tozny/AesCbcWithIntegrity$PrngFixes$LinuxPRNGSecureRandom.java |
| | | | com/salesforce/marketingcloud/util/c.java |
| | | | com/salesforce/marketingcloud/util/d.java |
| | | | com/salesforce/marketingcloud/util/e.java |
| | | | com/zipow/cmmlib/AppContext.java |
| | | | cs/d.java |
| | | | d30/w.java |
| | | | f2/h0.java |
| | | | gn/i.java |
| | | | h60/i.java |
| | | | kr/a.java |
| | | | kw/c.java |
| | | | l80/b.java |
| | | | m30/d.java |
| | | | ms/h.java |
| | | | ms/m.java |
| | | | ms/p.java |
| | | | nx/f.java |
| | | | org/conscrypt/DefaultSSLContextImpl.java |
| | | | org/conscrypt/FileClientSessionCache.java |
| | | | org/conscrypt/KeyManagerFactoryImpl.java |
| | | | p000do/c.java |
| | | | pr/g.java |
| | | | us/zoom/libtools/utils/ZmAppUtils.java |
| | | | us/zoom/video_sdk/b2.java |
| | | | us/zoom/video_sdk/e1.java |
| | | | us/zoom/video_sdk/e2.java |
| | | | us/zoom/video_sdk/j0.java |
| | | | us/zoom/video_sdk/j1.java |
| | | | us/zoom/video_sdk/m0.java |
| | | | us/zoom/video_sdk/q1.java |
| | | | us/zoom/video_sdk/r1.java |
| | | | us/zoom/video_sdk/s1.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| | | | vz/a.java<br>vz/e.java<br>vz/h.java<br>wy/a.java |
| | | | x/f.java<br>x0/j.java<br>z3/c.java |
| 00014 | Read file into a stream and put it into a JSON object | file | zu/j.java<br>a5/a.java<br>ay/p.java<br>b00/e.java<br>bo/c.java<br>kr/a.java<br>m30/d.java<br>wy/a.java<br>x0/j.java<br>z3/c.java |
| 00005 | Get absolute path of file and put it to JSON object | file | ay/p.java<br>b00/e.java<br>com/braintreepayments/api/m.java<br>com/grandroundshealth/grandrounds/data/remote/RemoteRepoImpl.java<br>com/grandroundshealth/grandrounds/presentation/insurance/InsuranceCardActivity.java<br>cv/a.java<br>gn/d.java<br>j0/e.java<br>m30/d.java<br>n0/e.java<br>n70/h.java<br>wy/a.java<br>yu/a.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| 00004 | Get filename and put it to JSON object | file collection | a5/a.java<br>ay/p.java<br>b00/e.java<br>c4/b.java<br>com/grandroundshealth/grandrounds/data/remote/RemoteRepoImpl.java<br>fv/a.java<br>m30/d.java<br>mg/a.java<br>n70/h.java<br>n70/n.java<br>qw/a.java<br>xq/c.java<br>yu/a.java |
| 00009 | Put data in cursor to JSON object | file | bo/c.java<br>com/braintreepayments/api/m.java<br>com/salesforce/marketingcloud/storage/db/a.java<br>com/salesforce/marketingcloud/storage/db/d.java<br>com/salesforce/marketingcloud/storage/db/f.java<br>com/salesforce/marketingcloud/storage/db/m.java<br>com/salesforce/marketingcloud/storage/db/upgrades/a.java<br>com/salesforce/marketingcloud/storage/db/upgrades/k.java<br>dz/a.java<br>e80/l.java<br>er/a.java<br>hq/a.java<br>j0/e.java<br>m30/d.java<br>mg/a.java<br>n70/l.java<br>ny/c.java<br>qw/a.java<br>v30/b.java<br>vy/b.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---------|-----------|-------|-------|
| 00192 | Get messages in the SMS inbox | sms | f20/g.java<br>hq/a.java<br>m30/f.java<br>us/zoom/video_sdk/r1.java |
| | | | a3/a.java<br>a70/q.java<br>c10/i.java<br>c3/b.java<br>com/auth0/android/provider/CustomTabsOptions.java<br>com/braintreepayments/api/DropInActivity.java<br>com/braintreepayments/api/i0.java<br>com/grandroundshealth/grandrounds/chat/presentation/ChatActivity.java<br>com/grandroundshealth/grandrounds/chat/presentation/dialogs/FilePreviewDialog.java<br>com/grandroundshealth/grandrounds/chat/presentation/m.java<br>com/grandroundshealth/grandrounds/chat/presentation/n2.java<br>com/grandroundshealth/grandrounds/chat/presentation/y1.java<br>com/grandroundshealth/grandrounds/extensions/ActivityExtensionsKt.java<br>com/grandroundshealth/grandrounds/extensions/FragmentExtensionsKt.java<br>com/grandroundshealth/grandrounds/helpers/SendBirdNotificationService.java<br>com/grandroundshealth/grandrounds/helpers/Utils.java<br>com/grandroundshealth/grandrounds/helpers/o0.java<br>com/grandroundshealth/grandrounds/presentation/base/BaseActivity.java<br>com/grandroundshealth/grandrounds/presentation/findCareRecommendation/FindCareRecommendationActivity.java<br>com/grandroundshealth/grandrounds/presentation/findcare/results/FindCareProviderDetailsActivity.java<br>com/grandroundshealth/grandrounds/presentation/findcare/results/ProviderLocationsAdapter.java<br>com/grandroundshealth/grandrounds/presentation/findcare/results/ProviderMatchAdDialog.java<br>com/grandroundshealth/grandrounds/presentation/findcare/results/l0.java<br>com/grandroundshealth/grandrounds/presentation/findcare/results/l2.java<br>com/grandroundshealth/grandrounds/presentation/findcare/results/o0.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| tf0063 | Implicit intent(view a web page, make a phone call, etc.) | control | com/grandroundshealth/grandrounds/presentation/flexibleRegistration/screens/signup/account/a.java<br>com/grandroundshealth/grandrounds/presentation/memberForms/b.java<br>com/grandroundshealth/grandrounds/presentation/nativeHome/NativeHomeActivity.java<br>com/grandroundshealth/grandrounds/presentation/nativeHome/tabs/BrowserFragment.java<br>com/grandroundshealth/grandrounds/presentation/nativeHome/tabs/home/adapters/c.java<br>com/grandroundshealth/grandrounds/presentation/nativeHome/tabs/home/l.java<br>com/grandroundshealth/grandrounds/presentation/openenrollment/b.java<br>com/grandroundshealth/grandrounds/presentation/splash/n.java<br>com/grandroundshealth/grandrounds/presentation/splash/o.java<br>com/grandroundshealth/grandrounds/presentation/telemedicine/intake/k.java<br>com/grandroundshealth/grandrounds/presentation/unifiedIntake/assessment/l0.java<br>com/grandroundshealth/grandrounds/views/CustomWebView.java<br>com/grandroundshealth/grandrounds/views/e0.java<br>com/grandroundshealth/grandrounds/views/f0.java<br>com/grandroundshealth/grandrounds/views/i0.java<br>com/grandroundshealth/grandrounds/views/o0.java<br>com/grandroundshealth/grandrounds/views/t0.java<br>com/grandroundshealth/grandrounds/views/u0.java<br>com/grandroundshealth/grandrounds/views/v0.java<br>com/salesforce/marketingcloud/notifications/b.java<br>lx/a.java<br>m30/f.java<br>nh/a.java<br>p00/j.java<br>ty/c.java<br>us/zoom/libtools/utils/ZmMimeTypeUtils.java<br>us/zoom/libtools/utils/ZmUIUtils.java<br>us/zoom/video_sdk/e2.java<br>us/zoom/video_sdk/t1.java<br>us/zoom/video_sdk/y1.java<br>uz/d.java<br>x5/g.java<br>yu/b.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| 00112 | Get the date of the calendar event | collection calendar | com/fasterxml/jackson/databind/ser/std/StdKeySerializers.java<br>com/fasterxml/jackson/databind/util/StdDateFormat.java<br>com/grandroundshealth/grandrounds/chat/presentation/ChatVM.java<br>xv/j.java<br>yy/a.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---------|-----------|-------|-------|
| 00051 | Implicit intent(view a web page, make a phone call, etc.) via setData | control | a70/q.java<br>c10/i.java<br>c3/b.java<br>com/braintreepayments/api/i0.java<br>com/grandroundshealth/grandrounds/chat/presentation/m.java<br>com/grandroundshealth/grandrounds/chat/presentation/n2.java<br>com/grandroundshealth/grandrounds/extensions/ActivityExtensionsKt.java<br>com/grandroundshealth/grandrounds/extensions/FragmentExtensionsKt.java<br>com/grandroundshealth/grandrounds/helpers/SendBirdNotificationService.java<br>com/grandroundshealth/grandrounds/helpers/Utils.java<br>com/grandroundshealth/grandrounds/helpers/o0.java<br>com/grandroundshealth/grandrounds/presentation/findcare/results/FindCareProviderDetailsActivity.java<br>com/grandroundshealth/grandrounds/presentation/findcare/results/ProviderLocationsAdapter.java<br>com/grandroundshealth/grandrounds/presentation/findcare/results/ProviderMatchAdDialog.java<br>com/grandroundshealth/grandrounds/presentation/flexibleRegistration/screens/signup/account/a.java<br>com/grandroundshealth/grandrounds/presentation/nativeHome/tabs/home/adapters/c.java<br>com/grandroundshealth/grandrounds/presentation/openenrollment/b.java<br>com/grandroundshealth/grandrounds/presentation/telemedicine/intake/k.java<br>nh/a.java<br>us/zoom/libtools/utils/ZmMimeTypeUtils.java<br>us/zoom/libtools/utils/ZmUIUtils.java<br>us/zoom/video_sdk/e2.java<br>us/zoom/video_sdk/t1.java<br>x5/g.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| 00162 | Create InetSocketAddress object and connecting to it | socket | e80/c.java<br>e80/n.java<br>m30/c.java<br>m30/n.java<br>org/conscrypt/AbstractConscryptSocket.java |
| 00163 | Create new Socket and connecting to it | socket | e80/c.java<br>e80/n.java<br>m30/c.java<br>m30/n.java<br>org/conscrypt/AbstractConscryptSocket.java<br>org/conscrypt/KitKatPlatformOpenSSLSocketImplAdapter.java<br>org/conscrypt/PreKitKatPlatformOpenSSLSocketImplAdapter.java |
| 00036 | Get resource file from res/raw directory | reflection | c3/b.java<br>com/braintreepayments/api/i0.java<br>com/grandroundshealth/grandrounds/chat/presentation/dialogs/FilePreviewDialog.java<br>com/grandroundshealth/grandrounds/data/remote/RemoteRepoImpl.java<br>com/grandroundshealth/grandrounds/extensions/ActivityExtensionsKt.java<br>com/grandroundshealth/grandrounds/extensions/FragmentExtensionsKt.java<br>com/grandroundshealth/grandrounds/helpers/Utils.java<br>com/grandroundshealth/grandrounds/presentation/universalLogin/UniversalWebAuthViewModel.java<br>com/salesforce/marketingcloud/notifications/b.java<br>hq/a.java<br>n70/l.java<br>us/zoom/libtools/utils/ZmMimeTypeUtils.java<br>us/zoom/libtools/utils/ZmUIUtils.java<br>us/zoom/video_sdk/r1.java<br>us/zoom/video_sdk/t1.java<br>us/zoom/video_sdk/y1.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| 00062 | Query WiFi information and WiFi Mac Address | wifi collection | n70/l.java<br>us/zoom/video_sdk/x1.java |
