ANDROID STATIC ANALYSIS REPORT

app_icon

🤖 Hello Heart (5.0.25)

File Name:	com.helloheart.app.healthplan_50003600.apk
Package Name:	com.helloheart.app.healthplan
Scan Date:	Aug. 30, 2025, 8:55 p.m.
App Security Score:	41/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	5/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	19	5	0	1

FILE INFORMATION

File Name: com.helloheart.app.healthplan_50003600.apk
Size: 87.24MB
MD5: f36a5270c78fd4ecd24fd89e891c0995
SHA1: 903fbb742e2baa8b9e39e48295725baba0b5af8f
SHA256: fa1aa23e35e9e0614203ade709d27005da85b9bf456ce9327d474d3ffc618aec

APP INFORMATION

App Name: Hello Heart
Package Name: com.helloheart.app.healthplan
Main Activity: com.helloheart.app.healthplan.MainActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 5.0.25

Android Version Code: 50003600

▦ APP COMPONENTS

Activities: 10
Services: 17
Receivers: 20
Providers: 13
Exported Activities: 1
Exported Services: 2
Exported Receivers: 5
Exported Providers: 0

✿ CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=IL, ST=Israel, L=Tel Aviv, O=Hello Doctor Ltd., OU=Hello Doctor Ltd., CN=*.hello.do
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-07-12 18:44:21+00:00
Valid To: 2040-07-05 18:44:21+00:00
Issuer: C=IL, ST=Israel, L=Tel Aviv, O=Hello Doctor Ltd., OU=Hello Doctor Ltd., CN=*.hello.do
Serial Number: 0x6990ca30
Hash Algorithm: sha256
md5: c925b269efce5d452a8c5c5a38e82e00
sha1: 5cf8146ee5d9d7c59c603f7bf3b8ba19bab648fc
sha256: 146649911293afc9a00beb4638c5eb3fb2f1a5f3b023fd24e55a84d4e2167b2c
sha512: 603bb767b7611e95d80a068a605ed50e3e0ab807818748b390019ef9738262f2dde021b48f12a49e89fa2279bd4734e64bd3888863514127eb7ebbae29d92877
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 7eb3e816b00b32b8152444c0c47fa01e60c69979833735e186a02d778c507539
Found 1 unique certificates

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.helloheart.app.healthplan.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.fingerprints.service.ACCESS_FINGERPRINT_MANAGER	unknown	Unknown permission	Unknown permission from android reference
com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY	unknown	Unknown permission	Unknown permission from android reference
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
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.BLUETOOTH_ADVERTISE	dangerous	required to advertise to nearby Bluetooth devices.	Required to be able to advertise to nearby Bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

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.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.
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.oppo.launcher.permission.WRITE_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.BROADCAST_CLOSE_SYSTEM_DIALOGS	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NOTIFICATION_POLICY	normal	marker permission for accessing notification policy.	Marker permission for applications that wish to access notification policy.

🔍 APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
f36a5270c78fd4ecd24fd89e891c0995.apk	**FINDINGS** / **DETAILS** Anti-VM Code — possible VM check
classes.dex	**FINDINGS** / **DETAILS** Anti-VM Code — Build.FINGERPRINT check Build.MANUFACTURER check possible Build.SERIAL check possible VM check Compiler — r8 without marker (suspicious)

FILE	DETAILS
classes2.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check network operator name check possible VM check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

FILE	DETAILS
classes3.dex	<table><tr><td>FINDINGS</td><td>DETAILS</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check possible Build.SERIAL check Build.TAGS check possible VM check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>
classes4.dex	<table><tr><td>FINDINGS</td><td>DETAILS</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

FILE	DETAILS
classes5.dex	<table><tr><td>**FINDINGS**</td><td>**DETAILS**</td></tr><tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

🗔 BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.helloheart.app.healthplan.MainActivity	Schemes: mailto://, branchandroid://, helloheart://, https://, Hosts: get.helloheart.com, Mime Types: */*,

🔒 NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

🪪 CERTIFICATE ANALYSIS

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

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

🔍 MANIFEST ANALYSIS

HIGH: **1** | WARNING: **9** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
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	Broadcast Receiver (com.dieam.reactnativepushnotification.modules.RNPushNotificationBootEventReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Broadcast Receiver (io.invertase.firebase.messaging.ReactNativeFirebaseMessagingReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
5	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
7	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
8	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
9	Activity (app.notifee.core.NotificationReceiverActivity) 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.
10	Broadcast Receiver (app.notifee.core.AlarmPermissionBroadcastReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

</> CODE ANALYSIS

HIGH: **2** | WARNING: **8** | INFO: **4** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				android/print/PdfConverter.java app/notifee/core/AlarmPermissionBroadcastReceiver.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				app/notifee/core/Logger.java app/notifee/core/RebootBroadcastReceiver.java
				app/notifee/core/b.java cl/json/RNShareImpl.java cl/json/RNSharePathUtil.java cl/json/social/InstagramShare.java cl/json/social/SingleShareIntent.java com/airbnb/android/react/lottie/LottieAnimationViewManager.java com/airbnb/android/react/maps/AirMapGradientPolyline.java com/airbnb/android/react/maps/AirMapHeatmap.java com/airbnb/android/react/maps/AirMapTileProvider.java com/airbnb/android/react/maps/AirMapTileWorker.java com/airbnb/android/react/maps/AirMapUrlTile.java com/airbnb/android/react/maps/FileUtil.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java com/bleplx/BlePlxModule.java com/bleplx/adapter/BleModule.java com/bleplx/adapter/Characteristic.java com/bleplx/adapter/Descriptor.java com/bleplx/adapter/utils/RefreshGattCustomOperation.java com/brentvatne/react/ReactVideoView.java com/datadog/android/core/internal/data/upload/CurlInterceptor.java com/datadog/android/ndk/internal/NdkCrashLog.java com/datadog/android/rum/DdRumContentProvider.java com/datadog/android/rum/internal/domain/scope/RumViewScope.java com/datadog/legacy/trace/api/DDTraceApiInfo.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/datadog/opentracing/DDTraceOTInfo.jav a com/datadog/reactnative/DatadogSDKWrappe rStorage.java com/datadog/reactnative/DdRumImplementat ion.java com/datadog/reactnative/DdSdkBridgeExtKt.ja va com/datadog/reactnative/DdSdkConfiguration ExtKt.java com/datadog/reactnative/DdSdkImplementati on.java com/datadog/reactnative/DdSdkNativeInitializ ation.java com/datadog/reactnative/ProxyAuthenticator.j ava com/datadog/trace/core/DDTraceCoreInfo.jav a com/dieam/reactnativepushnotification/helpe rs/ApplicationBadgeHelper.java com/dieam/reactnativepushnotification/modu les/RNPushNotification.java com/dieam/reactnativepushnotification/modu les/RNPushNotificationActions.java com/dieam/reactnativepushnotification/modu les/RNPushNotificationAttributes.java com/dieam/reactnativepushnotification/modu les/RNPushNotificationBootEventReceiver.java com/dieam/reactnativepushnotification/modu les/RNPushNotificationConfig.java com/dieam/reactnativepushnotification/modu les/RNPushNotificationHelper.java com/dieam/reactnativepushnotification/modu les/RNPushNotificationListenerService.java com/dieam/reactnativepushnotification/modu les/RNPushNotificationPicturesAggregator.java com/dieam/reactnativepushnotification/modu les/RNPushNotificationPublisher.java com/dieam/reactnativepushnotification/modu les/RNReceivedMessageHandler.java com/fingerprints/service/FingerprintManager.j

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ava com/github/barteksc/pdfviewer/PDFView.java com/github/mikephil/charting/charts/BarChart.java com/github/mikephil/charting/charts/BarLineChartBase.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/charts/CombinedChart.java com/github/mikephil/charting/charts/HorizontalBarChart.java com/github/mikephil/charting/charts/PieRadarChartBase.java com/github/mikephil/charting/components/AxisBase.java com/github/mikephil/charting/data/ChartData.java com/github/mikephil/charting/data/CombinedData.java com/github/mikephil/charting/data/LineDataSet.java com/github/mikephil/charting/data/PieEntry.java com/github/mikephil/charting/listener/BarLineChartTouchListener.java com/github/mikephil/charting/renderer/CombinedChartRenderer.java com/github/mikephil/charting/renderer/ScatterChartRenderer.java com/github/mikephil/charting/utils/FileUtils.java com/github/mikephil/charting/utils/Utils.java com/heanoria/library/reactnative/locationenabler/RNAndroidLocationEnablerModule.java com/horcrux/svg/Brush.java com/horcrux/svg/ClipPathView.java com/horcrux/svg/FilterView.java com/horcrux/svg/ImageView.java com/horcrux/svg/LinearGradientView.java com/horcrux/svg/PatternView.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/horcrux/svg/RadialGradientView.java com/horcrux/svg/UseView.java com/horcrux/svg/VirtualView.java com/ibits/react_native_in_app_review/AppReviewModule.java com/iterable/iterableapi/IterableActionRunner.java com/iterable/iterableapi/IterableLogger.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/RNInstallReferrerClient.java com/learnium/RNDeviceInfo/resolver/DeviceIdResolver.java com/logrocket/core/ApplicationInitProvider.java com/logrocket/core/CrashReportFactory.java com/logrocket/core/CustomEvent.java com/logrocket/core/CustomEventBuilder.java com/logrocket/core/LogRocketCore.java com/logrocket/core/PostAcceptanceTasks.java com/logrocket/core/PostInitializationTasks.java com/logrocket/core/SDK.java com/logrocket/core/util/logging/AndroidLogger.java com/lugg/ReactNativeConfig/ReactNativeConfigModule.java com/masteratul/exceptionhandler/DefaultErrorScreen.java com/mixpanel/android/mpmetrics/AnalyticsMessages.java com/mixpanel/android/mpmetrics/ConfigurationChecker.java com/mixpanel/android/mpmetrics/MPConfig.java com/mixpanel/android/mpmetrics/MPDbAdapter.java com/mixpanel/android/mpmetrics/MixpanelAPI.java com/mixpanel/android/mpmetrics/PersistentI

NO	ISSUE	SEVERITY	STANDARDS	FILES
				dentity.java
				com/mixpanel/android/mpmetrics/ResourceReader.java
				com/mixpanel/android/mpmetrics/SessionMetadata.java
				com/mixpanel/android/mpmetrics/SystemInformation.java
				com/mixpanel/android/util/HttpService.java
				com/mixpanel/android/util/MPLog.java
				com/oblador/keychain/KeychainModule.java
				com/oblador/keychain/cipherStorage/CipherStorageBase.java
				com/oblador/keychain/cipherStorage/CipherStorageFacebookConceal.java
				com/oblador/keychain/cipherStorage/CipherStorageKeystoreAesCbc.java
				com/oblador/keychain/cipherStorage/CipherStorageKeystoreRsaEcb.java
				com/oblador/keychain/decryptionHandler/DecryptionResultHandlerInteractiveBiometric.java
				com/oblador/keychain/decryptionHandler/DecryptionResultHandlerInteractiveBiometricManualRetry.java
				com/polidea/rxandroidble2/ClientComponent.java
				com/polidea/rxandroidble2/RxBleAdapterStateObservable.java
				com/polidea/rxandroidble2/RxBleClient.java
				com/polidea/rxandroidble2/RxBleClientImpl.java
				com/polidea/rxandroidble2/helpers/ValueInterpreter.java
				com/polidea/rxandroidble2/internal/QueueOperation.java
				com/polidea/rxandroidble2/internal/connection/DisconnectionRouter.java
				com/polidea/rxandroidble2/internal/connection/LoggingIllegalOperationHandler.java
				com/polidea/rxandroidble2/internal/logger/LoggerUtil.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				~~ogger~~Util.java com/polidea/rxandroidble2/internal/logger/LoggerUtilBluetoothServices.java com/polidea/rxandroidble2/internal/operations/CharacteristicLongWriteOperation.java com/polidea/rxandroidble2/internal/operations/DisconnectOperation.java com/polidea/rxandroidble2/internal/operations/LegacyScanOperation.java com/polidea/rxandroidble2/internal/operations/ScanOperation.java com/polidea/rxandroidble2/internal/operations/ScanOperationApi18.java com/polidea/rxandroidble2/internal/operations/ScanOperationApi21.java com/polidea/rxandroidble2/internal/scan/BackgroundScannerImpl.java com/polidea/rxandroidble2/internal/scan/InternalScanResultCreator.java com/polidea/rxandroidble2/internal/scan/ScanSettingsEmulator.java com/polidea/rxandroidble2/internal/scan/ScanSetupBuilderImplApi23.java com/polidea/rxandroidble2/internal/serialization/ClientOperationQueueImpl.java com/polidea/rxandroidble2/internal/serialization/ConnectionOperationQueueImpl.java com/polidea/rxandroidble2/internal/serialization/QueueSemaphore.java com/polidea/rxandroidble2/internal/util/BleConnectionCompat.java com/polidea/rxandroidble2/internal/util/CharacteristicPropertiesParser.java com/polidea/rxandroidble2/internal/util/CheckerLocationProvider.java com/polidea/rxandroidble2/internal/util/RxBleAdapterWrapper.java com/polidea/rxandroidble2/internal/util/ScanRecordParser.java com/reactnative/googlefit/ActivityHistory.java com/reactnative/googlefit/BloodPressureHistory.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	[The App logs information. Sensitive information should never be logged.](#)	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	ry.java com/reactnative/googlefit/CalorieHistory.java com/reactnative/googlefit/DistanceHistory.jav a com/reactnative/googlefit/GoogleFitManager.j ava com/reactnative/googlefit/GoogleFitModule.ja va com/reactnative/googlefit/NutritionHistory.jav a com/reactnative/googlefit/RecordingApi.java com/reactnative/googlefit/StepCounter.java com/reactnative/googlefit/StepHistory.java com/reactnative/googlefit/StepSensor.java com/reactnativecommunity/asyncstorage/Asy ncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/Asy ncStorageExpoMigration.java com/reactnativecommunity/asyncstorage/Asy ncStorageModule.java com/reactnativecommunity/asyncstorage/Rea ctDatabaseSupplier.java com/reactnativecommunity/geolocation/Geol ocationModule.java com/reactnativecommunity/webview/RNCWe bView.java com/reactnativecommunity/webview/RNCWe bViewClient.java com/reactnativecommunity/webview/RNCWe bViewManagerImpl.java com/rssignaturecapture/RSSignatureCaptureM ainView.java com/rssignaturecapture/RSSignatureCaptureVi ewManager.java com/rt2zz/reactnativecontacts/ContactsProvid er.java com/samsung/android/sdk/pass/Spass.java com/samsung/android/sdk/pass/SpassFinger print.java com/samsung/android/sdk/pass/d.java com/samsung/android/sdk/pass/support/Sdk Supporter.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				Supporter.java com/samsung/android/sdk/pass/support/v1/ FingerprintManagerProxyFactory.java
				com/shockwave/pdfium/PdfiumCore.java com/swmansion/gesturehandler/react/RNGes tureHandlerRootHelper.java com/swmansion/gesturehandler/react/RNGes tureHandlerRootView.java com/swmansion/reanimated/NativeMethods Helper.java com/swmansion/reanimated/ReanimatedMod ule.java com/swmansion/reanimated/ReanimatedUIM anagerFactory.java com/swmansion/reanimated/layoutReanimati on/AnimationsManager.java com/swmansion/reanimated/layoutReanimati on/ReanimatedNativeHierarchyManager.java com/swmansion/reanimated/layoutReanimati on/SharedTransitionManager.java com/swmansion/reanimated/nativeProxy/Nat iveProxyCommon.java com/swmansion/reanimated/sensor/Reanima tedSensorContainer.java com/swmansion/rnscreens/ScreenStackHeade rConfigViewManager.java com/th3rdwave/safeareacontext/SafeAreaVie w.java com/tom_roush/fontbox/afm/AFMParser.java com/tom_roush/fontbox/cff/Type1CharString. java com/tom_roush/fontbox/cff/Type1CharString Parser.java com/tom_roush/fontbox/ttf/CmapSubtable.ja va com/tom_roush/fontbox/ttf/GlyfCompositeDe script.java com/tom_roush/fontbox/ttf/KerningSubtable.j ava com/tom_roush/fontbox/ttf/KerningTable.java com/tom_roush/fontbox/type1/Type1Lexer.ja