| 00130 | Get the current WIFI information | wifi collection | n70/b.java<br>n70/l.java<br>n70/n.java<br>us/zoom/video_sdk/x1.java |
| 00116 | Get the current WiFi MAC address and put it into JSON | wifi collection | n70/l.java |
| 00076 | Get the current WiFi information and put it into JSON | collection wifi | n70/b.java<br>n70/l.java<br>n70/n.java |
| 00082 | Get the current WiFi MAC address | collection wifi | n70/l.java<br>us/zoom/video_sdk/x1.java |
| 00102 | Set the phone speaker on | command | org/webrtc/voiceengine/AudioDeviceAndroid.java<br>org/webrtc/voiceengine/AudioDeviceAndroidAAudio.java<br>org/webrtc/voiceengine/AudioDeviceAndroidOpenSLESHelper.java |
| 00056 | Modify voice volume | control | org/webrtc/voiceengine/AudioDeviceAndroid.java<br>org/webrtc/voiceengine/AudioDeviceAndroidOpenSLESHelper.java |
| 00191 | Get messages in the SMS inbox | sms | cr/e.java<br>us/zoom/libtools/utils/ZmMimeTypeUtils.java<br>us/zoom/video_sdk/b1.java<br>us/zoom/video_sdk/r1.java<br>yq/a.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| 00091 | Retrieve data from broadcast | collection | com/grandroundshealth/feature/wizard/presentation/WizardActivity.java<br>com/grandroundshealth/grandrounds/extensions/ActivityExtensionsKt.java<br>com/grandroundshealth/grandrounds/presentation/document/DocumentActivity.java<br>com/grandroundshealth/grandrounds/presentation/document/upload/DocumentUploadActivity.java<br>com/grandroundshealth/grandrounds/presentation/findcare/results/FindCareProviderDetailsActivity.java<br>com/grandroundshealth/grandrounds/presentation/telemedicine/intake/IntakeConfirmationActivity.java<br>com/grandroundshealth/grandrounds/presentation/unifiedEligibility/EligibilityActivity.java<br>com/grandroundshealth/grandrounds/presentation/visits/pastvisitdetails/VisitSummaryActivity.java<br>com/grandroundshealth/grandrounds/presentation/visits/postvisit/PostVisitNpsActivity.java<br>com/grandroundshealth/grandrounds/presentation/visits/postvisit/RateProviderActivity.java<br>com/salesforce/marketingcloud/alarms/b.java<br>com/salesforce/marketingcloud/messages/push/a.java<br>com/salesforce/marketingcloud/sfmcsdk/components/behaviors/BehaviorManagerImpl.java<br>p000do/c.java |
| 00024 | Write file after Base64 decoding | reflection file | com/airbnb/lottie/n.java |
| 00208 | Capture the contents of the device screen | collection screen | mn/i.java<br>us/zoom/internal/share/ScreenShareServer.java |
| 00209 | Get pixels from the latest rendered image | collection | com/zipow/nydus/camera/CameraCaptureImplV2.java<br>us/zoom/internal/share/ScreenShareServer.java<br>xw/f.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| 00016 | Get location info of the device and put it to JSON object | location collection | com/grandroundshealth/grandrounds/data/remote/RemoteRepoImpl.java<br>com/salesforce/marketingcloud/messages/d.java<br>n70/n.java |
| 00189 | Get the content of a SMS message | sms | com/grandroundshealth/grandrounds/helpers/ImagePickerHelper.java<br>com/grandroundshealth/grandrounds/restJsonRpc/data/remote/rpc/UploadDocumentRequestBodyBuilder.java<br>us/zoom/libtools/utils/ZmMimeTypeUtils.java<br>us/zoom/video_sdk/b1.java<br>us/zoom/video_sdk/r1.java |
| 00188 | Get the address of a SMS message | sms | com/grandroundshealth/grandrounds/helpers/ImagePickerHelper.java<br>com/grandroundshealth/grandrounds/restJsonRpc/data/remote/rpc/UploadDocumentRequestBodyBuilder.java<br>us/zoom/libtools/utils/ZmMimeTypeUtils.java<br>us/zoom/video_sdk/b1.java<br>us/zoom/video_sdk/r1.java |
| 00200 | Query data from the contact list | collection contact | com/grandroundshealth/grandrounds/helpers/ImagePickerHelper.java<br>com/grandroundshealth/grandrounds/restJsonRpc/data/remote/rpc/UploadDocumentRequestBodyBuilder.java<br>us/zoom/libtools/utils/ZmMimeTypeUtils.java<br>us/zoom/video_sdk/b1.java<br>us/zoom/video_sdk/r1.java |
| 00201 | Query data from the call log | collection calllog | com/grandroundshealth/grandrounds/helpers/ImagePickerHelper.java<br>com/grandroundshealth/grandrounds/restJsonRpc/data/remote/rpc/UploadDocumentRequestBodyBuilder.java<br>us/zoom/libtools/utils/ZmMimeTypeUtils.java<br>us/zoom/video_sdk/b1.java<br>us/zoom/video_sdk/r1.java |
| 00042 | Query WiFi BSSID and scan results | collection wifi | n70/n.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| 00137 | Get last known location of the device | location collection | d30/g.java<br>n70/n.java |
| 00033 | Query the IMEI number | collection | n70/n.java<br>us/zoom/libtools/utils/ZmDeviceUtils.java |
| 00115 | Get last known location of the device | collection location | n70/n.java |
| 00066 | Query the ICCID number | collection | n70/n.java |
| 00067 | Query the IMSI number | collection | n70/n.java |
| 00083 | Query the IMEI number | collection telephony | n70/n.java<br>us/zoom/libtools/utils/ZmDeviceUtils.java |
| 00113 | Get location and put it into JSON | collection location | n70/n.java |
| 00078 | Get the network operator name | collection telephony | hm/a.java<br>m30/l.java<br>uz/d.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---------|-----------|-------|-------|
| 00202 | Make a phone call | control | c10/i.java<br>com/grandroundshealth/grandrounds/chat/presentation/n2.java<br>com/grandroundshealth/grandrounds/extensions/ActivityExtensionsKt.java<br>com/grandroundshealth/grandrounds/presentation/findcare/results/ProviderLocationsAdapter.java<br>com/grandroundshealth/grandrounds/presentation/findcare/results/ProviderMatchAdDialog.java<br>com/grandroundshealth/grandrounds/presentation/flexibleRegistration/screens/signup/account/a.java<br>nh/a.java<br>us/zoom/libtools/utils/ZmMimeTypeUtils.java<br>us/zoom/video_sdk/t1.java |
| 00203 | Put a phone number into an intent | control | c10/i.java<br>com/grandroundshealth/grandrounds/chat/presentation/n2.java<br>com/grandroundshealth/grandrounds/extensions/ActivityExtensionsKt.java<br>com/grandroundshealth/grandrounds/presentation/findcare/results/ProviderLocationsAdapter.java<br>com/grandroundshealth/grandrounds/presentation/findcare/results/ProviderMatchAdDialog.java<br>com/grandroundshealth/grandrounds/presentation/flexibleRegistration/screens/signup/account/a.java<br>nh/a.java<br>us/zoom/libtools/utils/ZmMimeTypeUtils.java<br>us/zoom/video_sdk/t1.java |
| 00052 | Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.) | sms | us/zoom/libtools/utils/ZmMimeTypeUtils.java<br>us/zoom/video_sdk/b1.java<br>us/zoom/video_sdk/r1.java |
| 00012 | Read data and put it into a buffer stream | file | org/conscrypt/DefaultSSLContextImpl.java<br>us/zoom/video_sdk/e1.java<br>us/zoom/video_sdk/r1.java<br>us/zoom/video_sdk/s1.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---------|-----------|-------|-------|
| 00011 | Query data from URI (SMS, CALLLOGS) | sms calllog collection | us/zoom/libtools/utils/ZmMimeTypeUtils.java<br>us/zoom/video_sdk/b1.java<br>us/zoom/video_sdk/r1.java |
| 00077 | Read sensitive data(SMS, CALLLOG, etc) | collection sms calllog calendar | com/bumptech/glide/load/data/mediastore/ThumbFetcher.java<br>nn/c.java<br>us/zoom/libtools/utils/ZmMimeTypeUtils.java<br>us/zoom/video_sdk/b1.java<br>us/zoom/video_sdk/r1.java |
| 00015 | Put buffer stream (data) to JSON object | file | r70/d.java |
| 00114 | Create a secure socket connection to the proxy address | network command | i30/l.java<br>z70/i.java |
| 00072 | Write HTTP input stream into a file | command network file | kw/a.java |
| 00108 | Read the input stream from given URL | network command | com/braintreepayments/api/p0.java<br>kw/a.java |
| 00025 | Monitor the general action to be performed | reflection | p000do/c.java |
| 00125 | Check if the given file path exist | file | hp/b.java<br>p000do/c.java |
| 00065 | Get the country code of the SIM card provider | collection | us/zoom/video_sdk/c2.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---------|-----------|-------|-------|
| 00134 | Get the current WiFi IP address | wifi collection | us/zoom/video_sdk/x1.java |
| 00183 | Get current camera parameters and change the setting. | camera | com/zipow/nydus/camera/CameraCaptureImplV1.java<br>com/zipow/nydus/camera/CameraMgrV1.java |
| 00003 | Put the compressed bitmap data into JSON object | camera | bo/c.java<br>com/grandroundshealth/grandrounds/helpers/Utils.java<br>er/a.java<br>m30/d.java |
| 00187 | Query a URI and check the result | collection sms calllog calendar | us/zoom/libtools/utils/ZmMimeTypeUtils.java<br>us/zoom/video_sdk/b1.java |
| 00153 | Send binary data over HTTP | http | n70/p.java |
| 00171 | Compare network operator with a string | network | hm/a.java |
| 00132 | Query The ISO country code | telephony collection | hm/a.java |
| 00210 | Copy pixels from the latest rendered image into a Bitmap | collection | xw/f.java |
| 00175 | Get notification manager and cancel notifications | notification | com/grandroundshealth/grandrounds/helpers/HardLogoutHelper.java |
| 00002 | Open the camera and take picture | camera | com/zipow/nydus/camera/CameraCaptureImplV1.java |
| 00001 | Initialize bitmap object and compress data (e.g. JPEG) into bitmap object | camera | us/zoom/video_sdk/s1.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---|---|---|---|
| 00092 | Send broadcast | command | us/zoom/video_sdk/t1.java |
| 00131 | Get location of the current GSM and put it into JSON | collection location | n70/b.java |
| 00139 | Get the current WiFi id | collection wifi | n70/b.java |
| 00135 | Get the current WiFi id and put it into JSON. | wifi collection | n70/b.java |
| 00099 | Get location of the current GSM and put it into JSON | collection location | n70/b.java |