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/tom_roush/pdfbox/contentstream/PDFStreamEngine.java
				com/tom_roush/pdfbox/contentstream/operator/graphics/ClosePath.java
				com/tom_roush/pdfbox/contentstream/operator/graphics/CurveTo.java
				com/tom_roush/pdfbox/contentstream/operator/graphics/CurveToReplicateInitialPoint.java
				com/tom_roush/pdfbox/contentstream/operator/graphics/LineTo.java
				com/tom_roush/pdfbox/contentstream/operator/text/MoveText.java
				com/tom_roush/pdfbox/cos/COSDocument.java
				com/tom_roush/pdfbox/cos/COSString.java
				com/tom_roush/pdfbox/filter/ASCIIHexFilter.java
				com/tom_roush/pdfbox/filter/CCITTFaxFilter.java
				com/tom_roush/pdfbox/filter/DCTFilter.java
				com/tom_roush/pdfbox/filter/Filter.java
				com/tom_roush/pdfbox/filter/FlateFilter.java
				com/tom_roush/pdfbox/filter/LZWFilter.java
				com/tom_roush/pdfbox/filter/RunLengthDecodeFilter.java
				com/tom_roush/pdfbox/io/ScratchFile.java
				com/tom_roush/pdfbox/pdfparser/BaseParser.java
				com/tom_roush/pdfbox/pdfparser/COSParser.java
				com/tom_roush/pdfbox/pdfparser/FDFParser.java
				com/tom_roush/pdfbox/pdfparser/PDFObjectStreamParser.java
				com/tom_roush/pdfbox/pdfparser/PDFParser.java
				com/tom_roush/pdfbox/pdfparser/PDFStreamParser.java
				com/tom_roush/pdfbox/pdfparser/XrefTrailerResolver.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/tom_roush/pdfbox/pdfwriter/COSWriter.java com/tom_roush/pdfbox/pdmodel/PDDocument.java com/tom_roush/pdfbox/pdmodel/PDPage.java com/tom_roush/pdfbox/pdmodel/PDPageContentStream.java com/tom_roush/pdfbox/pdmodel/common/PDNameTreeNode.java com/tom_roush/pdfbox/pdmodel/common/PDNumberTreeNode.java com/tom_roush/pdfbox/pdmodel/documentinterchange/logicalstructure/PDStructureTreeRoot.java com/tom_roush/pdfbox/pdmodel/documentinterchange/taggedpdf/StandardStructureTypes.java com/tom_roush/pdfbox/pdmodel/encryption/SecurityHandler.java com/tom_roush/pdfbox/pdmodel/encryption/StandardSecurityHandler.java com/tom_roush/pdfbox/pdmodel/fdf/FDFAnnotation.java com/tom_roush/pdfbox/pdmodel/fdf/FDFAnnotationInk.java com/tom_roush/pdfbox/pdmodel/fdf/FDFAnnotationPolygon.java com/tom_roush/pdfbox/pdmodel/fdf/FDFAnnotationPolyline.java com/tom_roush/pdfbox/pdmodel/fdf/FDFDictionary.java com/tom_roush/pdfbox/pdmodel/font/FileSystemFontProvider.java com/tom_roush/pdfbox/pdmodel/font/FontMapper.java com/tom_roush/pdfbox/pdmodel/font/PDCIDFontType0.java com/tom_roush/pdfbox/pdmodel/font/PDCIDFontType2.java com/tom_roush/pdfbox/pdmodel/font/PDFon

NO	ISSUE	SEVERITY	STANDARDS	FILES
				t.java com/tom_roush/pdfbox/pdmodel/font/PDFontFactory.java
				com/tom_roush/pdfbox/pdmodel/font/PDSimpleFont.java
				com/tom_roush/pdfbox/pdmodel/font/PDTrueTypeFont.java
				com/tom_roush/pdfbox/pdmodel/font/PDType0Font.java
				com/tom_roush/pdfbox/pdmodel/font/PDType1CFont.java
				com/tom_roush/pdfbox/pdmodel/font/PDType1Font.java
				com/tom_roush/pdfbox/pdmodel/font/PDType3Font.java
				com/tom_roush/pdfbox/pdmodel/font/encoding/GlyphList.java
				com/tom_roush/pdfbox/pdmodel/graphics/color/PDColorSpace.java
				com/tom_roush/pdfbox/pdmodel/graphics/color/PDDeviceGray.java
				com/tom_roush/pdfbox/pdmodel/graphics/color/PDDeviceRGB.java
				com/tom_roush/pdfbox/pdmodel/graphics/image/PDImageXObject.java
				com/tom_roush/pdfbox/pdmodel/graphics/image/SampledImageReader.java
				com/tom_roush/pdfbox/pdmodel/graphics/predictor/PredictorAlgorithm.java
				com/tom_roush/pdfbox/pdmodel/graphics/state/PDSoftMask.java
				com/tom_roush/pdfbox/pdmodel/interactive/annotation/PDAnnotation.java
				com/tom_roush/pdfbox/pdmodel/interactive/digitalsignature/visible/PDFTemplateCreator.java
				com/tom_roush/pdfbox/pdmodel/interactive/digitalsignature/visible/PDVisibleSigBuilder.java
				com/tom_roush/pdfbox/rendering/CIDType0Glyph2D.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/tom_roush/pdfbox/rendering/TTFGlyph2D.java com/tom_roush/pdfbox/rendering/Type1Glyph2D.java com/tom_roush/pdfbox/text/PDFTextStreamEngine.java com/tom_roush/pdfbox/text/TextPosition.java com/tom_roush/pdfbox/util/PDFBoxResourceLoader.java com/tom_roush/pdfbox/util/PDFHighlighter.java com/vonovak/AddCalendarEventModule.java com/zmxv/RNSound/RNSoundModule.java eightbitlab/com/blurview/BlurView.java io/branch/referral/BranchJsonConfig.java io/branch/referral/BranchLogger.java io/branch/referral/validators/IntegrationValidator.java io/branch/rnbranch/RNBranchModule.java io/invertase/firebase/app/ReactNativeFirebaseApp.java io/invertase/firebase/common/RCTConvertFirebase.java io/invertase/firebase/common/ReactNativeFirebaseEventEmitter.java io/invertase/firebase/common/SharedUtils.java io/invertase/firebase/crashlytics/ReactNativeFirebaseCrashlyticsInitProvider.java io/invertase/firebase/crashlytics/ReactNativeFirebaseCrashlyticsModule.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingModule.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingReceiver.java io/invertase/firebase/storage/ReactNativeFirebaseStorageDownloadTask.java io/invertase/firebase/storage/ReactNativeFirebaseStorageTask.java io/invertase/firebase/storage/ReactNativeFirebaseStorageUploadTask.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/invertase/firebase/utils/ReactNativeFirebasePllESModule.java io/invertase/notifee/NotifeeReactUtils.java
				me/leolin/shortcutbadger/ShortcutBadger.java org/greenrobot/eventbus/Logger.java org/jctools/maps/ConcurrentAutoTable.java org/jctools/maps/NonBlockingHashMap.java org/jctools/maps/NonBlockingHashMapLong.java org/jctools/maps/NonBlockingIdentityHashMap.java org/jctools/maps/NonBlockingSetInt.java org/koin/android/logger/AndroidLogger.java timber/log/Timber.java
				com/datadog/android/api/net/RequestFactory.java com/datadog/android/core/internal/metrics/BatchMetricsDispatcher.java com/datadog/android/log/internal/LogsFeature.java com/datadog/android/rum/internal/FeaturesContextResolver.java com/datadog/android/rum/internal/domain/event/RumEventMeta.java com/datadog/android/rum/internal/domain/scope/ExternalResourceTimingsKt.java com/datadog/android/rum/internal/domain/scope/RumRawEvent.java com/datadog/android/rum/internal/domain/scope/RumSessionScope.java com/datadog/android/rum/internal/domain/scope/RumViewInfo.java com/datadog/android/rum/internal/metric/SessionEndedMetric.java com/datadog/android/telemetry/internal/TelemetryEventHandler.java com/datadog/android/trace/internal/FeatureSdkCoreExtKt.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/datadog/android/trace/internal/TracingF eature.java
				com/datadog/android/trace/internal/domain/ event/CoreTracerSpanToSpanEventMapper.jav a
				com/datadog/android/trace/internal/domain/ event/MetaKeysKt.java
				com/datadog/android/webview/WebViewTrac king.java
				com/datadog/android/webview/internal/Mixe dWebViewEventConsumer.java
				com/datadog/android/webview/internal/repla y/WebViewReplayEventConsumer.java
				com/datadog/android/webview/internal/repla y/WebViewReplayEventMapper.java
				com/datadog/android/webview/internal/rum/ domain/WebViewNativeRumViewsCache.java
				com/datadog/legacy/trace/api/Config.java
				com/datadog/legacy/trace/common/sampling /RateByServiceSampler.java
				com/datadog/opentracing/DDSpanContext.jav a
				com/datadog/opentracing/propagation/B3Htt pCodec.java
				com/datadog/opentracing/propagation/B3MH ttpCodec.java
				com/datadog/opentracing/propagation/Datad ogHttpCodec.java
				com/datadog/opentracing/propagation/Hayst ackHttpCodec.java
				com/datadog/opentracing/propagation/W3CH ttpCodec.java
				com/datadog/reactnative/JSONProxyConfigur ation.java
				com/datadog/trace/api/Config.java
				com/datadog/trace/api/ConfigDefaults.java
				com/datadog/trace/api/ConfigSetting.java
				com/datadog/trace/api/DDTags.java
				com/datadog/trace/api/config/CrashTrackingC onfig.java
	Files may contain hardcoded		CWE: CWE-312: Cleartext Storage of Sensitive Information	

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	sensitive information like usernames, passwords, keys etc.	warning	Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/datadog/trace/api/config/GeneralConfig.java com/datadog/trace/api/config/ProfilingConfig.java com/datadog/trace/api/config/RemoteConfigConfig.java com/datadog/trace/bootstrap/instrumentation/api/InstrumentationTags.java com/datadog/trace/bootstrap/instrumentation/api/PathwayContext.java com/datadog/trace/common/sampling/SpanSamplingRules.java com/datadog/trace/common/sampling/TraceSamplingRules.java com/datadog/trace/core/DDSpanContext.java com/datadog/trace/core/propagation/B3HttpCodec.java com/datadog/trace/core/propagation/DatadogHttpCodec.java com/datadog/trace/core/propagation/HaystackHttpCodec.java com/datadog/trace/core/propagation/HttpCodec.java com/datadog/trace/core/propagation/W3CHttpCodec.java com/datadog/trace/core/propagation/XRayHttpCodec.java com/datadog/trace/core/propagation/ptags/PTagsFactory.java com/datadog/trace/core/propagation/ptags/W3CPTagsCodec.java com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java com/heanoria/library/reactnative/locationenabler/RNAndroidLocationEnablerModule.java com/helloheart/app/healthplan/BuildConfig.java com/helloheart/app/healthplan/IterableEventsModule.java com/iterable/iterableapi/IterableConstants.jav

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a ru/zolador/keychain/KeychainModule.java com/tom_roush/pdfbox/pdmodel/interactive/ annotation/PDAnnotationRubberStamp.java com/tom_roush/pdfbox/pdmodel/interactive/ annotation/PDAnnotationText.java io/branch/referral/Branch.java io/branch/referral/BranchPreinstall.java io/branch/referral/PrefHelper.java io/branch/referral/ServerRequest.java io/branch/referral/ServerRequestQueue.java io/branch/referral/UniversalResourceAnalyser. java io/branch/referral/validators/DeepLinkRoutin gValidator.java io/invertase/firebase/common/TaskExecutorS ervice.java io/invertase/firebase/messaging/ReactNativeFi rebaseMessagingHeadlessService.java io/invertase/firebase/messaging/ReactNativeFi rebaseMessagingSerializer.java io/invertase/notifee/NotifeeEventSubscriber.ja va io/reactivex/internal/schedulers/SchedulerPoo lFactory.java org/jctools/maps/NonBlockingHashMap.java org/jctools/maps/NonBlockingIdentityHashMa p.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/RNFetchBlob/RNFetchBlobFS.java com/RNFetchBlob/Utils/PathResolver.java com/christopherdro/htmltopdf/RNHTMLtoPDFModule.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/utils/FileUtils.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnativecommunity/webview/RNCWebViewModuleImpl.java com/rssignaturecapture/RSSignatureCaptureMainView.java io/invertase/firebase/storage/ReactNativeFirebaseStorageCommon.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java
4	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/RNFetchBlob/RNFetchBlobBody.java com/airbnb/android/react/maps/AirMapModule.java com/airbnb/android/react/maps/FileUtil.java com/christopherdro/htmltopdf/RNHTMLtoPDFModule.java com/iterable/iterableapi/ui/BitmapLoader.java com/reactnativecommunity/webview/RNCWebViewModuleImpl.java com/rumax/reactnative/pdfviewer/PDFView.java com/tom_roush/pdfbox/io/RandomAccessBufferedFileInputStream.java com/tom_roush/pdfbox/io/ScratchFile.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/tom_roush/pdfbox/pdmodel/encryption/SecurityHandler.java
6	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/datadog/android/trace/AndroidTracer.java com/datadog/opentracing/DDTracer.java com/datadog/opentracing/StringCachingBigInteger.java com/tom_roush/pdfbox/pdmodel/graphics/predictor/PredictorAlgorithm.java
7	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/iterable/iterableapi/IterableDatabaseManager.java com/iterable/iterableapi/IterableTaskStorage.java com/mixpanel/android/mpmetrics/MPDbAdapter.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java
8	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	ai/forethought/view/webview/SolveWebView.java
9	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	com/reactnativecommunity/clipboard/ClipboardModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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/reactnativecommunity/clipboard/ClipboardModule.java io/branch/referral/ShareLinkManager.java
11	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/RNFetchBlob/RNFetchBlobUtils.java com/tom_roush/pdfbox/pdfwriter/COSWriter.java com/tom_roush/pdfbox/pdmodel/encryption/MessageDigests.java
12	The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	com/tom_roush/pdfbox/pdmodel/encryption/StandardSecurityHandler.java
13	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/tom_roush/pdfbox/pdmodel/encryption/MessageDigests.java
14	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/lyft/kronos/AndroidClockFactory.java