# 🗄 FIREBASE DATABASES ANALYSIS

| TITLE | SEVERITY | DESCRIPTION |
|---|---|---|
| App talks to a Firebase database | info | The app talks to Firebase database at https://dod-android-51dd2.firebaseio.com |
| Firebase Remote Config disabled | secure | Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/492158283327/namespaces/firebase:fetch?key=AIzaSyAv42tiga4w-8zHdzNlHJXv6x51oiyK_ac. This is indicated by the response: The response code is 403 |

# ⠿ ABUSED PERMISSIONS

| TYPE | MATCHES | PERMISSIONS |
|---|---|---|
| Malware Permissions | 14/25 | android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.READ_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 | 8/44 | android.permission.FOREGROUND_SERVICE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.BROADCAST_STICKY, 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 |
|---|---|

# ⊕ DOMAIN MALWARE CHECK

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| anthem.com | ok | **IP:** 162.95.221.218<br>**Country:** United States of America<br>**Region:** Indiana<br>**City:** Indianapolis<br>**Latitude:** 39.772247<br>**Longitude:** -86.156517<br>**View:** Google Map |
| grandrounds.qualtrics.com | ok | **IP:** 23.202.57.104<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Jose<br>**Latitude:** 37.339390<br>**Longitude:** -121.894958<br>**View:** Google Map |
| www.world | ok | **IP:** 99.83.155.228<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.606209<br>**Longitude:** -122.332069<br>**View:** Google Map |
| member.uat.includedhealth.com | ok | **IP:** 13.219.66.73<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |
| www.a | ok | No Geolocation information available. |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| www.manifestations | ok | No Geolocation information available. |
| c.paypal.com | ok | **IP:** 151.101.193.21<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| centinelapistag.cardinalcommerce.com | ok | **IP:** 198.217.251.250<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.609699<br>**Longitude:** -122.386948<br>**View:** Google Map |
| mobile.launchdarkly.com | ok | **IP:** 52.201.12.96<br>**Country:** United States of America<br>**Region:** Virginia<br>**City:** Ashburn<br>**Latitude:** 39.043720<br>**Longitude:** -77.487488<br>**View:** Google Map |
| manage.auth0.com | ok | **IP:** 172.64.148.184<br>**Country:** United States of America<br>**Region:** Texas<br>**City:** Dallas<br>**Latitude:** 32.783058<br>**Longitude:** -96.806671<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
| --- | --- | --- |
| firebaseinstallations.googleapis.com | ok | **IP:** 173.194.219.95<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |
| api2.amplitude.com | ok | **IP:** 52.13.80.81<br>**Country:** United States of America<br>**Region:** Oregon<br>**City:** Portland<br>**Latitude:** 45.523449<br>**Longitude:** -122.676208<br>**View:** Google Map |
| static.amplitude.com | ok | **IP:** 18.238.109.83<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |
| app.igodigital.com | ok | **IP:** 52.205.196.148<br>**Country:** United States of America<br>**Region:** Virginia<br>**City:** Ashburn<br>**Latitude:** 39.043720<br>**Longitude:** -77.487488<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| docs.mongodb.com | ok | **IP:** 3.33.186.135<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |
| www.risktabsprev10pxrise25pxblueding300ballfordearnwildbox.fairlackverspairjunetechifpickevil | ok | No Geolocation information available. |
| api.sandbox.braintreegateway.com | ok | **IP:** 159.242.242.129<br>**Country:** United States of America<br>**Region:** Illinois<br>**City:** Chicago<br>**Latitude:** 41.888401<br>**Longitude:** -87.635101<br>**View:** Google Map |
| www.wencodeuricomponent | ok | No Geolocation information available. |
| www.css | ok | No Geolocation information available. |
| www.interpretation | ok | No Geolocation information available. |
| api.eu.amplitude.com | ok | **IP:** 18.195.186.41<br>**Country:** Germany<br>**Region:** Hessen<br>**City:** Frankfurt am Main<br>**Latitude:** 50.115520<br>**Longitude:** 8.684170<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
| --- | --- | --- |
| xml.org | ok | **IP:** 104.239.142.8<br>**Country:** United States of America<br>**Region:** Texas<br>**City:** Windcrest<br>**Latitude:** 29.499678<br>**Longitude:** -98.399246<br>**View:** Google Map |
| issuetracker.google.com | ok | **IP:** 64.233.177.101<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |
| www.centivo.com | ok | **IP:** 141.193.213.10<br>**Country:** United States of America<br>**Region:** Texas<br>**City:** Austin<br>**Latitude:** 30.271158<br>**Longitude:** -97.741699<br>**View:** Google Map |
| api.braintreegateway.com | ok | **IP:** 52.40.66.148<br>**Country:** United States of America<br>**Region:** Oregon<br>**City:** Portland<br>**Latitude:** 45.523449<br>**Longitude:** -122.676208<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| www.paypal.com | ok | **IP:** 151.101.1.21<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** [Google Map](#) |
| www.years | ok | No Geolocation information available. |
| centinelapi.cardinalcommerce.com | ok | **IP:** 198.217.251.251<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.609699<br>**Longitude:** -122.386948<br>**View:** [Google Map](#) |
| includedhealth.com | ok | **IP:** 162.159.135.42<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** [Google Map](#) |
| c.sandbox.paypal.com | ok | **IP:** 151.101.3.1<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** [Google Map](#) |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| myuhc.com | ok | **IP:** 168.183.64.162<br>**Country:** United States of America<br>**Region:** Minnesota<br>**City:** Plymouth<br>**Latitude:** 45.047699<br>**Longitude:** -93.425941<br>**View:** [Google Map](#) |
| sr-client-cfg.eu.amplitude.com | ok | **IP:** 18.155.173.112<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** [Google Map](#) |
| docs.instabug.com | ok | **IP:** 104.16.241.118<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** [Google Map](#) |
| www.hortcut | ok | No Geolocation information available. |
| api-sr.eu.amplitude.com | ok | **IP:** 52.57.251.174<br>**Country:** Germany<br>**Region:** Hessen<br>**City:** Frankfurt am Main<br>**Latitude:** 50.115520<br>**Longitude:** 8.684170<br>**View:** [Google Map](#) |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| grandroundsappchat.com | ok | No Geolocation information available. |
| app.uat.includedhealth.com | ok | **IP:** 52.206.125.156<br>**Country:** United States of America<br>**Region:** Virginia<br>**City:** Ashburn<br>**Latitude:** 39.043720<br>**Longitude:** -77.487488<br>**View:** Google Map |
| api-sr.amplitude.com | ok | **IP:** 35.83.210.70<br>**Country:** United States of America<br>**Region:** Oregon<br>**City:** Portland<br>**Latitude:** 45.523449<br>**Longitude:** -122.676208<br>**View:** Google Map |
| patient.doctorondemand.com | ok | **IP:** 34.232.204.231<br>**Country:** United States of America<br>**Region:** Virginia<br>**City:** Ashburn<br>**Latitude:** 39.043720<br>**Longitude:** -77.487488<br>**View:** Google Map |
| www.googleorganizationautocompleterequirementsconservative | ok | No Geolocation information available. |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| grandrounds.com | ok | **IP:** 162.159.135.42<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** [Google Map](#) |
| connect.werally.com | ok | **IP:** 18.238.96.25<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** [Google Map](#) |
| salesforce-marketingcloud.github.io | ok | **IP:** 185.199.109.153<br>**Country:** United States of America<br>**Region:** Pennsylvania<br>**City:** California<br>**Latitude:** 40.065632<br>**Longitude:** -79.891708<br>**View:** [Google Map](#) |
| api.uat.includedhealth.com | ok | **IP:** 34.227.131.203<br>**Country:** United States of America<br>**Region:** Virginia<br>**City:** Ashburn<br>**Latitude:** 39.043720<br>**Longitude:** -77.487488<br>**View:** [Google Map](#) |

| DOMAIN | STATUS | GEOLOCATION |
|--------|--------|-------------|
| member-apps-config.s3-us-west-1.amazonaws.com | ok | **IP:** 16.15.0.154<br>**Country:** United States of America<br>**Region:** California<br>**City:** Palo Alto<br>**Latitude:** 37.409912<br>**Longitude:** -122.160400<br>**View:** [Google Map](#) |
| healthy.kaiserpermanente.org | ok | **IP:** 23.213.188.136<br>**Country:** Canada<br>**Region:** Ontario<br>**City:** Etobicoke<br>**Latitude:** 43.654209<br>**Longitude:** -79.567108<br>**View:** [Google Map](#) |
| api.instabug.com | ok | **IP:** 18.238.109.79<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** [Google Map](#) |
| b.stats.paypal.com | ok | **IP:** 34.106.92.18<br>**Country:** United States of America<br>**Region:** Utah<br>**City:** Salt Lake City<br>**Latitude:** 40.760780<br>**Longitude:** -111.891052<br>**View:** [Google Map](#) |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| player.vimeo.com | ok | **IP:** 162.159.138.60<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| dod-android-51dd2.firebaseio.com | ok | **IP:** 34.120.160.131<br>**Country:** United States of America<br>**Region:** Missouri<br>**City:** Kansas City<br>**Latitude:** 39.099731<br>**Longitude:** -94.578568<br>**View:** Google Map |
| apache.org | ok | **IP:** 151.101.2.132<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| www.zetetic.net | ok | **IP:** 18.238.96.111<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|--------|--------|-------------|
| unified.grandrounds.com | ok | **IP:** 44.218.99.116<br>**Country:** United States of America<br>**Region:** Virginia<br>**City:** Ashburn<br>**Latitude:** 39.043720<br>**Longitude:** -77.487488<br>**View:** Google Map |
| monitoring.instabug.com | ok | **IP:** 18.238.109.28<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** Google Map |
| doctorondemand.com | ok | **IP:** 162.159.135.42<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| www.w3.org | ok | **IP:** 104.18.22.19<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| github.com | ok | **IP:** 140.82.114.3<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| www.gravatar.com | ok | **IP:** 192.0.73.2<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.748425<br>**Longitude:** -122.413673<br>**View:** Google Map |
| 10.0.2.2 | ok | **IP:** 10.0.2.2<br>**Country:** -<br>**Region:** -<br>**City:** -<br>**Latitude:** 0.000000<br>**Longitude:** 0.000000<br>**View:** Google Map |
| www.google.com | ok | **IP:** 142.251.15.99<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| clientsdk.launchdarkly.com | ok | **IP:** 151.101.65.55<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| member.includedhealth.com | ok | **IP:** 34.197.52.97<br>**Country:** United States of America<br>**Region:** Virginia<br>**City:** Ashburn<br>**Latitude:** 39.043720<br>**Longitude:** -77.487488<br>**View:** Google Map |
| www.example.com | ok | **IP:** 23.220.73.43<br>**Country:** Colombia<br>**Region:** Antioquia<br>**City:** Medellin<br>**Latitude:** 6.251840<br>**Longitude:** -75.563591<br>**View:** Google Map |
| sr-client-cfg.amplitude.com | ok | **IP:** 13.224.53.103<br>**Country:** United States of America<br>**Region:** Arizona<br>**City:** Phoenix<br>**Latitude:** 33.448380<br>**Longitude:** -112.074043<br>**View:** Google Map |
| javax.xml.xmlconstants | ok | No Geolocation information available. |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| www.language | ok | No Geolocation information available. |
| api-m.paypal.com | ok | **IP:** 104.16.123.74<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** [Google Map](#) |
| clientstream.launchdarkly.com | ok | **IP:** 13.248.151.210<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.627499<br>**Longitude:** -122.346199<br>**View:** [Google Map](#) |
| unified.uat.grandrounds.com | ok | **IP:** 54.144.160.240<br>**Country:** United States of America<br>**Region:** Virginia<br>**City:** Ashburn<br>**Latitude:** 39.043720<br>**Longitude:** -77.487488<br>**View:** [Google Map](#) |
| www.style | ok | **IP:** 75.2.38.108<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.606209<br>**Longitude:** -122.332069<br>**View:** [Google Map](#) |

| DOMAIN | STATUS | GEOLOCATION |
| --- | --- | --- |
| .jpg | ok | No Geolocation information available. |
| zoom.us | ok | **IP:** 170.114.52.2<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Jose<br>**Latitude:** 37.333698<br>**Longitude:** -121.889297<br>**View:** Google Map |
| mc94sp7-ybnsmpcjkq37tg75jysq.device.marketingcloudapis.com | ok | **IP:** 96.43.154.32<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.788464<br>**Longitude:** -122.394608<br>**View:** Google Map |
| www.text-decoration | ok | No Geolocation information available. |
| maps.googleapis.com | ok | **IP:** 142.250.9.95<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| api.includedhealth.com | ok | **IP:** 184.73.117.42<br>**Country:** United States of America<br>**Region:** Virginia<br>**City:** Ashburn<br>**Latitude:** 39.043720<br>**Longitude:** -77.487488<br>**View:** Google Map |
| www.uclahealth.org | ok | **IP:** 104.18.172.68<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| www.yelp.com | ok | **IP:** 151.101.64.116<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| app.stack-27916.pancakes.ci.grandrounds.com | ok | No Geolocation information available. |
| play.google.com | ok | **IP:** 172.253.124.113<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| .css | ok | No Geolocation information available. |
| cmsdk.cardinalcommerce.com | ok | **IP:** 198.217.251.250<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.609699<br>**Longitude:** -122.386948<br>**View:** [Google Map](#) |
| firebase.google.com | ok | **IP:** 74.125.136.139<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** [Google Map](#) |
| auth0.com | ok | **IP:** 172.64.150.238<br>**Country:** United States of America<br>**Region:** Texas<br>**City:** Dallas<br>**Latitude:** 32.783058<br>**Longitude:** -96.806671<br>**View:** [Google Map](#) |
| www.includedhealth.com | ok | **IP:** 162.159.135.42<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** [Google Map](#) |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| braintreepayments.com | ok | **IP:** 151.101.67.1<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** [Google Map](#) |
| developer.paypal.com | ok | **IP:** 151.101.65.21<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** [Google Map](#) |
| patient-demo.doctorondemand.com | ok | **IP:** 54.85.61.220<br>**Country:** United States of America<br>**Region:** Virginia<br>**City:** Ashburn<br>**Latitude:** 39.043720<br>**Longitude:** -77.487488<br>**View:** [Google Map](#) |
| www.in | ok | No Geolocation information available. |
| app.includedhealth.com | ok | **IP:** 44.207.53.56<br>**Country:** United States of America<br>**Region:** Virginia<br>**City:** Ashburn<br>**Latitude:** 39.043720<br>**Longitude:** -77.487488<br>**View:** [Google Map](#) |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| www.paypalobjects.com | ok | **IP:** 151.101.67.1<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| www.recent | ok | No Geolocation information available. |
| appassets.androidplatform.net | ok | No Geolocation information available. |
| stage.app.igodigital.com | ok | **IP:** 98.86.87.253<br>**Country:** United States of America<br>**Region:** Washington<br>**City:** Seattle<br>**Latitude:** 47.606209<br>**Longitude:** -122.332069<br>**View:** Google Map |
| www.docs.developers.amplitude.com | ok | **IP:** 66.33.60.194<br>**Country:** Canada<br>**Region:** Ontario<br>**City:** Etobicoke<br>**Latitude:** 43.623768<br>**Longitude:** -79.559723<br>**View:** Google Map |
| www.icon | ok | No Geolocation information available. |
| www.c | ok | No Geolocation information available. |

| DOMAIN | STATUS | GEOLOCATION |
|--------|--------|-------------|
| xmlpull.org | ok | **IP:** 185.199.108.153<br>**Country:** United States of America<br>**Region:** Pennsylvania<br>**City:** California<br>**Latitude:** 40.065632<br>**Longitude:** -79.891708<br>**View:** [Google Map](#) |
| www.anthem.com | ok | **IP:** 23.63.252.98<br>**Country:** United States of America<br>**Region:** Texas<br>**City:** Dallas<br>**Latitude:** 32.783058<br>**Longitude:** -96.806671<br>**View:** [Google Map](#) |
| www.healthcare.gov | ok | **IP:** 2.19.156.60<br>**Country:** United Kingdom of Great Britain and Northern Ireland<br>**Region:** England<br>**City:** London<br>**Latitude:** 51.508530<br>**Longitude:** -0.125740<br>**View:** [Google Map](#) |