🪪 NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

🖧 BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00189	Get the content of a SMS message	sms	com/RNFetchBlob/Utils/PathResolver.java com/rt2zz/reactnativecontacts/ContactsProvider.java com/vonovak/Utils.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00188	Get the address of a SMS message	sms	com/RNFetchBlob/Utils/PathResolver.java com/rt2zz/reactnativecontacts/ContactsProvider.java com/vonovak/Utils.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/RNFetchBlob/Utils/PathResolver.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00191	Get messages in the SMS inbox	sms	com/RNFetchBlob/RNFetchBlobReq.java com/RNFetchBlob/Utils/PathResolver.java io/branch/coroutines/InstallReferrersKt.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00200	Query data from the contact list	collection contact	com/RNFetchBlob/Utils/PathResolver.java com/rt2zz/reactnativecontacts/ContactsProvider.java com/vonovak/Utils.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00187	Query a URI and check the result	collection sms calllog calendar	com/rt2zz/reactnativecontacts/ContactsProvider.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java

RULE ID	BEHAVIOUR	LABEL	FILES
00201	Query data from the call log	collection calllog	com/RNFetchBlob/Utils/PathResolver.java com/rt2zz/reactnativecontacts/ContactsProvider.java com/vonovak/Utils.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/RNFetchBlob/Utils/PathResolver.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00036	Get resource file from res/raw directory	reflection	app/notifee/core/Notifee.java cl/json/RNSharePathUtil.java com/airbnb/android/react/maps/AirMapMarker.java com/airbnb/android/react/maps/ImageReader.java com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java com/iterable/iterableapi/IterableActionRunner.java com/iterable/iterableapi/IterableNotificationHelper.java io/branch/referral/Branch.java io/invertase/firebase/common/SharedUtils.java me/leolin/shortcutbadger/impl/EverythingMeHomeBadger.java me/leolin/shortcutbadger/impl/HuaweiHomeBadger.java me/leolin/shortcutbadger/impl/NovaHomeBadger.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java n/o/t/i/f/e/e/n.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	android/print/PdfConverter.java cl/json/RNSharePathUtil.java cl/json/ShareFile.java cl/json/ShareFiles.java com/RNFetchBlob/RNFetchBlobFS.java com/RNFetchBlob/RNFetchBlobReq.java com/RNFetchBlob/Utils/PathResolver.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/datadog/android/core/internal/persistence/BatchId.java com/datadog/android/ndk/internal/DatadogNdkCrashHandler.java com/github/mikephil/charting/charts/Chart.java com/iterable/iterableapi/ui/BitmapLoader.java com/logrocket/core/persistence/disk/FileSystem.java com/logrocket/core/persistence/disk/OnDiskEventBatch.java com/logrocket/core/persistence/disk/OnDiskEventBatchCreator.java com/rssignaturecapture/RSSignatureCaptureMainView.java com/rumax/reactnative/pdfviewer/PDFView.java com/tom_roush/pdfbox/io/ScratchFile.java com/tom_roush/pdfbox/pdmodel/font/FileSystemFontProvider.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java
00091	Retrieve data from broadcast	collection	com/datadog/android/rum/_RumInternalProxy.java com/dieam/reactnativepushnotification/modules/RNPushNotification.java com/dieam/reactnativepushnotification/modules/RNPushNotificationPublisher.java com/iterable/iterableapi/IterableApi.java com/iterable/iterableapi/IterablePushActionReceiver.java com/iterable/iterableapi/ui/inbox/IterableInboxActivity.java com/masteratul/exceptionhandler/DefaultErrorScreen.java io/branch/referral/Branch.java

RULE ID	BEHAVIOUR	LABEL	FILES
00024	Write file after Base64 decoding	reflection file	cl/json/ShareFile.java cl/json/ShareFiles.java com/RNFetchBlob/RNFetchBlobBody.java com/RNFetchBlob/RNFetchBlobFS.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/RNFetchBlob/RNFetchBlobBody.java com/RNFetchBlob/RNFetchBlobFS.java com/airbnb/android/react/maps/AirMapLocalTile.java com/airbnb/android/react/maps/AirMapTileProvider.java com/airbnb/android/react/maps/FileUtil.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/beefe/picker/util/BuildProperties.java com/datadog/android/core/internal/persistence/file/batch/PlainBatchFileReaderWriter.java com/iterable/iterableapi/IterableUtil.java com/logrocket/core/CrashReportUploader.java com/logrocket/core/persistence/disk/CrashReportFileSystem.java com/logrocket/core/persistence/disk/FileSystem.java com/logrocket/core/persistence/disk/OnDiskEventBatch.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/rumax/reactnative/pdfviewer/PDFView.java com/tom_roush/fontbox/afm/AFMParser.java com/tom_roush/fontbox/cmap/CMapParser.java com/tom_roush/fontbox/pfb/PfbParser.java com/tom_roush/fontbox/ttf/RAFDataStream.java com/tom_roush/pdfbox/multipdf/PDFMergerUtility.java com/tom_roush/pdfbox/pdmodel/fdf/FDFDocument.java com/tom_roush/pdfbox/pdmodel/font/FileSystemFontProvider.java com/tom_roush/pdfbox/pdmodel/font/PDTrueTypeFont.java com/tom_roush/pdfbox/pdmodel/font/PDType0Font.java com/tom_roush/pdfbox/pdmodel/graphics/image/PDImageXObject.java com/tom_roush/pdfbox/pdmodel/interactive/digitalsignature/visible/PDVisibleSignDesigner.java okio/Okio__JvmOkioKt.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/iterable/iterableapi/IterableRequestTask.java com/logrocket/core/CrashReportUploader.java com/logrocket/core/TelemetryReporter.java com/logrocket/core/persistence/HttpUploadOperation.java com/mixpanel/android/util/HttpService.java com/rumax/reactnative/pdfviewer/AsyncDownload.java
00089	Connect to a URL and receive input stream from the server	command network	com/github/wuxudong/rncharts/utils/DrawableUtils.java com/iterable/iterableapi/IterableRequestTask.java com/iterable/iterableapi/ui/BitmapLoader.java com/logrocket/core/TelemetryReporter.java com/logrocket/core/persistence/HttpUploadOperation.java com/mixpanel/android/util/HttpService.java com/rumax/reactnative/pdfviewer/AsyncDownload.java
00109	Connect to a URL and get the response code	network command	com/iterable/iterableapi/IterableDeeplinkManager.java com/iterable/iterableapi/IterableRequestTask.java com/iterable/iterableapi/ui/BitmapLoader.java com/logrocket/core/CrashReportUploader.java com/logrocket/core/TelemetryReporter.java com/logrocket/core/persistence/HttpUploadOperation.java com/mixpanel/android/util/HttpService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	ai/forethought/ForethoughtActivity.java app/notifee/core/Notifee.java cl/json/RNShareImpl.java cl/json/social/InstagramShare.java cl/json/social/SingleShareIntent.java com/RNFetchBlob/RNFetchBlobReq.java com/chirag/RNMail/RNMailModule.java com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java com/iterable/iterableapi/IterableActionRunner.java com/iterable/iterableapi/IterableNotificationHelper.java com/levelasquez/androidopensettings/AndroidOpenSettings.java io/branch/referral/Branch.java io/branch/referral/validators/DeepLinkRoutingValidator.java io/branch/rnbranch/RNBranchModule.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java n/o/t/i/f/e/e/m.java
00175	Get notification manager and cancel notifications	notification	com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java
00072	Write HTTP input stream into a file	command network file	com/iterable/iterableapi/ui/BitmapLoader.java com/rumax/reactnative/pdfviewer/AsyncDownload.java
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/github/wuxudong/rncharts/utils/DrawableUtils.java com/rumax/reactnative/pdfviewer/AsyncDownload.java
00094	Connect to a URL and read data from it	command network	com/iterable/iterableapi/ui/BitmapLoader.java com/mixpanel/android/util/HttpService.java com/rumax/reactnative/pdfviewer/AsyncDownload.java

RULE ID	BEHAVIOUR	LABEL	FILES
00108	Read the input stream from given URL	network command	com/iterable/iterableapi/ui/BitmapLoader.java com/mixpanel/android/util/HttpService.java com/rumax/reactnative/pdfviewer/AsyncDownload.java
00078	Get the network operator name	collection telephony	com/learnium/RNDeviceInfo/RNDeviceModule.java com/mixpanel/android/mpmetrics/SystemInformation.java io/branch/referral/SystemObserver.java
00056	Modify voice volume	control	com/zmxv/RNSound/RNSoundModule.java
00012	Read data and put it into a buffer stream	file	com/datadog/android/core/internal/persistence/file/batch/PlainBatchFileReaderWriter.java com/tom_roush/fontbox/pfb/PfbParser.java com/tom_roush/pdfbox/pdmodel/fdf/FDFDocument.java
00005	Get absolute path of file and put it to JSON object	file	com/logrocket/core/persistence/disk/OnDiskEventBatchCreator.java
00004	Get filename and put it to JSON object	file collection	com/logrocket/core/LogRocketCore.java com/logrocket/core/persistence/disk/OnDiskEventBatchCreator.java com/mixpanel/android/mpmetrics/MPDbAdapter.java
00009	Put data in cursor to JSON object	file	com/mixpanel/android/mpmetrics/MPDbAdapter.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	app/notifee/core/Notifee.java cl/json/social/InstagramShare.java com/iterable/iterableapi/IterableActionRunner.java com/levelasquez/androidopensettings/AndroidOpenSettings.java io/branch/referral/Branch.java io/branch/rnbranch/RNBranchModule.java n/o/t/i/f/e/e/m.java

RULE ID	BEHAVIOUR	LABEL	FILES
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/airbnb/android/react/maps/AirMapTileProvider.java com/airbnb/android/react/maps/ImageUtil.java
00092	Send broadcast	command	io/branch/rnbranch/RNBranchModule.java
00043	Calculate WiFi signal strength	collection wifi	com/reactnativecommunity/netinfo/ConnectivityReceiver.java
00192	Get messages in the SMS inbox	sms	cl/json/RNSharePathUtil.java com/RNFetchBlob/Utils/PathResolver.java
00112	Get the date of the calendar event	collection calendar	com/reactnative/googlefit/CalorieHistory.java
00014	Read file into a stream and put it into a JSON object	file	com/logrocket/core/CrashReportUploader.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00038	Query the phone number	collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00130	Get the current WIFI information	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00134	Get the current WiFi IP address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java
00082	Get the current WiFi MAC address	collection wifi	com/learnium/RNDeviceInfo/RNDeviceModule.java
00003	Put the compressed bitmap data into JSON object	camera	io/branch/referral/network/BranchRemoteInterfaceUrlConnection.java
00147	Get the time of current location	collection location	com/reactnativecommunity/geolocation/GeolocationModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
00075	Get location of the device	collection location	com/reactnativecommunity/geolocation/GeolocationModule.java
00115	Get last known location of the device	collection location	com/reactnativecommunity/geolocation/GeolocationModule.java

🛢 FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://helloheart-8b854.firebaseio.com
		The Firebase Remote Config at https://firebaseremoteconfig.googleapis.com/v1/projects/662954201697/namespaces/firebase:fetch?key=AIzaSyA5G2ioe6mq-pFqY2QLiaSHxvVBZQUTbpY is enabled. Ensure that the configurations are not sensitive. This is indicated by the response: {'entries': {'a1c_diabetes_links': 'show_links', 'abnormal_reading_manual_request_timeout': '400', 'abnormal_reading_monitor_request_timeout': '1000', 'accuracy_perception_affects': 'on', 'actionable_reminders': 'on', 'activity_mitigation_feature_flag': 'off', 'activity_tab_status': 'on', 'bpEmptyState_feature': 'on', 'bp_contact_doctor_text': 'talk_doctor_text', 'bp_error_detection_feature': 'on', 'bp_graph_version': 'v1', 'bp_irregular_hr_feature': 'on', 'bp_reminders_from_bell_entry': 'your_next_reading_flow', 'bp_reminders_from_registry': 'off', 'bp_reminders_settings': 'v2', 'bp_spike_new_flow': 'on', 'bradycardia_alert': 'on', 'bt_notifications': 'random_message_with_unpaired_devices', 'bt_scanner_mode': '0', 'bt_scanner_version': 'v1', 'cholesterol_home_testing_clinical_trial': 'off', 'cholesterol_meds_impact_section': 'on', 'cholesterol_results_explanation': 'off', 'clinician_report_medications_taken': 'on', 'clinician_report_show_meds_compliance_graph_if_compliance_above_value': '30', 'clinician_report_show_meds_compliance_graph_if_has_tracking_days_above': '30', 'closing_gaps_in_care': 'on', 'closing_gaps_in_care_text': '', 'connect_monitor_from_manual_bp_screen': 'on', 'consent_ehr': 'EHR_consent_existing_risk', 'consent_ehr_existing_continue': 'learn_more_link_only', 'consistent_bradycardia_alert': 'on', 'consistent_tachycardia_alert': 'on', 'correlations_insight_content': 'interactive_insights', 'correlations_insights': 'on', 'correlations_sneak_peek_activity': 'off', 'correlations_sneak_peek_drugs': 'off', 'cvs_minute_clinic': 'on', 'cvs_phase2_schedule_in_app': 'on', 'cvs_schedule_timeslots_format': 'H:mm A', 'datadog_status': 'on', 'dd_sampling_rate': '10', 'defer_max_streak': 'off', 'direct_to_care_stage_two_flow': 'off', 'edit_bp_reminders_from_bell': 'on', 'ehr_consent_screen_x_button': 'off', 'ehr_disabled': 'on', 'ehr_sneak_peek_chol': 'off', 'ehr_sneak_peek_meds_chol': 'on', 'enable_ar_questionnaire': 'on', 'enable_clinician_report_for_last_x_days': 'on',

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config enabled	warning	'enable_cvs_questionnaire': 'on', 'enable_disabled_user_login_message': 'off', 'enable_htc_questionnaire': 'on', 'enable_log_rocket': 'on', 'enable_login_animation': 'off', 'enable_manage_feedback': 'off', 'enable_mental_barriers_feedback': 'off', 'enable_notes_on_readings': 'on', 'enable_notifications_popup': 'let_us_send_reminders', 'enable_pdf_flagged_reading_and_graph': 'on', 'enable_sms_marketing': 'false', 'enhanced_record_service': 'on', 'event_bus_logger': 'on', 'extended_login_flow': 'on', 'feel_check_symptoms': 'on', 'feel_check_symptoms_announcement_enabled': 'on', 'filter_insights_on_client_side': 'on', 'first_x_bps_challenge': 'none', 'first_x_bps_challenge_goal': '7', 'flu_shot_banner_show_limit': '5', 'flu_shot_bp_report_banner': 'off', 'flu_shot_me_tab_schedule': 'off', 'ftue_medical_conditions_list_changes': 'on', 'hearts_on_tracker': 'off', 'himd_bp_trends_remote_source': 'off', 'himd_trends_remote_request_timeout': '500', 'hipaa_fax': 'on', 'holdout_settings': '{"seed":"","percentage":5,"existingUserFromTimestamp":1731499200000,"excludedCompanies":""}', 'homepage_loading_timeout': '1500', 'how_to_measure_flow': 'off', 'how_to_measure_flow_improvements': 'off', 'hr_steps_pearson_correlation_feature': 'on', 'hr_time_correlation_feature': 'on', 'hr_weight_correlation_feature': 'on', 'hyperlipidemia': 'on', 'hyperlipidemia_manage_tooltip': 'on', 'hyperlipidemia_notifications': 'on', 'imbpth_hpyotenstion_support': 'on', 'imbpth_on_tracker': 'off', 'import_medications': 'off', 'in_app_support_chat': 'on', 'inapp_communication_endpoint': 'on', 'insight_templates': 'on', 'insights_button_text': 'helpful_text', 'insights_card_design': 'rounded_insight_cards_green_title', 'insights_feedback_toast': 'on', 'insights_feedback_tooltip': 'on', 'insights_templates_variant': '-1', 'is_abnormal_reading_api_version': 'v2', 'is_medicare_user': 'off', 'last_name_editable': 'on', 'legal_changes_disclaimers_cross_app': 'on', 'legal_changes_disclaimers_cross_app_no_bp': 'on', 'legal_changes_disclaimers_trackers': 'on', 'limit_tracker_data': '-1', 'lipid_test_cvs_schedule': 'on', 'logout_time_interval': '3628800000', 'low_pulse_hr_meds_banner': 'on', 'manage_flow': 'off', 'marginal_pulse_alert': 'on', 'med_notification_splitting': 'on', 'medication_feature_version': 'v1', 'medication_streak': 'off_no_card', 'meds_anncmnt': 'after_bp', 'meds_anncmnt_existing_user': 'never_forget', 'meds_anncmnt_new_user': 'never_forget', 'meds_announcement_dismiss_with_snooze': 'off', 'meds_as_needed_frequency': 'off', 'meds_daily_report_banner': 'on', 'meds_did_you_take': 'none', 'meds_interactions_banner': 'off', 'meds_streak_badges': 'off', 'meds_tab_empty_state': 'animated', 'meds_taking_times': 'off', 'menopause_age_threshold': '45', 'mental_barriers': 'off', 'my_trends': 'off', 'new_insight_tooltip_visibility_duration': 'five_seconds', 'next_actions_contentful_manager': 'off', 'no_clinic_results_popup': 'off', 'no_promo_flow': 'off', 'offline_reading_limit_number': '3', 'onboarding_flow_steps': '["onboardingShippingForm", "onboardingIntro", "onboardingProvenOutcomes", "onboardingHealthStats", "onboardingMedications", "onboardingEthnicity", "onboardingGoals", "onboardingGoalsCards", "onboardingInterests", "onboardingGoalsBPFreq", "onboardingFtueRemindersPermissions", "onboardingActivity", "onboardingProfileName", "onboardingPregnancyMode", "onboardingGetStarted", "onboardingAddPastBP"]', 'onboarding_flow_version': 'v3', 'onboarding_re_engagement_flow_steps': '["onboardingIntro"]', 'profile_page_revamp': 'off', 'pulse_alert_retake': 'on', 'quick_actions': 'off', 'quick_actions_suggest_drilldown': 'on', 'readability_design': 'on', 'readability_tracker_buttons': 'off', 'rebind_monitor': 'on', 'referral_to_other_programs': 'on', 'reminders_bell_tooltip_style': 'with_button', 'reminders_icon_animated': 'off', 'reminders_tooltip_type': 'under_bell_icon', 'satisfaction_score': 'on', 'set_weather_thresholds': 'on', 'share_on_tracker': 'on', 'shipping_confirmation': 'correct_monitor_status', 'should_show_tap_reading_popup': 'off', 'show_inapp_review': 'on', 'show_last_onboarding_screen': 'on', 'solution_bp_correlations_insights': 'off', 'solution_time_correlations_insights': 'on', 'spike_feedback_questionnaire': 'on', 'sticky_button': 'sticky', 'streak_educational_flow': 'on', 'stress_management_activity_cards': 'on', 'stress_referral_banner': 'on', 'stress_referral_link': 'on', 'stressful_days': 'off', 'support_phone_reg': 'true', 'symptom_expanded_option_collapse': 'static', 'symptoms_correlations_insights_timeout': '1500', 'symptoms_correlations_insights_utc': 'on', 'tab_navigator_version': 'v3', 'tachycardia_alert': 'on', 'take_another_reading_tips_during_streak': 'off', 'test_key': '1', 'tracker_readability_design': 'on', 'unlock_report_after_bp_count': '3', 'use_ftue_info_in_crisis_prevention_flow': 'on', 'user_termination': 'on', 'user_testimonial_feature': 'on', 'user_testimonial_text': 'think_text', 'what_did_you_do': 'on'}, 'state': 'UPDATE', 'templateVersion': '1422'}

TITLE	SEVERITY	DESCRIPTION

⠿ ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/25	android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.INTERNET, android.permission.SYSTEM_ALERT_WINDOW, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_CONTACTS, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.WAKE_LOCK, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	8/44	android.permission.ACTIVITY_RECOGNITION, android.permission.READ_CALENDAR, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, android.permission.FOREGROUND_SERVICE, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.ACCESS_NOTIFICATION_POLICY

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
pinterest.com	ok	**IP:** 151.101.128.84 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
help.branch.io	ok	**IP:** 104.18.20.218 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
plus.google.com	ok	**IP:** 172.217.12.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	ok	**IP:** 142.250.188.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cs.android.com	ok	**IP:** 142.250.72.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** [Google Map](#)
github.com	ok	**IP:** 140.82.113.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** [Google Map](#)
twitter.com	ok	**IP:** 172.66.0.227 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** [Google Map](#)
intake.profile.s	ok	No Geolocation information available.
app.logrocket.com	ok	**IP:** 104.198.23.205 **Country:** United States of America **Region:** Iowa **City:** Council Bluffs **Latitude:** 41.261940 **Longitude:** -95.860832 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
notifee.app	ok	**IP:** 13.52.188.95 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** [Google Map](#)
docs.swmansion.com	ok	**IP:** 104.21.27.136 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** [Google Map](#)
api.mixpanel.com	ok	**IP:** 35.190.25.25 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** [Google Map](#)
branch.app.link	ok	**IP:** 18.238.109.69 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
solve-widget.forethought.ai	ok	**IP:** 172.66.44.175 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** [Google Map](#)
api3-eu.branch.io	ok	**IP:** 18.155.173.118 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** [Google Map](#)
api.branch.io	ok	**IP:** 18.238.109.24 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** [Google Map](#)
bnc.lt	ok	**IP:** 18.238.109.120 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** [Google Map](#)

DOMAIN	STATUS	GEOLOCATION
cdn.branch.io	ok	**IP:** 18.238.109.80 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
r.logrocket.io	ok	**IP:** 104.198.23.205 **Country:** United States of America **Region:** Iowa **City:** Council Bluffs **Latitude:** 41.261940 **Longitude:** -95.860832 **View:** Google Map
r.lr-intake.com	ok	**IP:** 104.198.23.205 **Country:** United States of America **Region:** Iowa **City:** Council Bluffs **Latitude:** 41.261940 **Longitude:** -95.860832 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
helloheart-8b854.firebaseio.com	ok	**IP:** 35.190.39.113 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.iterable.com	ok	**IP:** 44.223.131.16 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.googleapis.com	ok	**IP:** 142.250.68.42 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
docs.logrocket.com	ok	**IP:** 104.16.242.118 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
links.iterable.com	ok	**IP:** 54.224.98.192 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
e.logrocket.com	ok	**IP:** 172.66.147.58 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api2.branch.io	ok	**IP:** 18.238.109.69 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
api.hello.do	ok	**IP:** 34.197.37.71 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

🕵 TRACKERS

TRACKER	CATEGORIES	URL
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
Facebook Flipper	Analytics	https://reports.exodus-privacy.eu.org/trackers/392
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"ANDROID_CLIENT_API_KEY" : "eyJhcGkiOiJyZWFjdC1uYXRpdmUtYW5kcm9pZC1jbGllbnQiLCJrZXkiOiJaVFhzTmNnVldLSFhWeGN4UW1Wd0JaaVFZZUZIVVpvTUNtQ1BadVdRS1JKekkVZcXVZZUVnWG5CQ2ZKeEx2aFdFIn0"
"BUGSNAG_API_KEY" : "emptyKey"
"CONTENTFUL_AUTH_TOKEN" : "-ocHOJUyoxVhw5bTiTPb0k3AcfZMLb2M3nTcaPRguig"
"FORETHOUGHT_API_KEY" : "9b6241c9-ad8a-4b71-ad0e-4986540784ea"
"GOOGLE_MAPS_IOS_API_KEY" : "AIzaSyC8fShF4YwIjhjZfgsoeYqOXFE16D2P-vY"

POSSIBLE SECRETS

"HUMAN_API_CLIENT_ID" : "35026d8d18e4485a3ede8b17295230f87c720d6a"

"IOS_CLIENT_API_KEY" : "eyJhcGkiOiJyZWFjdC1uYXRpdmUtaW9zLWNsaWVudCIsImtleSI6ImhDQ0Z0anJwRm9GYW5BQXpHHTE1hbWl4Z1pjbm1GUFFqUXFFYlhGGc3Fwc3BUV1dmUGd0dmZodlhpXUXBrdXJJclEifQ"

"ITERABLE_API_KEY" : "a418ad72e06c4af6981300af1cb19881"

"LOG_ROCKET_KEY" : "ujp5kq/helloheart"

"MIXPANEL_TOKEN" : "6b0600ea3b4cdca6c96c14b465805cfe"

"RUM_CLIENT_TOKEN" : "pub462babc64ce262bcb7e628cfa28cd338"

"firebase_database_url" : "https://helloheart-8b854.firebaseio.com"

"google_api_key" : "AIzaSyA5G2ioe6mq-pFqY2QLiaSHxvVBZQUTbpY"

"google_crash_reporting_api_key" : "AIzaSyA5G2ioe6mq-pFqY2QLiaSHxvVBZQUTbpY"

"google_maps_api_key" : "AIzaSyDHolzT2_UNfl0M0HAoHOLSwbAwXyMYaO8"

FFFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A93AD2CAFFFFFFFFFFFFFFFFFF

DB7C2ABF62E35E668076BEAD2088

POSSIBLE SECRETS

FFFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DCC4024FFFFFFFFFFFFFFFF

0400FAC9DFCBAC8313BB2139F1BB755FEF65BC391F8B36F8F8EB7371FD558B01006A08A41903350678E58528BEBF8A0BEFF867A7CA36716F7E01F81052

0400D9B67D192E0367C803F39E1A7E82CA14A651350AAE617E8F01CE94335607C304AC29E7DEFBD9CA01F596F927224CDECF6C

E95E4A5F737059DC60DFC7AD95B3D8139515620F

FFFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AACAA68FFFFFFFFFFFFFFFF

0620048D28BCBD03B6249C99182B7C8CD19700C362C46A01

2580F63CCFE44138870713B1A92369E33E2135D266DBB372386C400B

74D59FF07F6B413D0EA14B344B20A2DB049B50C3

26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6

0370F6E9D04D289C4E89913CE3530BFDE903977D42B146D539BF1BDE4E9C92

POSSIBLE SECRETS

046AB1E344CE25FF3896424E7FFE14762ECB49F8928AC0C76029B4D5800374E9F5143E568CD23F3F4D7C0D4B1E41C8CC0D1C6ABD5F1A46DB4C

FFFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3D
F1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB1
82B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9C
E98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B423861285C97FFFFFFFFFFFFFFFF

64033881142927202683649881450433473985931760268884941288852745803908878638612

04AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25DBF55296C3A545E3872760AB73617DE4A96262C6F5D9E98BF9292DC29F
8F41DBD289A147CE9DA3113B5F0B8C00A60B1CE1D7E819D7A431D7C90EA0E5F

FFFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3D
F1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB1
82B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9C
E98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99
C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF6
9EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B
6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1
A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23
BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855
322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C
1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C
6272B045B3B71F9DC6B80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CCFF46AAA36AD004CF600C8381E425A31D951AE64FDB23FCEC
9509D43687FEB69EDD1CC5E0B8CC3BDF64B10EF86B63142A3AB8829555B2F747C932665CB2C0F1CC01BD70229388839D2AF05E454504AC78B7582822846C0BA35C
35F5C59160CC046FD8251541FC68C9C86B022BB7099876A460E7451A8A93109703FEE1C217E6C3826E52C51AA691E0E423CFC99E9E31650C1217B624816CDAD9A95
F9D5B8019488D9C0A0A1FE3075A577E23183F81D4A3F2FA4571EFC8CE0BA8A4FE8B6855DFE72B0A66EDED2FBABFBE58A30FAFABE1C5D71A87E2F741EF8C1FE86FEA
6BBFDE530677F0D97D11D49F7A8443D0822E506A9F4614E011E2A94838FF88CD68C8BB7C5C6424CFFFFFFFFFFFFFFFF