# ✉ EMAILS

| EMAIL | FILE |
|-------|------|
| contactus@instabug.com | ry/d.java |

| EMAIL | FILE |
|---|---|
| member-experience@includedhealth.com<br>support@includedhealth.com | com/grandroundshealth/grandrounds/helpers/Constants.java |

# 🕵 TRACKERS

| TRACKER | CATEGORIES | URL |
|---|---|---|
| Amplitude | Profiling, Analytics | https://reports.exodus-privacy.eu.org/trackers/125 |
| Google Firebase Analytics | Analytics | https://reports.exodus-privacy.eu.org/trackers/49 |
| Instabug | Crash reporting | https://reports.exodus-privacy.eu.org/trackers/206 |
| Pusher | | https://reports.exodus-privacy.eu.org/trackers/223 |
| Salesforce Marketing Cloud | | https://reports.exodus-privacy.eu.org/trackers/220 |

# 🔑 HARDCODED SECRETS

| POSSIBLE SECRETS |
|---|
| "com.google.firebase.crashlytics.mapping_file_id" : "3aa34659da494b36805f9c17e8b551ed" |
| "com_auth0_client_id" : "kZPKHeMKTJZLTeLSKRx3Bb0EiOEI0nX3" |

## POSSIBLE SECRETS

"com_auth0_client_id_uat" : "77w5Or7n2NnuWJUgTPBhN9m6ij5iXQf7"

"com_auth0_domain" : "auth.development.grandrounds.com"

"com_auth0_domain_prod" : "auth.grandrounds.com"

"com_auth0_domain_uat" : "auth.uat.grandrounds.com"

"firebase_database_url" : "https://dod-android-51dd2.firebaseio.com"

"google_api_key" : "AIzaSyAv42tiga4w-8zHdzNlHJXv6x51oiyK_ac"

"google_crash_reporting_api_key" : "AIzaSyAv42tiga4w-8zHdzNlHJXv6x51oiyK_ac"

"included_health_com_auth0_client_id_prod" : "T7PBJdyYXgIqSocWfysjJEcGGhXjDq9a"

"included_health_com_auth0_client_id_uat" : "gyHZeDVKXXQVG9rL18YbWZXnM3EVxteQ"

"included_health_com_auth0_domain_prod" : "auth.includedhealth.com"

"included_health_com_auth0_domain_uat" : "auth.uat.includedhealth.com"

"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"

"session_length_recommended" : "Recommended"

54fb2a5f0fede9b0ea756a67bb0a6f6a60db41a9a5e436dc2e4b27ec1a362b04

11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

## POSSIBLE SECRETS

4391d3bf0fc9eb52447db85c77a58e5f71fd86d3da1a57738ebea28fb1a3e6ad

98db1a35f176d05b0f9a80f32bd0483f391ced8f638b32d1740fcdec31ff30ce

c349ffffd134f32c7297d6b01728fc9c62371080d550094c78ab4566b938c2d3

c4e15629344aec2f0771a08553201c64ed43fcda9d168d83c61a3479dee779c4

318b3395e3f412c002d5f146f62c7808163076ab7d9e5915842428f976c7b73b

b86c9c92afc00959802a7bfb16b6cdd4bc6e9eb9025ac14984bd7ed76fb5defb

a84e81a0d1a8b95e3643694dc6f6b12f70f1acbea5af378c6d64631a95825e77

F6389234-1024-481F-9173-37D9D7F5051F

907d9a0c69710fb36e77d3875c402217f10580b057754448df82857d4ce652e8

e7049899270c86d5773b07f788912f5ae148506cd69988ea88617e27715bd783

0e55f3d6f7d16cfb62d801a6300e87f64d92a705cd7e3eae8df421a165503b4f

02b98052270800c8cb168be0676b5671449c0f7e2fe38c97c58886287758b8c2

d587dbd3ba55f2470b5b7668ad2db8fcd48aad26ebc9d21051edef57bae0dd72

d09017f6b0ded8ed5757d8b9dacd29d77a3461428b1a92ff6cf819ef53904eef

1a218cf73b10d3796748809942ba97f2d77950d8a115b2fb5b5e2be3af512737

## POSSIBLE SECRETS

cb0c98d752ddff2ac2cdd0cac75fa4fcb96e556ef9b57d3215d878c4f4cebda2

39681b3b25ca6a8e7f3049af923c204a2e0f3910bfdbbcd53c864216b685d548

8b2b94680514e32bc167da9848db16560f56652424960d29f01b7caff5b31837

80a17e47-4890-4e46-a2cf-0620c34963c3

d2a9b5d5d2c08280f2769d9e8ad7c0fc35b5a1c63f6552ddd97432124a94fea6

b4050a850c04b3abf54132565044b0b7d7bfd8ba270b39432355ffb4

230a3161ebfc70d0c09d10f2e8f1b1298f34b7f6ba07f4a64d955fedcdd1c340

7abab5ee-d2d0-4fca-a33c-155a8d5ea121

375062e4f041c8ebdbfc2382b2dbd289c0fbc2dd3393ed93a26a2dff16636db2

a12b2ae3691e96b21d1e28c911846455ea15da4391d4f4c5e28e50b225303b2e

a0f4361aa14cbd9556a94068801df97b66770412

a7f6306ba75f3d6c6c224081a92ea8bc6f94153f358fa0940d9dbd0bf54a0b37

b1c1c819ff74b3835a7089ed4e316984f5c9492380bc65ed6c0c1e81bebf8910

facc0367da9c11f2c6cb015ff9b6008a0d67587d4c4086c976abb3b5e54bede8

60a7d1d1-6fc8-481c-98b4-94ace48937c9

## POSSIBLE SECRETS

8e84a1adf045b3291be6d92573a25845e6a4223bd60baf7d5530848d71b45684

00ac090fe06dba093528946c8df5f45d68de90e97e9e531ae6e05e7dced07ede

a9ec7cfd213a1be8b41c2c20c78662c7c7addd8fad4182d5252aeb61fa928005

47ff6e52af334ff61aaf72119833d149507ab446c5b10568dcc770c145fc8ce0

fb1074372836c3a0c87b422fafe666b3eac3d8414be24992a04f54f4d46bbaad

866c648b56013f7f75920ac0452cb5668e8a44f1a5cda5ca71f4b7ab75fb7c5b

5eabf340c1c89ea86f602d4af1a74e9728067d4e2886f1a7113635325a7e998b

2222984e582cb73b13855f30bd00dd31de89a2e52c1a18b0d5975642d0c45207

925b0398-2130-4af1-a834-8f9f26fdfae0

39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319

0cb5309bea886c3bb3e6d802fc93d1d6517a805360fe654db89c087d12202031

115792089210356248762697446949407573530086143415290314195533631308867097853951

516c5216ef294ad04157e4a22e3541978cd90e44d681ce50ee19e8b09dc93dc6

fdbf475d0892fd619f48cf36bd7eada835a30c1d808e8eab52e4d2fe87da9572

5181942b9ebc31ce68dacb56c16fd79f

## POSSIBLE SECRETS

68647976601306097149819007990813932172694353001433054093944634591855431833976553942450577463332171975329639963713633211138647686124403803403728088927070054 49