1E589A8595423412134FAA2DBDEC95C8D8675E58

0c14416e6f6e796d6f75732053656e64657220202020

POSSIBLE SECRETS

04A1455B334DF099DF30FC28A169A467E9E47075A90F7E650EB6B7A45C7E089FED7FBA344282CAFBD6F7E319F7C0B0BD59E2CA4BDB556D61A5

A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377

MQVwithSHA512KDFAndSharedInfo

000102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F

04B8266A46C55657AC734CE38F018F2192

F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C03

8834235323891921647916487503603088853144765972529603627924508606096998339

9cdbd84c9f1ac2f38d0f80f42ab952e7338bf511

2866537B676752636A68F56554E12640276B649EF7526267

FC1217D4320A90452C760A58EDCD30C8DD069B3C34453837A34ED50CB54917E1C2112D84D164F444F8F74786046A

a418ad72e06c4af6981300af1cb19881

POSSIBLE SECRETS

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

2981889391773124073347127324031476992724055081238369568914649526160456590247

91A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C40094DBACDB586FB20

00E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B

3FCDA526B6CDF83BA1118DF35B3C31761D3545F32728D003EEB25EFE96

8CF83642A709A097B447997640129DA299B1A47D1EB3750BA308B0FE64F5FBD3

3045AE6FC8422F64ED579528D38120EAE12196D5

AC6BDB41324A9A9BF166DE5E1389582FAF72B6651987EE07FC3192943DB56050A37329CBB4A099ED8193E0757767A13DD52312AB4B03310DCD7F48A9DA04FD50E
8083969EDB767B0CF6095179A163AB3661A05FBD5FAAAE82918A9962F0B93B855F97993EC975EEAA80D740ADBF4FF747359D041D5C33EA71D281E446B14773BCA9
7B43A23FB801676BD207A436C6481F1D2B9078717461A5B9D32E688F87748544523B524B0D57D5EA77A2775D2ECFA032CFBDBF52FB3786160279004E57AE6AF874E
7303CE53299CCC041C7BC308D82A5698F3A8D0C38271AE35F8E9DBFBB694B5C803D89F7AE435DE236D525F54759B65E372FCD68EF20FA7111F9E4AFF73

04188DA80EB03090F67CBF20EB43A18800F4FF0AFD82FF101207192B95FFC8DA78631011ED6B24CDD573F977A11E794811

64210519E59C80E70FA7E9AB72243049FEB8DEECC146B9B1

POSSIBLE SECRETS

04A8C7DD22CE28268B39B55416F0447C2FB77DE107DCD2A62E880EA53EEB62D57CB4390295DBC9943AB78696FA504C11

0101D556572AABAC800101D556572AABAC8001022D5C91DD173F8FB561DA6899164443051D

F1FD178C0B3AD58F10126DE8CE42435B3961ADBCABC8CA6DE8FCF353D86E9C00

00C8619ED45A62E6212E1160349E2BFA844439FAFC2A3FD1638F9E

5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B

eyJhcGkiOiJyZWFjdC1uYXRpdmUtYW5kcm9pZC1jbGllbnQiLCJrZXkiOiJaVFhzTmNnVldLSFhWeGGN4UW1Wd0JaaVFFZZUZlVVpvTUNNtQ1BadVdRS1JKekVVZcXVZZUVnWG5CQ2ZKeEx2aFdFIn0

07A526C63D3E25A256A007699F5447E32AE456B50E

7503CFE87A836AE3A61B8816E25450E6CE5E1C93ACF1ABC1778064FDCBEFA921DF1626BE4FD036E93D75E6A50E3A41E98028FE5FC235F5B889A589CB5215F2A4

0307AF69989546103D79329FCC3D74880F33BBE803CB

04A3E8EB3CC1CFE7B7732213B23A656149AFA142C47AAFBC2B79A191562E1305F42D996C823439C56D7F7B22E14644417E69BCB6DE39D027001DABE8F35B25C9BE

FFFFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3D
F1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB1
82B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9C
E98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99
C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF6
9EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B
6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1
A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E655F6AFFFFFFFFFFFFFFFFFF

790408F2EEDAF392B012EDEFB3392F30F4327C0CA3F31FC383C422AA8C16

POSSIBLE SECRETS

35026d8d18e4485a3ede8b17295230f87c720d6a

3045AE6FC8422f64ED579528D38120EAE12196D5

00FC1217D4320A90452C760A58EDCD30C8DD069B3C34453837A34ED50CB54917E1C2112D84D164F444F8F74786046A

10686D41FF744D4449FCCF6D8EEA03102E6812C93A9D60B978B702CF156D814EF

64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1

0257927098FA932E7C0A96D3FD5B706EF7E5F5C156E16B7E7C86038552E91D

0238af09d98727705120c921bb5e9e26296a3cdcf2f35757a0eafd87b830e7

FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551

fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17

0479BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8

00F50B028E4D696E676875615175290472783FB1

ffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632551

678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4

9494fec095f3b85ee286542b3836fc81a5dd0a0349b4c239dd38744d488cf8e31db8bcb7d33b41abb9e5a33cca9144b1cef332c94bf0573bf047a3aca98cdf3b

POSSIBLE SECRETS

FFFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C934063199FFFFFFFFFFFFFFFFFF

662C61C430D84EA4FE66A7733D0B76B7BF93EBC4AF2F49256AE58101FEE92B04

B4E134D3FB59EB8BAB57274904664D5AF50388BA

02A29EF207D0E9B6C55CD260B306C7E007AC491CA1B10C62334A9E8DCD8D20FB7

040369979697AB43897789566789567F787A7876A65400435EDB42EFAFB2989D51FEFCE3C80988F41FF883

42debb9da5b3d88cc956e08787ec3f3a09bba5f48b889a74aaf53174aa0fbe7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76137e792f3f0db859d095e4a5b932024f079ecf2ef09c797452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94cccf1449ac43d586d0beee43251b0b2287349d68de0d144403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1b27d0639f695e347d8d1cf9ac819a26ca9b04cb0eb9b7b035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffbc97134025fe8ce04c4399ad96569be91a546f4978693c7a

2AA058F73A0E33AB486B0F610410C53A7F132310

4099B5A457F9D69F79213D094C4BCD4D4262210B

040081BAF91FDF9833C40F9C181343638399078C6E7EA38C001F73C8134B1B4EF9E150

91E38443A5E82C0D880923425712B2BB658B9196932E02C78B2582FE742DAA28

A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5374

POSSIBLE SECRETS

7d7374168ffe3471b60a857686a19475d3bfa2ff

3826F008A8C51D7B95284D9D03FF0E00CE2CD723A

985BD3ADBAD4D696E676875615175A21B43A97E3

6db14acc9e21c820ff28b1d5ef5de2b0

048BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F046997

3086d221a7d46bcde86c90e49284eb15

b8adf1378a6eb73409fa6c9c637ba7f5

9760508f15230bccb292b982a2eb840bf0581cf5

AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F0

010092537397ECA4F6145799D62B0A19CE06FE26AD

714114B762F2FF4A7912A6D2AC58B9B5C2FCFE76DAEB7129

FD0D693149A118F651E6DCE6802085377E5F882D1B510B44160074C1288078365A0396C8E681

E95E4A5F737059DC60DF5991D45029409E60FC09

10E723AB14D696E6768756151756FEBF8FCB49A9

041D1C64F068CF45FFA2A63A81B7C13F6B8847A3E77EF14FE3DB7FCAFE0CBD10E8E826E03436D646AAEF87B2E247D4AF1E8ABE1D7520F9C2A45CB1EB8E95CFD55262B70B29FEEC5864E19C054FF99129280E46462177918111142820341263C5315

POSSIBLE SECRETS

153d5d6172adb43045b68ae8e1de1070b6137005686d29d3d73a7749199681ee5b212c9b96bfdcfa5b20cd5e3fd2044895d609cf9b410b7a0f12ca1cb9a428cc

044AD5F7048DE709AD51236DE65E4D4B482C836DC6E410664002BB3A02D4AAADACAE24817A4CA3A1B014B5270432DB27D2

020ffa963cdca8816ccc33b8642bedf905c3d358573d3f27fbbd3b3cb9aaaf

6b8cf07d4ca75c88957d9d670591

71FE1AF926CF847989EFEF8DB459F66394D90F32AD3F15E8

043AE9E58C82F63C30282E1FE7BBF43FA72C446AF6F4618129097E2C5667C2223A902AB5CA449D0084B7E5B3DE7CCC01C9

5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b

216EE8B189D291A0224984C1E92F1D16BF75CCD825A087A239B276D3167743C52C02D6E7232AA

3086d221a7d46bcde86c90e49284eb153dab

0021A5C2C8EE9FEB5C4B9A753B7B476B7FD6422EF1F3DD674761FA99D6AC27C8A9A197B272822F6CD57A55AA4F50AE317B13545F

0402FE13C0537BBC11ACAA07D793DE4E6D5E5C94EEE80289070FB05D38FF58321F2E800536D538CCDAA3D9

4A8C7DD22CE28268B39B55416F0447C2FB77DE107DCD2A62E880EA53EEB62D57CB4390295DBC9943AB78696FA504C11

5667676A654B20754F356EA92017D946567C46675556F19556A04616B567D223A5E05656FB549016A96656A557

C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86297

POSSIBLE SECRETS

4D696E676875615175985BD3ADBADA21B43A97E2

A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7

A4D1CBD5C3FD34126765A442EFB99905F8104DD258AC507FD6406CFF14266D31266FEA1E5C41564B777E690F5504F213160217B4B01B886A5E91547F9E2749F4D7F
BD7D3B9A92EE1909D0D2263F80A76A6A24C087A091F531DBF0A0169B6A28AD662A4D18E73AFA32D779D5918D08BC8858F4DCEF97C2A24855E6EEB22B3B2E5

0091A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C40094DBACDB586FB20

0429A0B6A887A983E9730988A68727A8B2D126C44CC2CC7B2A6555193035DC76310804F12E549BDB011C103089E73510ACB275FC312A5DC6B76553F0CA

e3f1f98c9da02a93bb547f448b472d727e14b22455235796fe49863856252508

D35E472036BC4FB7E13C785ED201E065F98FCFA5B68F12A32D482EC7EE8658E98691555B44C59311

020A601907B8C953CA1481EB10512F78744A3205FD

1A8F7EDA389B094C2C071E3647A8940F3C123B697578C213BE6DD9E6C8EC7335DCB228FD1EDF4A39152CBCAAF8C0398828041055F94CEEEC7E21340780FE41BD

32879423AB1A0375895786C4BB46E9565FDE0B5344766740AF268ADB32322E5C

A59A749A11242C58C894E9E5A91804E8FA0AC64B56288F8D47D51B1EDC4D65444FECA0111D78F35FC9FDD4CB1F1B79A3BA9CBEE83A3F811012503C8117F98E5048
B089E387AF6949BF8784EBD9EF45876F2E6A5A495BE64B6E770409494B7FEE1DBB1E4B2BC2A53D4F893D418B7159592E4FFFDF6969E91D770DAEBD0B5CB14C00AD
68EC7DC1E5745EA55C706C4A1C5C88964E34D09DEB753AD418C1AD0F4FDFD049A955E5D78491C0B7A2F1575A008CCD727AB376DB6E695515B05BD412F5B8C2F4C
77EE10DA48ABD53F5DD498927EE7B692BBBCDA2FB23A516C5B4533D73980B2A3B60E384ED200AE21B40D273651AD6060C13D97FD69AA13C5611A51B9085

71169be7330b3038edb025f1

POSSIBLE SECRETS

5E5CBA992E0A680D885EB903AEA78E4A45A469103D448EDE3B7ACCC54D521E37F84A4BDD5B06B0970CC2D2BBB715F7B82846F9A0C393914C792E6A923E2117AB8
05276A975AADB5261D91673EA9AAFFEECBFA6183DFCB5D3B7332AA19275AFA1F8EC0B60FB6F66CC23AE4870791D5982AAD1AA9485FD8F4A60126FEB2CF05DB8A7F
0F09B3397F3937F2E90B9E5B9C9B6EFEF642BC48351C46FB171B9BFA9EF17A961CE96C7E7A7CC3D3D03DFAD1078BA21DA425198F07D2481622BCE45969D9C4D606
3D72AB7A0F08B2F49A7CC6AF335E08C4720E31476B67299E231F8BD90B39AC3AE3BE0C6B6CACEF8289A2E2873D58E51E029CAFBD55E6841489AB66B5B4B9BA6E2F
784660896AFF387D92844CCB8B69475496DE19DA2E58259B090489AC8E62363CDF82CFD8EF2A427ABCD65750B506F56DDE3B988567A88126B914D7828E2B63A6D7
ED0747EC59E0E0A23CE7D8A74C1D2C2A7AFB6A29799620F00E11C33787F7DED3B30E1A22D09F1FBDA1ABBBFBF25CAE05A13F812E34563F99410E73B

6b0600ea3b4cdca6c96c14b465805cfe

040503213F78CA44883F1A3B8162F188E553CD265F23C1567A16876913B0C2AC245849283601CCDA380F1C9E318D90F95D07E5426FE87E45C0E8184698E45962364E
34116177DD2259

eyJhcGkiOiJyZWFjdC1uYXRpdmUtaW9zLWNsaWVudCIsImtleSI6ImhDQ0Z0anJwRm9GYW5BQXppHTE1hbWl4Z1pjbm1GUFFqUXFFYWlhGc3Fwc3BUV1dmUGd0dmZodXpX
UXBrdXJclEifQ

00E8BEE4D3E2260744188BE0E9C723

13407807929942597099574024998205846127479365820592393377723561443721764030073546976801874298166903427690031858186486050853753882811946
569946433649006084095

FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1
356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE65381FFFFFFFFFFFFFFFFF

13353181327272067343385951994831900121794237596784748689948235959936964252873471246159040332773182141032801252925387191478859899310331
0567744136196364803064721377826656898686468463277710150809401182608770201615324990468332931294920912776241137878030224355746606283971 6
5937642683267426978088006163152816347 5887

90066455B5CFC38F9CAA4A48B4281F292C260FEEF01FD61037E56258A7795A1C7AD46076982CE6BB956936C6AB4DCFE05E6784586940CA544B9B2140E1EB523F009
D20A7E7880E4E5BFA690F1B9004A27811CD9904AF70420EEFD6EA11EF7DA129F58835FF56B89FAA637BC9AC2EFAAB903402229F491D8D3485261CD068699B6BA58A
1DDBBEF6DB51E8FE34E8A78E542D7BA351C21EA8D8F1D29F5D5D15939487E27F4416B0CA632C59EFD1B1EB66511A5A0FBF615B766C5862D0BD8A3FE7A0E0DA0FB
2FE1FCB19E8F9996A8EA0FCCDE538175238FC8B0EE6F29AF7F642773EBE8CD5402415A01451A840476B2FCEB0E388D30D4B376C37FE401C2A2C2F941DAD179C540C
1C8CE030D460C4D983BE9AB0B20F69144C1AE13F9383EA1C08504FB0BF321503EFE43488310DD8DC77EC5B8349B8BFE97C2C560EA878DE87C11E3D597F1FEA742D
73EEC7F37BE43949EF1A0D15C3F3E3FC0A8335617055AC91328EC22B50FC15B941D3D1624CD88BC25F3E941FDDC6200689581BFEC416B4B2CB73

POSSIBLE SECRETS

B99B99B099B323E02709A4D696E6768756151751

03CE10490F6A708FC26DFE8C3D27C4F94E690134D5BFF988D8D28AAEAEDE975936C66BAC536B18AE2DC312CA493117DAA469C640CAF3

5181942b9ebc31ce68dacb56c16fd79f

AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA703308717D4D9B009BC66842AECDA12AE6A380E62881FF2F2D82C68528AA6056583A48F3

043B4C382CE37AA192A4019E763036F4F5DD4D7EBB938CF935318FDCED6BC28286531733C3F03C4FEE

798851416634109768976271189357563237473079519165076397583004726923388735339 59

90EAF4D1AF0708B1B612FF35E0A2997EB9E9D263C9CE659528945C0D

287926658148546112969923474583802841350286367782291130057563347309963038881 24

8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a9
78d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f

00C9BB9E8927D4D64C377E2AB2856A5B16E3EFB7F61D4316AE

8e722de3125bddb05580164bfe20b8b432216a62926c57502ceede31c47816edd1e89769124179d0b695106428815065

D6031998D1B3BBFEBF59CC9BBFF9AEE1

115792089237316195423570985008687907853269984665640564039457584007913129639316

b3fb3400dec5c4adceb8655d4c94

0401F481BC5F0FF84A74AD6CDF6FDEF4BF6179625372D8C0C5E10025E399F2903712CCF3EA9E3A1AD17FB0B3201B6AF7CE1B05

POSSIBLE SECRETS

24B7B137C8A14D696E6768756151756FD0DA2E5C

ae2044fb577e65ee8bb576ca48a2f06e

F1FD178C0B3AD58F10126DE8CE42435B53DC67E140D2BF941FFDD459C6D655E1

030024266E4EB5106D0A964D92C4860E2671DB9B6CC5

10B7B4D696E6768756151751537C8A16FD0DA2211

3EE30B568FBAB0F883CCEBD46D3F3BB8A2A73513F5EB79DA66190EB085FFA9F492F375A97D860EB4

9CA8B57A934C54DEEDA9E54A7BBAD95E3B2E91C54D32BE0B9DF96D8D35

D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E24

03F7061798EB99E238FD6F1BF95B48FEEB4854252B

85053bf24bba75239b16a601d9387e17

6b8cf07d4ca75c88957d9d67059037a4

AADD9DB8DBE9C48B3FD4E6AE33C9FC07CB308DB3B3C9D20ED6639CCA70330870553E5C414CA92619418661197FAC10471DB1D381085DDADDB58796829CA90069

962eddcc369cba8ebb260ee6b6a126d9346e38c5

E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B

0202F9F87B7C574D0BDECF8A22E6524775F98CDEBDCB

POSSIBLE SECRETS

E0D2EE25095206F5E2A4F9ED229F1F256E79A0E2B455970D8D0D865BD94778C576D62F0AB7519CCD2A1A906AE30D

1ddaa4b892e61b0f7010597ddc582ed3

1157920892373161954235709850086879078530737629084992432253781558050790688850323

bb85691939b869c1d087f601554b96b80cb4f55b35f433c2

06973B15095675534C7CF7E64A21BD54EF5DD3B8A0326AA936ECE454D2C

cc22d6dfb95c6b25e49c0d6364a4e5980c393aa21668d953

401028774D7777C7B7666D1366EA432071274F89FF01E718

FFFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA237327FFFFFFFFFFFFFFFF

0481AEE4BDD82ED9645A21322E9C4C6A9385ED9F70B5D916C1B43B62EEF4D0098EFF3B1F78E2D0D48D50D1687B93B97D5F7C6D5047406A5E688B352209BCB9F8227DDE385D566332ECC0EABFA9CF7822FDF209F70024A57B1AA000C55B881F8111B2DCDE494A5F485E5BCA4BD88A2763AED1CA2B2FA8F0540678CD1E0F3AD80892

044A96B5688EF573284664698968C38BB913CBFC8223A628553168947D59DCC912042351377AC5FB32

627710173538668076383578942320766641608390870039032496127 9

AlzaSyC8fShF4YwIjhjZfgsoeYqOXFE16D2P

db92371d2126e9700324977504e8c90e

659EF8BA043916EEDE8911702B22

POSSIBLE SECRETS

b869c82b35d70e1b1ff91b28e37a62ecdc34409b

0452DCB034293A117E1F4FF11B30F7199D3144CE6DFEAFFEF2E331F296E071FA0DF9982CFEA7D43F2E

03E5A88919D7CAFCBF415F07C2176573B2

04026EB7A859923FBC82189631F8103FE4AC9CA2970012D5D46024804801841CA44370958493B205E647DA304DB4CEB08CBBD1BA39494776FB988B47174DCA88C7E2945283A01C89720349DC807F4FBF374F4AEADE3BCA95314DD58CEC9F307A54FFC61EFC006D8A2C9D4979C0AC44AEA74FBEBBB9F772AEDCB620B01A7BA7AF1B320430C8591984F601CD4C143EF1C7A3

D2C0FB15760860DEF1EEF4D696E6768756151754

255705fa2a306654b1f4cb03d6a750a30c250102d4988717d9ba15ab6d3e

32010857077C5431123A46B808906756F543423E8D27877578125778AC76

4D41A619BCC6EADF0448FA22FAD567A9181D37389CA

0017858FEB7A98975169E171F77B4087DE098AC8A911DF7B01

MQVwithSHA256KDFAndSharedInfo

CFA0478A54717B08CE64805B76E5B14249A77A4838469DF7F7DC987EFCCFB11D

469A28EF7C28CCA3DC721D044F4496BCCA7EF4146FBF25C9

aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7

01AF286BCA1AF286BCA1AF286BCA1AF286BCA1AF286BC9FB8F6B85C556892C20A7EB964FE7719E74F490758D3B

5c4ece41241a1bb513f6e3e5df74ab7d5183dfffbd71bfd43127920d880569fd

POSSIBLE SECRETS

85E25BFE5C86226CDB12016F7553F9D0E693A268

24b2477514809255df232947ce7928c4

77E2B07370EB0F832A6DD5B62DFC88CD06BB84BE

0713612DCDDCB40AAB946BDA29CA91F73AF958AFD9

77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399

340282366920938463463374607431768211455

04B199B13B9B34EFC1397E64BAEB05ACC265FF2378ADD6718B7C7C1961F0991B842443772152C9E0AD

BB8E5E8FBC115E139FE6A814FE48AAA6F0ADA1AA5DF91985

D09E8800291CB85396CC6717393284AAA0DA64BA

14518877557776399015115874320830702024226143809848893135505709196593151770659565743590789126541491676439926842369913057775743308316665
11589145701059710742276692757882915756220901998212975756543223550490431013061082131040808010565293748926901442915057819663730454818359
47239164288532817130229924555666307371985 5

005DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2

6BA06FE51464B2BD26DC57F48819BA9954667022C7D03

8d5155894229d5e689ee01e6018a237e2cae64cd

520883949DFDBC42D3AD198640688A6FE13F41349554B49ACC31DCCD884539816F5EB4AC8FB1F1A6

POSSIBLE SECRETS

e43bb460f0b80cc0c0b075798e948060f8321b7d

7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9

0418DE98B02DB9A306F2AFCD7235F72A819B80AB12EBD653172476FECD462AABFFC4FF191B946A5F54D8D0AA2F418808CC25AB056962D30651A114AFD2755AD33
6747F93475B7A1FCA3B88F2B6A208CCFE469408584DC2B2912675BF5B9E582928

C196BA05AC29E1F9C3C72D56DFFC6154A033F1477AC88EC37F09BE6C5BB95F51C296DD20D1A28A067CCC4D4316A4BD1DCA55ED1066D438C35AEBAABF57E7DAE4
28782A95ECA1C143DB701FD48533A3C18F0FE23557EA7AE619ECACC7E0B51652A8776D02A425567DED36EABD90CA33A1E8D988F0BBB92D02D1D20290113BB562C
E1FC856EEB7CDD92D33EEA6F410859B179E7E789A8F75F645FAE2E136D252BFFAFF89528945C1ABE705A38DBC2D364AADE99BE0D0AAD82E5320121496DC65B3930
E38047294FF877831A16D5228418DE8AB275D7D75651CEFED65F78AFC3EA7FE4D79B35F62A0402A1117599ADAC7B269A59F353CF450E6982D3B1702D9CA83

0443BD7E9AFB53D8B85289BCC48EE5BFE6F20137D10A087EB6E7871E2A10A599C710AF8D0D39E2061114FDD05545EC1CC8AB4093247F77275E0743FFED117182EAA
9C77877AAAC6AC7D35245D1692E8EE1

00FDFB49BFE6C3A89FACADAA7A1E5BBC7CC1C2E5D831478814

00C9517D06D5240D3CFF38C74B20B6CD4D6F9DD4D9

023b1660dd701d0839fd45eec36f9ee7b32e13b315dc02610aa1b636e346df671f790f84c5e09b05674dbb7e45c803dd

517cc1b727220a94fe13abe8fa9a6ee0

7A1F6653786A68192803910A3D30B2A2018B21CD54

POSSIBLE SECRETS

FFFFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3D F1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB1 82B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9C E98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99 C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF6 9EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B66C62E37FFFFFFFFFFFFFFFFFF

703900853520833051995477180190184378409208826471640810353226014583522983966601

1CEF494720115657E18F938D7A7942394FF9425C1458C57861F9EEA6ADBE3BE10

fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f 9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7

87A8E61DB4B6663CFFBBD19C651959998CEEF608660DD0F25D2CEED4435E3B00E00DF8F1D61957D4FAF7DF4561B2AA3016C3D91134096FAA3BF4296D830E9A7C20 9E0C6497517ABD5A8A9D306BCF67ED91F9E6725B4758C022E0B1EF4275BF7B6C5BFC11D45F9088B941F54EB1E59BB8BC39A0BF12307F5C4FDB70C581B23F76B63A CAE1CAA6B7902D52526735488A0EF13C6D9A51BFA4AB3AD8347796524D8EF6A167B5A41825D967E144E5140564251CCACB83E6B486F6B3CA3F7971506026C0B857 F689962856DED4010ABD0BE621C3A3960A54E710C375F26375D7014103A4B54330C198AF126116D2276E11715F693877FAD7EF09CADB094AE91E1A1597

95475cf5d93e596c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bbdd84c9836be1f31c0777725aeb6c2fc38b85f48076fa76bcd8146cc89a6fb2f706 dd719898c2083dc8d896f84062e2c9c94d137b054a8d8096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9eb60eee8b030376b236bc 73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520086746175c8885925ebc64c6147906773496990cb714ec 667304e261faee33b3cbdf008e0c3fa90650d97d3909c9275bf4ac86ffcb3d03e6dfc8ada5934242dd6d3bcca2a406cb0b

b462babc64ce262bcb7e628cfa28cd338

0217C05610884B63B9C6C7291678F9D341

021085E2755381DCCCE3C1557AFA10C2F0C0C2825646C5B34A394CBCFA8BC16B22E7E789E927BE216F02E1FB136A5F

6C010747560991222210569111C77D77E77A777E7E7E77FCB

POSSIBLE SECRETS

115792089210356248762697446949407573530086143415290314195533631308867097853951

D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FF

04B6B3D4C356C139EB31183D4749D423958C27D2DCAF98B70164C97A2DD98F5CFF6142E0F7C8B204911F9271F0F3ECEF8C2701C307E8E4C9E183115A1554062CFB

4A6E0856526436F2F88DD07A341E32D04184572BEB710

03eea2bae7e1497842f2de7769cfe9c989c072ad696f48034a

7F519EADA7BDA81BD826DBA647910F8C4B9346ED8CCDC64E4B1ABD11756DCE1D2074AA263B88805CED70355A33B471EE

7fffffffffffffffffffffff800000cfa7e8594377d414c03821bc582063

C8619ED45A62E6212E1160349E2BFA844439FAFC2A3FD1638F9E

30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d2029d83c1c158547f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346d3f529252

0051953EB9618E1C9A1F929A21A0B68540EEA2DA725B99B315F3B8B489918EF109E156193951EC7E937B1652C0BD3BB1BF073573DF883D2C34F1EF451FD46B503F00

BDB6F4FE3E8B1D9E0DA8C0D46F4C318CEFE4AFE3B6B8551F

0066647EDE6C332C7F8C0923BB58213B333B20E9CE4281FE115F7D8F90AD

295F9BAE7428ED9CCC20E7C359A9D41A22FCCD9108E17BF7BA9337A6F8AE9513

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

0340340340340340340340340340340340340340340340340340323C313FAB50589703B5EC68D3587FEC60D161CC149C1AD4A91

POSSIBLE SECRETS

5D9306BACD22B7FAEB09D2E049C6E2866C5D1677762A8F2F2DC9A11C7F7BE8340AB2237C7F2A0

040303001D34B856296C16C0D40D3CD7750A93D1D2955FA80AA5F40FC8DB7B2ABDBDE53950F4C0D293CDD711A35B67FB1499AE60038614F1394ABFA3B4C850D927E1E7769C8EEC2D19037BF27342DA639B6DCCFFFEB73D69D78C6C27A6009CBBCA1980F8533921E8A684423E43BAB08A576291AF8F461BB2A8B3531D2F0485C19B16E2F1516E23DD3C1A4827AF1B8AC15B

1b9fa3e518d683c6b65763694ac8efbaec6fab44f2276171a42726507dd08add4c3b3f4c1ebc5b1222ddba077f722943b24c3edfa0f85fe24d0c8c01591f0be6f63

0095E9A9EC9B297BD4BF36E059184F

1A62BA79D98133A16BBAE7ED9A8E03C32E0824D57AEF72F88986874E5AAE49C27BED49A2A95058068426C2171E99FD3B43C5947C857D

7A556B6DAE535B7B51ED2C4D7DAA7A0B5C55F380

28091019353058090096996979000309560759124368558014865957655842872397301267595

28E9FA9E9D9F5E344D5A9E4BCF6509A7F39789F515AB8F92DDBCBD414D940E93

25FBC363582DCEC065080CA8287AAFF09788A66DC3A9E

43FC8AD242B0B7A6F3D1627AD5654447556B47BF6AA4A64B0C2AFE42CADAB8F93D92394C79A79755437B56995136

1157920892373161954235709850086879078532699846656405640394575840079131296393 19

5363ad4cc05c30e0a5261c028812645a122e22ea20816678df02967c1b23bd72

EEAF0AB9ADB38DD69C33F80AFA8FC5E86072618775FF3C0B9EA2314C9C256576D674DF7496EA81D3383B4813D692C6E0E0D5D8E250B98BE48E495C1D6089DAD15DC7D7B46154D6B6CE8EF4AD69B15D4982559B297BCF1885C529F566660E57EC68EDBC3C05726CC02FD4CBF4976EAA9AFD5138FE8376435B9FC61D2FC0EB06E3