2671b4ad9c21fbf95c71c442a1e9c97b28a4ab27bc5a945cd38e9b3b9192b1f2

aec84c10d1c04372e3928d5333d03fe7cdec6fa6064310e00e71e5badaaa9a87

ef07c3d1b2015bb7513ff36f347da1fc1d321fc080fe451e78f3ccc960ad47ec

8704f7b1ce1afaf889fcb4cb674f39957b22ec4e10b7798a78e5ad01001f6576

daa18932332f575e15e1003460f334487b74928f6221bd66108d3e4a58850416

16679223-6260-4dc4-91ed-d29e765f752f

09050e2423dec835c7f6102a923d0772cb84ba6a08b122a007e38f841d523638

8fa977342b4437ff7bf405f8bc4a73b109a9e5caf1572ecbb64a85e948a2612e

f357c96e9d42abcaf66b0ff8f6733b3718db1c5b656e59ef89afdd03b88bfc4f

6cc5e1afe46bed3a0eaa8d1d741e2e58681cce75ac2a1409a17a71b4bd8dab29

11579208921035624876269744694940757352999695522413576034242259061068512044369

1fd9a10aee82cf5aedcd99a5ac43c5f44ee7bf6e4236c9992dd023e96dea82f9

72aca0d17ff9b41db0a37a28f7a7ea8713e4d8c030564106ec8ed000848a7e20

8e57dad0fe84a9f91294b8f65e117ef9d58ae2826fb7731027533f6258a1aae6

## POSSIBLE SECRETS

80c2aae5b81c7144ef5ead540b44708d11dcb51f4d5158233ea4ab587918b2c9

57d9c3e1-0797-4b55-af1b-213a1c8b32a0

8be47471b8e4a70457fe2982587f6a3e1dcf0fd7b23518b020f31cd878aa1fed

27eca5c117181bd01897bc4c91a19bbab3f5621dfdbf0775d97c856ba5e25d79

4ebea47d3cd270d9b338483f9bea309aa894b58175ea9f814965ac6011d07b85

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

0694ac0b07660b0f2621919e268fe7e5072f881430a810e3dfd67d34908eac59

50f4d94100437b6d36bc8e18905a605a3536c76e003a8b8158eb1c9d1a02fb6b

58f2e999177d750df03c8cc2a8584bbc8e417ea566b6272f8b397d938c449ed8

d3966ff6dab6e25012de345b8c613b4ec9d7403f11e724a33918c194793301b0

4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

d39ff34e6b8e0e8fac825e9294875a9947d6d0171ee7010fb7f8693947b03743

cfa03fe0881fdfb9da7e4d3a5f716278925e36e7257bc1636da47c3a91604719

f87bd119015368c4e7eba9cc3abf8c9f4cbf263967cb2da9d464ab26406cb055

f0a095e2116f1310911553a4912cbc17283e8c7045e901c785daa6e42d70a9eb

## POSSIBLE SECRETS

ea1826d6acae842ce4f07bdcdd349fc6206d5999e42a27262cf835c20a894280

694ecffd6c45e68eeed0cc294efbb29d623a2239f4e3f2dfdef07b876bb4e11f

7ba7ccd4e3a99c2a0ce12aa112b610667daf6575c62bbf6e52186007bfe302d7

8ef07cd99aa2698776808d32e933b190110ca4417f9d16248b27fae67bf61581

ae2044fb577e65ee8bb576ca48a2f06e

f1679ed909e40fa0f10371f62a07c5e71d2fa5e9e7ed3dad1ac51b87477caa7c

d9316cad25180f236c5dba804172314de86517ef55ac7ee3ed7e068f62fd67f3

39402006196394479212279040100143613805079739270465446679469052796276593991132635693989563081522949135544336539 42643

69ef694d253b0027f69979e1f82116db517ddc7a974d6c5b46629b945a32fb38

9418bbf61509a53cbb28a948f58bab8a1fd649627b4193d3cfb28c11edf35e76

bf9ed8e06b2dd37d311b742c76e7854e724d4afbabf41ef8d457028d04248a28

8587ca25b427551471607ff3a9c73c82d40ee92f088f04a345a263b0b0411772

9c1a968ac1f140d7b11adaa7e6e598f987cbb9e35a6b5bdb3388b3c5c0cead6c

96832689b5b51b3e98667e740cd070f5a590a43e97781cce8d4797210e61c20d

b-586a583c-d090-4b56-ab39-34d86493d579

## POSSIBLE SECRETS

de27601127310acabbf81e7bec5ac3190630b06134ad46386bb6bff47512d18f

33d69137f717f3eb52d6d8a8134e084a5f25512a800bb252f022bf07df55cb9b

06a7a56a2b72195dbc384aa0ab7fe2b4492203a8e101af495a2b2d87ee50a813

sfmcAppToken=ZwxcFbtUbMDYhazbETbEBncI

9ce1fbacd514784a1b4c017a0cb2933a

AIzaSyAd8ajEllwvUZsxOckd5aul0cYEEQPizqk

a3d23ca80f1cc1353d151cae4cab8ad8e7188fb038dd45175824dcb82d25b0f3

f42e4b2c3f9732de58b6b0c3e47954a48b618d95c81a65d1136a0fb5b54477d9

81e758ebf4894f57cb30521017143c71146cb8f1576953be80437681b363dc9b

956d31b6-ce80-4783-a131-56ca2d7943e8

5df63c35204735cc2b9e8c03c7e2c8def4e340519e084367812363babd3a0628

8a31e699faa87c9f2c3e853b991ace7765280dd15473c9ec1603dad820ccc485

17114d1e25b9c90d1a7e19fadaf37aeb5971f6e14af9c57f950c086e4aac1cd2

8bf5395d7823ae1bd501b2ae64d8c7d3ae8b583422d1154416fae150ff1a93c6

c5babb6ba070462ffc52b724d54828f4c165bff33ce94cef89b3c11bec7daa32

## POSSIBLE SECRETS

051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00

94936c82e6284a1811c33111b6a8343aa0e273ad7f0900eed4d92dd4b6b91fd5

b07d3e3f81aa9c3fed04cf360ba78f109b8c6566651b0562d2dd04def79ee8a5

6e4403f6d7f108547367fb51369aed43c81013506e82f3b8c374cc52874c0b68

7d83a75d7ffd68237d43e0b6fa6d6ad23cdbe2247fddbc50406297a40f60f1b7

5a4cf4990a702e1e8b08daf90f2447cda574a45fe62c0bd292a1ae9a5adc0b28

331482b3f077ee7a9117038e145239191c63e4c5b8b3d8385dc1018759db83e5

0d60aba58445e4297e9ca577bfb8a36d8f05b32c1e80900ec74d731d49bfe91b

2d1ecb5b6d3ed82acb79c43d5fb10dd6

17558a65455c83d5b9636598a871eb2530801a4469156a2cd4c75499569629d9

918021876ffc85c4f999d1752c41e4355f3945a69c75f89b0d3551464146b22d

a8ad19739626ef183921abb42e35abf32778a548ca12eef9bb3d7206388f38d3

32285baf7f5771d8c6fa39272384bd46560ea5d7342d5c679da086272c1b7d86

7135f59fbb9f7b59f893f39410491e90f469f8a2bf922555bb286d21967a2f43

b4ef81b27d61680727b639482c4dda4ef6c14c4dbd8545156cfea7f333a7f1b7

## POSSIBLE SECRETS

7e1c915fcd1b1b2467edc1c86198b5dc0c9230ae5f231c3e3326f899dfd412be

6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

googleDirectionToken=AIzaSyCmQ6pxvUqjkATd9KS

705a6513dcda931e5d9be8b91292994d1de5f8880355158f76f05e8df0ab02f6

a5887600-9914-471e-b571-14fd03dd624a

28488e721189fe3a9e16a75be646a9b2b92bf7ed9bb5096ddef5fbf06b4a1c82

308201e53082014ea00302010202044faa0a6b300d06092a864886f70d01010505003036310b300906035504061302555331273025060355040a131e5a6f6d20566964656f20436f6d6d756e69636174696f6e7320496e632e3020170d3132303530393036313035315a180f32303036323034323733036313035315a3036310b300906035504061302555331273025060355040a131e5a6f6d20566964656f20436f6d6d756e69636174696f6e7320496e632e30819f300d06092a864886f70d010101050003818d00308189028181009b463f2d26827dcd115aecc70e5124b9d68cd78e401489c9eae4cd19bc4ca0576ad28168a81f71e8d8b5a7cdc956d937510df3cfa956c28d55668894c33ce08052946ae4af1455becfd2243897f1731fd17a547260c5a52daaebf8ab8a9aad1ad18f99ff696dcf7d713f6540f102c274fbfbc895045f25af67d0fe8dedc536510203010001300d06092a864886f70d0101050500038181000db7990467b840f362bad88c35874abe4d10d3a872356e57581f06fcbac79ebf6d82bb380d14461eded133d9630d77a6b7bcc9953f1ab02437c6317646218b6a37f3c75e833096fa24a473a9b53b1cca4269f0c753ec33239c9a293ea87c27121f424cb9ec1d7765c7fc0c51b7ee2ec4ab9d15a896eeb150ac06fe67086f1c70