POSSIBLE SECRETS

1157920892373161954235709850086879078532699846656405640394575840079131296399355

0101BAF95C9723C57B6C21DA2EFF2D5ED588BDD5717E212F9D

91771529896554605945588149018382750217296858393520724172743325725474374979801

96341f1138933bc2f503fd44

14201174159756348119636828602231808974327613839524373876287257344192745939351271897363116607846760036084894662356762579528277471921224
19290710461342083806363940845126918288940005715246254452957693493567527289568315417754417631393844571917550968471078465956625479423122
93338483924514339614727760681880609734239

A335926AA319A27A1D00896A6773A4827ACDAC73

1AB597A5B4477F59E39539007C7F977D1A567B92B043A49C6B61984C3FE3481AAF454CD41BA1F051626442B3C10

0409487239995A5EE76B55F9C2F098A89CE5AF8724C0A23E0E0FF77500

6b016c3bdcf18941d0d654921475ca71a9db2fb27d1d37796185c2942c0a

c469684435deb378c4b65ca9591e2a5763059a2e

340E7BE2A280EB74E2BE61BADA745D97E8F7C300

683631961449557007844441656118272528951021708887614420550950512875503140832023

7CBBBCF9441CFAB76E1890E46884EAE321F70C0BCB4981527897504BEC3E36A62BCDFA2304976540F6450085F2DAE145C22553B465763689180EA2571867423E

0228F9D04E900069C8DC47A08534FE76D2B900B7D7EF31F5709F200C4CA205

POSSIBLE SECRETS

040060F05F658F49C1AD3AB1890F7184210EFD0987E307C84C27ACCFB8F9F67CC2C460189EB5AAAA62EE222EB1B35540CFE902374601E369050B7C4E42ACBA1DACBF04299C3460782F918EA427E6325165E9EA10E3DA5F6C42E9C55215AA9CA27A5863EC48D8E0286B

000E0D4D696E6768756151750CC03A4473D03679

470fa2b4ae81cd56ecbcda9735803434cec591fa

F5CE40D95B5EB899ABBCCFF5911CB8577939804D6527378B8C108C3D2090FF9BE18E2D33E3021ED2EF32D85822423B6304F726AA854BAE07D0396E9A9ADDC40F

7830A3318B603B89E2327145AC234CC594CBDD8D3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CA

2E2F85F5DD74CE983A5C4237229DAF8A3F35823BE

3d84f26c12238d7b4f3d516613c1759033b1a5800175d0b1

6A91174076B1E0E19C39C031FE8685C1CAE040E5C69A28EF

42941826148615804143873447737955502392672345968607143066798112994089471231420027060385216699563848719957657284814898909770759462613437669456364882730370838934791080835932647976778601915343474400961034231316672578686920482194932878633360203384797092684342247621055760235016132614780652761028509445403338652341

114ca50f7a8e2f3f657c1108d9d44cfd8

04009D73616F35F4AB1407D73562C10F00A52830277958EE84D1315ED31886

DB7C2ABF62E35E7628DFAC6561C5

07A11B09A76B562144418FF3FF8C2570B8

1A827EF00DD6FC0E234CAF046C6A5D8A85395B236CC4AD2CF32A0CADBDC9DDF620B0EB9906D0957F6C6FEACD615468DF104DE296CD8F

POSSIBLE SECRETS

MQVwithSHA384KDFAndSharedInfo

072546B5435234A422E0789675F432C89435DE5242

5a3c8ceabdec4a959f554bfaa7448f9f

047B6AA5D85E572983E6FB32A7CDEBC14027B6916A894D3AEE7106FE805FC34B44

00BDDB97E555A50A908E43B01C798EA5DAA6788F1EA2794EFCF57166B8C14039601E55827340BE

E2E31EDFC23DE7BDEBE241CE593EF5DE2295B7A9CBAEF021D385F7074CEA043AA27272A7AE602BF2A7B9033DB9ED3610C6FB85487EAE97AAC5BC7928C1950148

0432C4AE2C1F1981195F9904466A39C9948FE30BBFF2660BE1715A4589334C74C7BC3736A2F4F6779C59BDCEE36B692153D0A9877CC62A474002DF32E52139F0A0

22123dc2395a05caa7423daeccc94760a7d462256bd56916

9DEF3CAFB939277AB1F12A8617A47BBBDBA51DF499AC4C80BEEEA9614B19CC4D5F4F5F556E27CBDE51C6A94BE4607A291558903BA0D0F84380B655BB9A22E8DCDF028A7CEC67F0D08134B1C8B97989149B609E0BE3BAB63D47548381DBC5B1FC764E3F4B53DD9DA1158BFD3E2B9C8CF56EDF019539349627DB2FD53D24B7C48665772E437D6C7F8CE442734AF7CCB7AE837C264AE3A9BEB87F8A2FE9B8B5292E5A021FFF5E91479E8CE7A28C2442C6F315180F93499A234DCF76E3FED135F9BB

04B70E0CBD6BB4BF7F321390B94A03C1D356C21122343280D6115C1D21BD376388B5F723FB4C22DFE6CD4375A05A07476444D5819985007E34

108576C80499DB2FC16EDDF6853BBB278F6B6FB437D9

0163F35A5137C2CE3EA6ED8667190B0BC43ECD69977702709B

03188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012

57896044618658097711785492504343953927102133160255826820068844496087732066703

POSSIBLE SECRETS

FFFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3D
F1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB1
82B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9C
E98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99
C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE13098533C8B3FFFFFFFFFFFFFFFFFF

1854BEBDC31B21B7AEFC80AB0ECD10D5B1B3308E6DBF11C1

04640ECE5C12788717B9C1BA06CBC2A6FEBA85842458C56DDE9DB1758D39C0313D82BA51735CDB3EA499AA77A7D6943A64F7A3F25FE26F06B51BAA2696FA9035D
A5B534BD595F5AF0FA2C892376C84ACE1BB4E3019B71634C01131159CAE03CEE9D9932184BEEF216BD71DF2DADF86A627306ECFF96DBB8BACE198B61E00F8B332

04161FF7528B899B2D0C28607CA52C5B86CF5AC8395BAFEB13C02DA292DDED7A83

F518AA8781A8DF278ABA4E7D64B7CB9D49462353

FFFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1
356D6D51C245E485B576625E7EC6F44C42E9A63A3620FFFFFFFFFFFFFFFFFF

DB7C2ABF62E35E668076BEAD208B

0401A57A6A7B26CA5EF52FCDB816479700B3ADC94ED1FE674C06E695BABA1D

12511cfe811d0f4e6bc688b4d

002757A1114D696E6768756151755316C05E0BD4

C302F41D932A36CDA7A3463093D18DB78FCE476DE1A86294

10099790675505530477208181553592522486984108257205345787482351587557714799052927277724415285269929879648335669968284202797289605274717
317548059048560713474685214192868091256150280222218564753919090265611636784727014501906679429093018544621639973087222173288983032319409
735540321340097258832287685094674066396 2

POSSIBLE SECRETS

7BC86E2102902EC4D5890E8B6B4981ff27E0482750FEFC03

31a92ee2029fd10d901b113e990710f0d21ac6b6

027d29778100c65a1da1783716588dce2b8b4aee8e228f1896

5789604461865809771178549250434395392663499233282028201972879 2003956564823190

7BC382C63D8C150C3C72080ACE05AFA0C2BEA28E4FB22787139165EFBA91F90F8AA5814A503AD4EB04A8C7DD22CE2826

EE353FCA5428A9300D4ABA754A44C00FDFEC0C9AE4B1A1803075ED967B7BB73F

010090512DA9AF72B08349D98A5DD4C7B0532ECA51CE03E2D10F3B7AC579BD87E909AE40A6F131E9CFCE5BD967

B4050A850C04B3ABF54132565044B0B7D7BFD8BA270B39432355FFB4

29C41E568B77C617EFE5902F11DB96FA9613CD8D03DB08DA

DC9203E514A721875485A529D2C722FB187BC8980EB866644DE41C68E143064546E861C0E2C9EDD92ADE71F46FCF50FF2AD97F951FDA9F2A2EB6546F39689BD3

0236B3DAF8A23206F9C4F299D7B21A9C369137F2C84AE1AA0D

127971af8721782ecffa3

036b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

68A5E62CA9CE6C1C299803A6C1530B514E182AD8B0042A59CAD29F43

04DB4FF10EC057E9AE26B07D0280B7F4341DA5D1B1EAE06C7D9B2F2F6D9C5628A7844163D015BE86344082AA88D95E2F9D

POSSIBLE SECRETS

5037EA654196CFF0CD82B2C14A2FCF2E3FF8775285B545722F03EACDB74B

7B425ED097B425ED097B425ED097B425ED097B425ED097B4260B5E9C7710C864

11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

13D56FFAEC78681E68F9DEB43B35BEC2FB68542E27897B79

51DEF1815DB5ED74FCC34C85D709

b28ef557ba31dfcbdd21ac46e2a91e3c304f44cb87058ada2cb815151e610046

1f3bdba585295d9a1110d1df1f9430ef8442c5018976ff3437ef91b81dc0b8132c8d5c39c32d0e004a3092b7d327c0e7a4d26d2c7b69b58f9066652911e457779de

3FB32C9B73134D0B2E77506660EDBD484CA7B18F21EF205407F4793A1A0BA12510DBC15077BE463FFF4FED4AAC0BB555BE3A6C1B0C6B47B1BC3773BF7E8C6F6290
1228F8C28CBB18A55AE31341000A650196F931C77A57F2DDF463E5E9EC144B777DE62AAAB8A8628AC376D282D6ED3864E67982428EBC831D14348F6F2F9193B5045
AF2767164E1DFC967C1FB3F2E55A4BD1BFFE83B9C80D052B985D182EA0ADB2A3B7313D3FE14C8484B1E052588B9B7D2BBD2DF016199ECD06E1557CD0915B3353B
BB64E0EC377FD028370DF92B52C7891428CDC67EB6184B523D1DB246C32F63078490F00EF8D647D148D47954515E2327CFEF98C582664B4C0F6CC41659

5DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2

5FF6108462A2DC8210AB403925E638A19C1455D21

B4C4EE28CEBC6C2C8AC12952CF37F16AC7EFB6A9F69F4B57FFDA2E4F0DE5ADE038CBC2FFF719D2C18DE0284B8BFEF3B52B8CC7A5F5BF0A3C8D2319A5312557E1

03375D4CE24FDE434489DE8746E71786015009E66E38A926DD

0289FDFBE4ABE193DF9559ECF07AC0CE78554E2784EB8C1ED1A57A

115792089237316195423570985008687907853269984665640564039457584007913129639936

POSSIBLE SECRETS

D35E472036BC4FB7E13C785ED201E065F98FCFA6F6F40DEF4F92B9EC7893EC28FCD412B1F1B32E27

7ae96a2b657c07106e64479eac3434e99cf0497512f58995c1396c28719501ee

f76e0b3a-3e6b-4759-8841-c5360a9b6ffc

003088250CA6E7C7FE649CE85820F7

FFFFFFFE0000000075A30D1B9038A115

9ba48cba5ebcb9b6bd33b92830b2a2e0e192f10a

040D9029AD2C7E5CF4340823B2A87DC68C9E4CE3174C1E6EFDEE12C07D58AA56F772C0726F24C6B89E4ECDAC24354B9E99CAA3F6D3761402CD

5EEEFCA380D02919DC2C6558BB6D8A5D

04017232BA853A7E731AF129F22FF4149563A419C26BF50A4C9D6EEFAD612601DB537DECE819B7F70F555A67C427A8CD9BF18AEB9B56E0C11056FAE6A3

04C0A0647EAAB6A48753B033C56CB0F0900A2F5C4853375FD614B690866ABD5BB88B5F4828C1490002E6773FA2FA299B8F

E8C2505DEDFC86DDC1BD0B2B6667F1DA34B82574761CB0E879BD081CFD0B6265EE3CB090F30D27614CB4574010DA90DD862EF9D4EBEE4761503190785A71C760

10D9B4A3D9047D8B154359ABFB1B7F5485B04CEB868237DDC9DEDA982A679A5A919B626D4E50A8DD731B107A9962381FB5D807BF2618

04015D4860D088DDB3496B0C6064756260441CDE4AF1771D4DB01FFE5B34E59703DC255A868A1180515603AEAB60794E54BB7996A70061B1CFAB6BE5F32BBFA783
24ED106A7636B9C5A7BD198D0158AA4F5488D08F38514F1FDF4B4F40D2181B3681C364BA0273C706

9b6241c9-ad8a-4b71-ad0e-4986540784ea

5F49EB26781C0EC6B8909156D98ED435E45FD59918

POSSIBLE SECRETS

C2173F1513981673AF4892C23035A27CE25E2013BF95AA33B22C656F277E7335

c49d360886e704936a6678e1139d26b7819f7e90

10B51CC12849B234C75E6DD2028BF7FF5C1CE0D991A1

71169be7330b3038edb025f1d0f9

3DF91610A83441CAEA9863BC2DED5D5AA8253AA10A2EF1C98B9AC8B57F1117A72BF2C7B9E7C1AC4D77FC94CADC083E67984050B75EBAE5DD2809BD638016F723

fe0e87005b4e83761908c5131d552a850b3f58b749c37cf5b84d6768

8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B31F166E6CAC0425A7CF3AB6AF6B7FC3103B883202E9046565

7167EFC92BB2E3CE7C8AAAFF34E12A9C557003D7C73A6FAF003F99F6CC8482E540F7

023809B2B7CC1B28CC5A87926AAD83FD28789E81E2C9E3BF10

687D1B459DC841457E3E06CF6F5E2517B97C7D614AF138BCBF85DC806C4B289F3E965D2DB1416D217F8B276FAD1AB69C50F78BEE1FA3106EFB8CCBC7C5140116

1243ae1b4d71613bc9f780a03690e

02197B07845E9BE2D96ADB0F5F3C7F2CFFBD7A3EB8B6FEC35C7FD67F26DDF6285A644F740A2614

8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC50

AC4032EF4F2D9AE39DF30B5C8FFDAC506CDEBE7B89998CAF74866A08CFE4FFE3A6824A4E10B9A6F0DD921F01A70C4AFAAB739D7700C29F52C57DB17C620A8652BE5E9001A8D66AD7C17669101999024AF4D027275AC1348BB8A762D0521BC98AE247150422EA1ED409939D54DA7460CDB5F6C6B250717CBEF180EB34118E98D119529A45D6F834566E3025E316A330EFBB77A86F0C1AB15B051AE3D428C8F8ACB70A8137150B8EEB10E183EDD19963DDD9E263E4770589EF6AA21E7F5F2FF381B539CCE3409D13CD566AFBB48D6C019181E1BCFE94B30269EDFE72FE9B6AA4BD7B5A0F1C71CFFF4C19C418E1F6EC017981BC087F2A7065B384B890D3191F2BFA

POSSIBLE SECRETS

4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5

044BA30AB5E892B4E1649DD0928643ADCD46F5882E3747DEF36E956E97

04BED5AF16EA3F6A4F62938C4631EB5AF7BDBCDBC31667CB477A1A8EC338F94741669C976316DA6321

6EE3CEEB230811759F20518A0930F1A4315A827DAC

5789604461865809771178549250434395392663499233282028201972879200395656482319 3

9162fbe73984472a0a9d0590

393C7F7D53666B5054B5E6C6D3DE94F4296C0C599E2E2E241050DF18B6090BDC90186904968BB

324A6EDDD512F08C49A99AE0D3F961197A76413E7BE81A400CA681E09639B5FE12E59A109F78BF4A373541B3B9A1

02F40E7E2221F295DE297117B7F3D62F5C6A97FFCB8CEFF1CD6BA8CE4A9A18AD84FFABBD8EFA59332BE7AD6756A66E294AFD185A78FF12AA520E4DE739BACA0C7F
FEFF7F2955727A

004D696E67687561517512D8F03431FCE63B88F4

f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b5
47c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a

e8b4011604095303ca3b8099982be09fcb9ae616

B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF

00E0D2EE25095206F5E2A4F9ED229F1F256E79A0E2B455970D8D0D865BD94778C576D62F0AB7519CCD2A1A906AE30D

033C258EF3047767E7EDE0F1FDAA79DAEE3841366A132E163ACED4ED2401DF9C6BDCDE98E8E707C07A2239B1B097

POSSIBLE SECRETS

0400C6858E06B70404E9CD9E3ECB662395B4429C648139053FB521F828AF606B4D3DBAA14B5E77EFE75928FE1DC127A2FFA8DE3348B3C1856A429BF97E7E31C2E5BD66011839296A789A3BC0045C8A5FB42C7D1BD998F54449579B446817AFBD17273E662C97EE72995EF42640C550B9013FAD0761353C7086A272C24088BE94769FD16650

2E45EF571F00786F67B0081B9495A3D95462F5DE0AA185EC

416E6F6E796D6F75732053656E64657220202020

BDB6F4FE3E8B1D9E0DA8C0D40FC962195DFAE76F56564677

046B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C2964FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5

6127C24C05F38A0AAAF65C0EF02C

0667ACEB38AF4E488C407433FFAE4F1C811638DF20

07B6882CAAEFA84F9554FF8428BD88E246D2782AE2

00FD0D693149A118F651E6DCE6802085377E5F882D1B510B44160074C1288078365A0396C8E681

BD71344799D5C7FCDC45B59FA3B9AB8F6A948BC5

038D16C2866798B600F9F08BB4A8E860F3298CE04A5798

6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

4E13CA542744D696E67687561517552F279A8C84

C302F41D932A36CDA7A3462F9E9E916B5BE8F1029AC4ACC1

POSSIBLE SECRETS

70B5E1E14031C1F70BBEFE96BDDE66F451754B4CA5F48DA241F331AA396B8D1839A855C1769B1EA14BA53308B5E2723724E090E02DB9

027B680AC8B8596DA5A4AF8A19A0303FCA97FD7645309FA2A581485AF6263E313B79A2F5

AD107E1E9123A9D0D660FAA79559C51FA20D64E5683B9FD1B54B1597B61D0A75E6FA141DF95A56DBAF9A3C407BA1DF15EB3D688A309C180E1DE6B85A1274A0A66D3F8152AD6AC2129037C9EDEFDA4DF8D91E8FEF55B7394B7AD5B7D0B6C12207C9F98D11ED34DBF6C6BA0B2C8BBC27BE6A00E0A0B9C49708B3BF8A317091883681286130BC8985DB1602E714415D9330278273C7DE31EFDC7310F7121FD5A07415987D9ADC0A486DCDF93ACC44328387315D75E198C641A480CD86A1B9E587E8BE60E69CC928B2B9C52172E413042E9B23F10B0E16E79763C9B53DCF4BA80A29E3FB73C16B8E75B97EF363E2FFA31F71CF9DE5384E71B81C0AC4DFFE0C10E64F

10C0FB15760860DEF1EEF4D696E676875615175D

103FAEC74D696E676875615175777FC5B191EF30

c97445f45cdef9f0d3e05e1e585fc297235b82b5be8ff3efca67c59852018192

c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

4B337D934104CD7BEF271BF60CED1ED20DA14C08B3BB64F18A60888D

3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

340282366920938463463374607431768211456

B10B8F96A080E01DDE92DE5EAE5D54EC52C99FBCFB06A3C69A6A9DCA52D23B616073E28675A23D189838EF1E2EE652C013ECB4AEA906112324975C3CD49B83BFACCBDD7D90C4BD7098488E9C219A73724EFFD6FAE5644738FAA31A4FF55BCCC0A151AF5F0DC8B4BD45BF37DF365C1A65E68CFDA76D4DA708DF1FB2BC2E4A4371

1053CDE42C14D696E67687561517533BF3F83345

C49D360886E704936A6678E1139D26B7819F7E90

POSSIBLE SECRETS

b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae466748d9b5a536

D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FC

D7C134AA264366862A18302575D0FB98D116BC4B6DDEBCA3A5A7939F

e4437ed6010e88286f547fa90abfe4c42212

02120FC05D3C67A99DE161D2F4092622FECA701BE4F50F4758714E8A87BBF2A658EF8C21E7C5EFE965361F6C2999C0C247B0DBD70CE6B7

0108B39E77C4B108BED981ED0E890E117C511CF072

0405F939258DB7DD90E1934F8C70B0DFEC2EED25B8557EAC9C80E2E198F8CDBECD86B1205303676854FE24141CB98FE6D4B20D02B4516FF702350EDDB0826779C813F0DF45BE8112F4

BDDB97E555A50A908E43B01C798EA5DAA6788F1EA2794EFCF57166B8C14039601E55827340BE

026108BABB2CEEBCF787058A056CBE0CFE622D7723A289E08A07AE13EF0D10D171DD8D

801C0D34C58D93FE997177101F80535A4738CEBCBF389A99B36371EB

703900853520833051995477180190184378410795166300451804712843468443705633502619

e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf

0403F0EBA16286A2D57EA0991168D4994637E8343E3600D51FBC6C71A0094FA2CDD545B11C5C0C797324F1

E87579C11079F43DD824993C2CEE5ED3

36DF0AAFD8B8D7597CA10520D04B

POSSIBLE SECRETS

1270212482889324174659070427771764435257876535089165358128175072657050312609850984974231883334834011809259999951209889341306592056149967242541210492743493570749203127695614516892241105793112488126102296785346384016935200132889950003622606842227508135323070045173416336850045410625869714168836867788425378203883

13945487119911582560140965510769071310704170705992803179775800145437576535772298409412436852228823983303911468164807668823692122073732267216074074777170091113455043205380464769490468612011308781624074018480047704715733666292624942357124882396854222175366014339148568084052033685945849480318734128858048952516 3

00689918DBEC7E5A0DD6DFC0AA55C7

036768ae8e18bb92cfcf005c949aa2c6d94853d0e660bbf854b1c9505fe95a

f8183668ba5fc5bb06b5981e6d8b795d30b8978d43ca0ec572e37e09939a9773

724c1f27-9293-47a0-80d5-0add16edf2ac

6A941977BA9F6A435199ACFC51067ED587F519C5ECB541B8E44111DE1D40

A7F561E038EB1ED560B3D147DB782013064C19F27ED27C6780AAF77FB8A547CEB5B4FEF422340353

1C97BEFC54BD7A8B65ACF89F81D4D4ADC565FA45

04925BE9FB01AFC6FB4D3E7D4990010F813408AB106C4F09CB7EE07868CC136FFF3357F624A21BED5263BA3A7A27483EBF6671DBEF7ABB30EBEE084E58A0B077AD42A5A0989D1EE71B1B9BC0455FB0D2C3

60dcd2104c4cbc0be6eeefc2bdd610739ec34e317f9b33046c9e4788

2472E2D0197C49363F1FE7F5B6DB075D52B6947D135D8CA445805D39BC345626089687742B6329E70680231988

POSSIBLE SECRETS

E95E4A5F737059DC60DFC7AD95B3D8139515620C

617fab6832576cbbfed50d99f0249c3fee58b94ba0038c7ae84c8c832f2c

0100FAF51354E0E39E4892DF6E319C72C8161603FA45AA7B998A167B8F1E629521

70390085352083305199547718019018437841079516630045180471284346843705633502616

1340780792994259709957402499820584612747936582059239333772356144372176403007354697680187429816690342769003185818648605085375388281194656994643364900608409

FFFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DBE115974A3926F12FEE5E438777CB6A932DF8CD8BEC4D073B931BA3BC832B68D9DD300741FA7BF8AFC47ED2576F6936BA424663AAB639C5AE4F5683423B4742BF1C978238F16CBE39D652DE3FDB8BEFC848AD922222E04A4037C0713EB57A81A23F0C73473FC646CEA306B4BCBC8862F8385DDFA9D4B7FA2C087E879683303ED5BDD3A062B3CF5B3A278A66D2A13F83F44F82DDF310EE074AB6A364597E899A0255DC164F31CC50846851DF9AB48195DED7EA1B1D510BD7EE74D73FAF36BC31ECFA268359046F4EB879F924009438B481C6CD7889A002ED5EE382BC9190DA6FC026E479558E4475677E9AA9E3050E2765694DFC81F56E880B96E7160C980DD98EDD3DFFFFFFFFFFFFFFFFFFF

8CB91E82A3386D280F5D6F7E50E641DF152F7109ED5456B412B1DA197FB71123ACD3A729901D1A71874700133107EC53

4230017757A767FAE42398569B746325D45313AF0766266479B75654E65F

c39c6c3b3a36d7701b9c71a1f5804ae5d0003f4

POSSIBLE SECRETS
040356DCD8F2F95031AD652D23951BB366A80648F06D867940A5366D9E265DE9EB240F

PLAYSTORE INFORMATION

Title: Hello Heart • For heart health

Score: 4.7032967 **Installs:** 100,000+ **Price:** 0 **Android Version Support: Category:** Health & Fitness **Play Store URL:** com.helloheart.app.healthplan

Developer Details: Hello Heart, 6147608896752824064, None, https://www.helloheart.com, contact@helloheart.com,

Release Date: Oct 20, 2015 **Privacy Policy:** Privacy link

Description:

Provided by participating employers and health plans, Hello Heart is a FREE easy-to-use app that empowers you to improve your blood pressure and cholesterol with simple tracking, personalized insights, and daily tips and reminders. Check if your organization offers Hello Heart at https://join.helloheart.com More than 50% of people with high blood pressure lower it within 2 weeks of joining Hello Heart. ==How it works== Track Your Heart Health •Blood pressure •Pulse and potential irregular heartbeat •Lab results (e.g. cholesterol) •Activity •Medications •Weight Our FDA-cleared monitor connects with your phone via Bluetooth so you can track and see your blood pressure and heart rate readings right in the Hello Heart app. Easily import your cholesterol test results from your clinic and sync your Apple Health data, too. Understand Your Numbers Find out what high, low, or normal blood pressure may mean for your health. Manage Heart Disease Risks Tracking your blood pressure and cholesterol regularly can help you reduce your risk of developing chronic conditions like heart disease or even the event of a heart attack. Get Personalized Health Tips Heart health doesn't have to be hard. We think small lifestyle changes are the way to go. And we'll show you how with a heart healthy tip each time you log in. Protect Your Data We're committed to complying with HIPAA and adopt strict security standards to safeguard your data.

SCAN LOGS

Timestamp	Event	Error
2025-08-30 20:55:22	Generating Hashes	OK

2025-08-30 20:55:22	Extracting APK	OK
2025-08-30 20:55:22	Unzipping	OK
2025-08-30 20:55:23	Parsing APK with androguard	OK
2025-08-30 20:55:24	Extracting APK features using aapt/aapt2	OK
2025-08-30 20:55:24	Getting Hardcoded Certificates/Keystores	OK
2025-08-30 20:55:26	Parsing AndroidManifest.xml	OK
2025-08-30 20:55:26	Extracting Manifest Data	OK
2025-08-30 20:55:26	Manifest Analysis Started	OK
2025-08-30 20:55:27	Performing Static Analysis on: Hello Heart (com.helloheart.app.healthplan)	OK
2025-08-30 20:55:28	Fetching Details from Play Store: com.helloheart.app.healthplan	OK
2025-08-30 20:55:28	Checking for Malware Permissions	OK

2025-08-30 20:55:28	Fetching icon path	OK
2025-08-30 20:55:28	Library Binary Analysis Started	OK
2025-08-30 20:55:28	Reading Code Signing Certificate	OK
2025-08-30 20:55:29	Running APKiD 2.1.5	OK
2025-08-30 20:55:36	Detecting Trackers	OK
2025-08-30 20:55:41	Decompiling APK to Java with JADX	OK
2025-08-30 20:56:08	Converting DEX to Smali	OK
2025-08-30 20:56:08	Code Analysis Started on - java_source	OK
2025-08-30 20:56:13	Android SBOM Analysis Completed	OK
2025-08-30 20:56:25	Android SAST Completed	OK
2025-08-30 20:56:25	Android API Analysis Started	OK

2025-08-30 20:56:37	Android API Analysis Completed	OK
2025-08-30 20:56:38	Android Permission Mapping Started	OK
2025-08-30 20:56:52	Android Permission Mapping Completed	OK
2025-08-30 20:56:53	Android Behaviour Analysis Started	OK
2025-08-30 20:57:05	Android Behaviour Analysis Completed	OK
2025-08-30 20:57:05	Extracting Emails and URLs from Source Code	OK
2025-08-30 20:57:10	Email and URL Extraction Completed	OK
2025-08-30 20:57:10	Extracting String data from APK	OK
2025-08-30 20:57:10	Extracting String data from Code	OK
2025-08-30 20:57:10	Extracting String values and entropies from Code	OK
2025-08-30 20:57:15	Performing Malware check on extracted domains	OK

2025-08-30 20:57:17	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.