7851c93f58f3ad1e8dda7fe391a8c740cac0b59dc45521e8860a99509443c336

da7206aeb981f593437889447220364b00912e0d65f2926d401f239e1e2dd739

0929310af287ae54ac286aa4b377e28e

196d2cf3098716cc12426fcdae82b1a89661aff740b5fe7c4f4e3b7ae45e01ce

48ff93924da535f205a6c1317b8b5fa51ed4929fd786017bfaba2943cd56cbff

## POSSIBLE SECRETS

amplitudeDebugToken=2d1ecb5b6d3ed82acb79c43d5fb10dd6

87de51d264445a0acc7d017c735c7daa296f741f4f807e38e84e969b33221d71

05028213e19304ed4a1af316369af27e53a8e899fe5e68292b4b45e30d1fdd32

20792b88430cc44a8a5373bd6e37b4bfbaf0fcbf98b6b7fdbec665dfe31f8c00

B2774DFE-0FDB-4968-9ADA-8DB9977D87C7

0caf82126290ea5d574fe64f656ae2114790d1c530cd45fe122e54a2b53aa477

92f8acdc9e5aa8abd9a5bca506af2857d442dcbadade4c0909a3ecf856412632

34c5d0218f540e28ba02dfc1b43a5dd26daaeee347565b8393de389d29f2b8f3

fe770f49f74ca85a4ff374b06607e785fa3760e10c6065d991ff774a6fc3616e

6a8ec58fc43077828e267e3c5abb361fe939f2faae6f0d8e8e29f57ef5d8acba

5bcdcb40e968f490a16885f7b2c03c0f318dfcc8630951f29bb7e4ad38e70a2e

889b1c8271e8c66fde9688c57c864843b0e5f2efcd07d7975e3c8ece150618ac

e1294c887fd702ead25c588ca639b431949e2625fd6bdece153203404caf4d53

07f634caac2ca1610a50390e5235794f1d7374055e1c5e0ac6c4d7440b74402c

6f2e4a8d885617e2793d5e76d1c8a7058c0dd1f3e657af8c90503bfd6cd5c1f1

## POSSIBLE SECRETS

d54802ba8a1e1c85402d31968c99a8d0bab0205e384e727ce5532777f1f48847

8e53b21b65a992a4a32fff11276cc0fd5cf99ecb67b56c0b2c9da605d9da318a

efc4e3ab-3fb5-4ac3-95b6-a998c23542e3

10a9834a1b4f5d99c9948af200c0b7e5d989dc1545d49008ab60311cd6cf918a

1bc4b1b3761cfe569fefcdfd493c16d3922033514fdca52243269aab8c1f594f

2bbb0ed79f845a05e71c5f4b512925bd7bfbd8d7dfb2c108dc6b58254d18ed9a

a1ed6319c665d812b6fd8761a3fc095c25a30ce4173692f8f6213d61238d1d8a

f2eae87dff09f2a386fef4b7479516c800185ce97440def7fc9c084d9da92c5c

c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

a73ee63fcd5ba9e6c74423a23b894da266cb42b0bd4f1d9ccf638ac2742bc871

3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

765c0a26124f2c89d720a9f1b29736fdaa18d705d96df26c5e5eaa8a291c751b

b70e0cbd6bb4bf7f321390b94a03c1d356c21122343280d6115c1d21

f579c124309057138c03c921ab27e77b2bf787f5c6f0f3c0bcf26422549b7ab1

a49976fc76d4b6e9ad40690a11a2cc04cb078660136b5360f64d321565df9b9c

## POSSIBLE SECRETS

2d4240c3ec3b85d4f372c6130f89bba736fbc595ada8a342d864ab58e4f8d505

3535cb13198f109d02cc70b9711709359f80053b2dd58528cfaab976e8d7e1aa

amplitudeProdToken=893020632f019f34c099e04b1b14a253

9c47d7d9-7193-49fc-a16e-df5def9a4e7b

cc1379b7e8c147a9abf4068c7af4089e927ec3ae258b8436ae550061e050ce08

fb16d596d2e4a66c684ffece8b37601e

f7cafa616e787777bcf46e2ed76ad26742815665e0f905af93c63884053b36b7

b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

9012aa277720eab2d136fe23eb663468439c42a151e183988218222442d654d3

x34mMawEUcCG8l95riWCOK+kAJYejVmdt44l6tzcyUc=

08a4978ed338aad725827ec20872229c9b3ddb9fed1376aa5a8b22c0df91fd6f

aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7

560278d5a25db7e00c61daba7285dc9a34526c54ff03b8b94cad3013b06403d4

494c8a25532fe95ee6f4f57eb2a00ace364a55988a4b289393e52258a810909d

06cf23ccb9f82289c1c06ce8163cf68039ca33a77bf97e2f051f4b39b5313fb1

## POSSIBLE SECRETS

10ef865862d32bb9b7dc205e32504360f2da79a29ba020180e38c2c9efcf1944

ED2F9AF9-03A8-4C01-8A1D-5D9DC8720B67

205e460b479e2e5b48aec07710c08d50

811854d207e16d6a53da3b004e9a4e772562413301551ee190ace4ac8a17908d

5a9b80e3560e32d8bba67c9fae77a8b2f37149b4defc0715801cbf29dfcec217

fde635ef53540bddbcf106a0f5c4837c366f1742ed53bdadfd7d4d256a8df87c

141893a70aea67a2b13f1e04c6e11efee45c6e93a1e1c3d853d7fdfc0d9640ca

67a2ee790fa7cedb0b67a0264bc8982c5383a9214d52447aa33c8a742537bd00

7b4d24ebf576e3c7531ffbc316c1de717352b5e1ebc5823ba1ea7ad63d5335cb

9eb3453d2737feb0c868f7c27e461d5a8ab5212bd8f5e815cd1b9d2b094621fe

81d29626c39077b6bd1f85c14b890465d591341fa13ceff5e2a9edf8d701a029

80d48aa4b46362f0dca5e080734fa1641e4cca5961343204c541a95e376485a7

973f6963bcf96494c08914b98a9082c822de1f1ec7345abfaf8aff722a70f82f

893020632f019f34c099e04b1b14a253

376bb2eec4fce2967b6f819fea9e151d317442f47b9112b84cc049dee809ce95

## POSSIBLE SECRETS

cfb4fe79-4bae-43c1-9b1d-96ebf48ef840

72d93c96cc97af7840e1b99ed85b755d

24b381a16f4507a9b34f4caf80478d409472a19f86671b2bc7ad518eb6ece777

3c0ee8f7504942806ae8cf76460f9937

87f3bba2cd7d2f65c0bde63bc23ec623ae2142fc9879ff2a34e2e280037c8034

507c7b9c-ad50-4078-a67b-aa2069874d24

ada1732b940b5d9168b73546f21fc2f2b6814179e6f05a7fa8bf8a7562c400f7

e4fd4580ce8edb55741b54e4105904010bab2ffc51ddfb90970eea8be1ec88bc

6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151

f689cb84a265ebd2f01d04f147c14807f3740265fc36ff6c455005572633f3a6

854fe2036819ede5db6f364b7b902207c9a89a74f5005e1467e5ea4eb73568b2

4fbd39cb04b91cacb8ac595e18265ca283eb20b1bf061aec95e430a1c46ee793

3b8f1ea953503a969df80edcd77d6dfee3c0266305f43af749ff0f9cc0e6fb65

849f26e2-2df6-11e4-ab12-14109fdc48df

e881d739f2b849ab17d0ce784f1d75c6aa51f59415621e46ef399159e212c159

## POSSIBLE SECRETS

d19b36a24a11405568f13b70b80ee8de3bd97cd8ae2e443ee9e5c8d15d44e1fd

c48d90827d8c2e770b170c67843d649d4bddf1c9a802ce4fcf29f2493f48e053

e17be0b529289ce893def03144fbefc793ee27e2d8425753b9b28af3c9c4027d

5932b6a42943c6ea41c043ca736d77b0d37709c4a4c7102aeea7bb816a026c21

8d6bcafeac1afc339b929778f6b83ece0dcdfb8edfc97c1fadb9fce46710bf20

120dcb481786ceef3b960a3d9cd6cc41e92f8e50539ce8112578183f37ad0307

45150e3e79dd2eecbaf4ec07553d87e75cd46ab0943e333ea9a19cd01e552dc3

bd376388b5f723fb4c22dfe6cd4375a05a07476444d5819985007e34

f4e6c9f2-7ff2-4eb5-b510-c1eb94446f8b

f3300e4e-e586-4b55-94ec-14ad41818c69

bc5e64b3-5724-4b2b-a1ac-2c103bccc289

136b1479e7fb50c1f62b9e115dab282df7ecdce5e1d8ef941f53e770c13c4655

694a4d58ca15706fc471e957f0db71c2c24794cbe764745270397071e5bb0a43

7fc1bbfa687b5be8cff9b58dbee1bf0df7e6ed9b98de29efca3f3b21dff47009

2c93f24ccd2167a52141510cb74912c4eed7a9309db40f26539e71327ba9980d

## POSSIBLE SECRETS

a1b32a084c411800bb3a55e0ca85014b5633b522934c9b431dd5ffe7e6224302

9af816b40fa99dcf8e52756bc2a67de0eb6de091fa0c18ba204b94eeaf7f4471

b2cb3f9f7b1122bb5dc8246a020dd12813ddeaee9c2c0c08e71164ce5493a52c

888e7cb56985fb169dffcf598416520977ce5e6f452332989ead257d87e4fd21

5fe0c0f3fd6aca2650a712cf9878d7a5c9277650844eaf0099bd180bb6002bc2

2b2a9b4a3f5b282c5f1058148d83dde7127f28f1a5f9052d07afca5ee73551b0

5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

6f9d6ca93c493c782017d27b1d8a7ba6dea028793aaa27963622a0ea9b490843

googlePlacesToken=AIzaSyD0nnrWHsr3u9CnxByF0gbpfsYTIn2yuSA

aa572b07-50e3-4550-bef0-96155755497f

aaff7846806484d0ab1a1a5622c00696c26ff4536dd11a522ab1fb9a004d21c2

2107ff57c9e55bd30eedf524a92d4683f13a295cc9eff74a3c3d6112b3a67c01

ded84a95-950c-46a4-aa22-881ecec30671

d784ba0c2e12baebb5258b5c12ff27f353200ffda84650b5e43d795d460ab416

c54b07f20a861bffbd9b7ddc06f4fa25ddb116251bb30d555f7b21e7a8dc6025

## POSSIBLE SECRETS

a706641a389a96f2408c17d2369c438de31b5a4961a85bdf1122a5c39358c6b3

b3cef0c7cc9c6335aec52510aeb70c7cb34e111c5e7bed337cf7a504490ee509

bca9585213e4db495f15b424f5ef2fe27e7ad8c66df4da4d80fca97d12c439a3

5bea1e06757fcbbd6ee8ba37dfccbb4de7adb6b92f87b47669329e901430671d

23d9cbabab56da64e0e7c2dbae00a7a92481341904cd0ea8f3267b13ba420ef4

6592acf07aa34508c56d765983516cc5dc37eda54279711bf62dc68677da3c15

e4d9a72f88aef86b0d6e54aa38692d101d366d331d382926e9bb62cb1ddc2e3d

ab253b89-9ece-4a03-9b96-f1b16ed2d42f

feb6f1d7-5cd6-4580-80ce-02e4613c6dfd

86e309774c8b1a57308b415a73ba95e0f5c95bfffac40a1eb47d159e0d2dbdc2

6f4f06081a1fdfed3bcff8e82d2d4288b624f1f55697a4a55105c234679eef42

bf2ebc36f3d735101c49aaa2899ba1454805d3cee63d1a5e191941735c619f17

51953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00

6b1fad42aa655fe62a81272e459f44dede565b444fac91af9b651cfcd2a6ba1a

bcf9d4ad71c5cabd0d3d203b5be8a38f533110be0bd2f38e51c39a40f5fdde6c

## POSSIBLE SECRETS

82af5016bc4374c7bcf18eb64d1589b4005b9ebc57521e23b73772d3c4a1f732

22d6eff8e37cbcc124752193bc0af79bc6e82fa34fd6077164062b3793682237

a3b3d23dae6bc54af9157b0b4323efc11c5ab6ec4ce8a6f685ac7e19333d0594

20e24b41beb3f57f007dd439c0050e6043761993e8838b67df68cf0fc355a432

dab1b1eacb3aea4acd8f69517f7d3c80dacc7ee658d52ed000d45948425c7035

b-1e7b1978-c634-4968-8cd4-e092004d4c6c

4048c68178e7efa164cf212f87e066733e1a58efe0740c0f7b25972e150da55b

AIzaSyD0nnrWHsr3u9CnxByF0gbpfsYTIn2yuSA

e6bca3d256be4087b0aa3248d487b806c4eb89978f05700d3d77674a5286c6c6

6bbc3921bfdcd14eb837269760fb9c3b6ac25444ad952b9c7188681bf0aeb9aa

f8f8b12d2c57f19b4897262fb35f5c17d714035e3c4ffcbf2916219c7e721be7

b5d7f4fa79b053dac61df1d18da04a42b4de8e1266c0a18d53c44a452c76eb45

77786545b9bcaac8c0e8856faa137a238da181a197df391fca3c113e3e77b3c3

dc28f0f1eb5bb7115a33821427a3d70931fc5948388b68667bfab0a0cdccd195

# ▶ PLAYSTORE INFORMATION

**Title:** Doctor On Demand

**Score:** 4.7537827 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support: Category:** Medical **Play Store URL:** [com.doctorondemand.android.patient](com.doctorondemand.android.patient)

**Developer Details:** Doctor On Demand, Inc, Doctor+On+Demand,+Inc, None, http://www.doctorondemand.com/contact, support@doctorondemand.com,

**Release Date:** Oct 7, 2013 **Privacy Policy:** [Privacy link](Privacy link)

**Description:**

Doctor On Demand by Included Health offers 24/7 access to board-certified doctors, licensed therapists, and psychiatrists via secure video visits from your phone, tablet, or computer. When you're feeling sick, want a doctor's note, need help with a prescription, and more, we make it easy to get quality telehealth anytime, anywhere—with or without insurance. Download the free Doctor On Demand app to get started. Why Choose Doctor On Demand? Fast Access to Online Doctors – See a board-certified, US-based provider with telehealth appointments anytime, day or night. Therapy & Psychiatry – Book virtual visits for mental health concerns like stress, anxiety, depression, PTSD, trauma, and more. Online Urgent Care, Treatment, Prescriptions – For colds, flu, allergies, skin conditions, UTIs, headaches, and more, our providers can send prescriptions to nearby pharmacies if medically appropriate. Doctor's Notes – Need a doctor's note for work or school? We've got you covered. See an urgent care provider for help. Insurance or Self-Pay – We work with major health plans and many employers to reduce the costs of visits for eligible members. If not covered, we offer affordable visit costs to all patients with no surprise bills. How It Works    1. Download the app and create an account for free.    2. Choose to see the first available provider, or schedule a visit.    3. Get personalized care, prescriptions, and treatment plans in an online visit. Conditions We Treat ✔ Cold, Flu & Sinus Infections ✔ UTI Treatment Online ✔ Acne, Rashes & Skin Issues ✔ Allergies & Asthma ✔ High Cholesterol, Diabetes & Thyroid Screening ✔ Headaches & Migraines ✔ Mental Health Support: Anxiety, Depression, Grief & More ✔ Prescription Refills & Lab Orders Frequently Asked Questions 🕐 When are doctors available? Our virtual providers are available 24/7, 365 days a year, including weekends and holidays. Mental health appointments are often available within days—much faster than traditional providers who can take weeks 💲 How much does a visit cost? You'll always see your exact visit cost upfront. We accept most insurance plans and partner with top employers and health plans to lower your costs. No insurance? Our telehealth visit costs are affordable. ⚕ Who are the doctors? Our US-based, board-certified doctors, licensed psychiatrists, and therapists have an average of 15 years of experience and come from diverse specialties to ensure you receive expert care. 📱How does it work? Join a telehealth visit to connect face to face with a provider from your phone, tablet, or computer in as little as ten minutes. Like an in-person visit, your provider will discuss with you how you're feeling, your healthcare history, and propose a recommended treatment plan. Labs, screenings, and prescriptions will be sent to nearby facilities. ⚕What can you treat? Our urgent care doctors can treat hundreds of issues, including cold and flu, urinary tract infections, allergies, headache, sprains, and skin conditions. They can also order labs and screenings to help with preventative care and help manage chronic care conditions. Our extensive team of therapists and psychiatrists are able to treat anxiety, stress, depression, PTSD, trauma and loss relationships, and more. Your Privacy is Our Priority We adhere to strict HIPAA guidelines to protect your health data and personal information. Our providers are unable to prescribe controlled substances. Get Started Today Join millions of patients who trust Doctor On Demand for fast, convenient, and reliable healthcare. Download the app now to sign up for free!

## ≡ SCAN LOGS

| Timestamp | Event | Error |
|---|---|---|

| | | |
|---|---|---|
| 2025-08-29 21:43:23 | Generating Hashes | OK |
| 2025-08-29 21:43:24 | Extracting APK | OK |
| 2025-08-29 21:43:24 | Unzipping | OK |
| 2025-08-29 21:43:24 | Parsing APK with androguard | OK |
| 2025-08-29 21:43:25 | Extracting APK features using aapt/aapt2 | OK |
| 2025-08-29 21:43:25 | Getting Hardcoded Certificates/Keystores | OK |
| 2025-08-29 21:43:29 | Parsing AndroidManifest.xml | OK |
| 2025-08-29 21:43:29 | Extracting Manifest Data | OK |
| 2025-08-29 21:43:29 | Manifest Analysis Started | OK |
| 2025-08-29 21:43:29 | Reading Network Security config from network_security_config.xml | OK |
| 2025-08-29 21:43:29 | Parsing Network Security config | OK |

| | | |
|---|---|---|
| 2025-08-29 21:43:29 | Performing Static Analysis on: Doctor On Demand (com.doctorondemand.android.patient) | OK |
| 2025-08-29 21:43:30 | Fetching Details from Play Store: com.doctorondemand.android.patient | OK |
| 2025-08-29 21:43:30 | Checking for Malware Permissions | OK |
| 2025-08-29 21:43:30 | Fetching icon path | OK |
| 2025-08-29 21:43:30 | Library Binary Analysis Started | OK |
| 2025-08-29 21:43:30 | Reading Code Signing Certificate | OK |
| 2025-08-29 21:43:31 | Running APKiD 2.1.5 | OK |
| 2025-08-29 21:43:38 | Detecting Trackers | OK |
| 2025-08-29 21:43:45 | Decompiling APK to Java with JADX | OK |
| 2025-08-29 21:44:16 | Converting DEX to Smali | OK |
| 2025-08-29 21:44:16 | Code Analysis Started on - java_source | OK |

| 2025-08-29 21:44:26 | Android SBOM Analysis Completed | OK |
|---|---|---|
| 2025-08-29 21:44:49 | Android SAST Completed | OK |
| 2025-08-29 21:44:49 | Android API Analysis Started | OK |
| 2025-08-29 21:45:09 | Android API Analysis Completed | OK |
| 2025-08-29 21:45:10 | Android Permission Mapping Started | OK |
| 2025-08-29 21:45:53 | Android Permission Mapping Completed | OK |
| 2025-08-29 21:45:54 | Android Behaviour Analysis Started | OK |
| 2025-08-29 21:46:21 | Android Behaviour Analysis Completed | OK |
| 2025-08-29 21:46:21 | Extracting Emails and URLs from Source Code | OK |
| 2025-08-29 21:46:35 | Email and URL Extraction Completed | OK |
| 2025-08-29 21:46:35 | Extracting String data from APK | OK |

| 2025-08-29 21:46:35 | Extracting String data from Code | OK |
| --- | --- | --- |
| 2025-08-29 21:46:35 | Extracting String values and entropies from Code | OK |
| 2025-08-29 21:46:44 | Performing Malware check on extracted domains | OK |
| 2025-08-29 21:46:52 | Saving to Database | OK |

## Report Generated by - MobSF v4.4.0

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