ANDROID STATIC ANALYSIS REPORT

Virta (2.83.0)

File Name:	com.participantapp_340028300.apk
Package Name:	com.participantapp
Scan Date:	Sept. 1, 2025, 7:04 a.m.
App Security Score:	61/100 (LOW RISK)
Grade:	A
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	INFO	✓ SECURE	HOTSPOT
0	16	4	3	2

FILE INFORMATION

File Name: com.participantapp_340028300.apk
Size: 22.22MB
MD5: 38748ef2e58c9d4837426fcf4d320582
SHA1: adc7e86e6a89246fb4f7c0961e26e5149c43184b
SHA256: a2e9e0dea1cabdab417adf387c3fb23626105600b4c027590549d5cd01b65847

APP INFORMATION

App Name: Virta
Package Name: com.participantapp
Main Activity: com.participantapp.SplashActivity
Target SDK: 34
Min SDK: 28
Max SDK:
Android Version Name: 2.83.0

Android Version Code: 340028300

APP COMPONENTS

Activities: 11
Services: 7
Receivers: 11
Providers: 8
Exported Activities: 1
Exported Services: 0
Exported Receivers: 5
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-05-06 05:54:23+00:00
Valid To: 2049-05-06 05:54:23+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xbaa9772653e5bf0ab303bd53335a7c137431b373
Hash Algorithm: sha256
md5: bf159c3a096fa5f51a678903b91c02f7
sha1: 578ca06eaf50925c6dba7463fbfd7a84a0fc0804
sha256: db7a8c292719dc2ceef143aad51c7b737e734cfa7a1af766a09222c5bb13d58b
sha512: acc142335bf43d7ed3245e1c8262d05f2b39d56a7806afc2174ebb8650593e5d9c72814fa22210dd968c11a5a92d6ce06e81a53e2dd75df924b41b7ca4e08a2c
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: a2dc94f2c8db571c1801a3200b28cfede08c87829147119060286 6dc29eff528
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.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.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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.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.

APKID ANALYSIS

FILE	DETAILS

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

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

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

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.participantapp.MainActivity	Schemes: virtahealth://, https://, Hosts: my.virtahealth.com, ablink.e.virtahealth.com, ablink.updates.virtahealth.com,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	virtahealth.axomo.com	info	Domain config is configured to trust bundled certs @raw/gd_bundle_g2.

CERTIFICATE ANALYSIS

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

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

MANIFEST ANALYSIS

HIGH: **0** | WARNING: **7** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Activity (com.participantapp.MainActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Broadcast Receiver (com.dieam.reactnativepushnotification.modules.RNPushNotificationActions) 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.
5	Broadcast Receiver (com.dieam.reactnativepushnotification.modules.RNPushNotificationPublisher) 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.
6	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
7	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
8	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.

CODE ANALYSIS

HIGH: **0** | WARNING: **7** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/RNFetchBlob/RNFetchBlobReq.java com/airbnb/android/react/lottie/LottieAnimationViewManager.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java com/amplitude/experiment/reactnative/LogcatLogger.java com/amplitude/reactnative/LogcatLogger.java com/aurelhubert/ahbottomnavigation/AHBottomNavigation.java com/braze/support/BrazeLogger.java com/brentvatne/react/ReactVideoView.java com/dieam/reactnativepushnotification/helpers/ApplicationBadgeHelper.java com/dieam/reactnativepushnotification/modules/RNPushNotification.java com/dieam/reactnativepushnotification/modules/RNPushNotificationActions.java com/dieam/reactnativepushnotification/modules/RNPushNotificationAttributes.java com/dieam/reactnativepushnotification/modules/RNPushNotificationBootEventReceiver.java com/dieam/reactnativepushnotification/modules/RNPushNotificationConfig.java com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java com/dieam/reactnativepushnotification/modules/RNPushNotificationListenerService.java com/dieam/reactnativepushnotification/modules/RNPushNotificationPicturesAggregator.java com/dieam/reactnativepushnotification/modules/RNPushNotificationPublisher.java com/dieam/reactnativepushnotification/modules/RNReceivedMessageHandler.java com/emeraldsanto/encryptedstorage/RNEncryptedStorageModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/horcrux/svg/Brush.java com/horcrux/svg/ClipPathView.java com/horcrux/svg/ImageView.java com/horcrux/svg/LinearGradientView.java com/horcrux/svg/MaskView.java com/horcrux/svg/PatternView.java com/horcrux/svg/RadialGradientView.java com/horcrux/svg/UseView.java com/horcrux/svg/VirtualView.java com/imagepicker/ImageMetadata.java com/imagepicker/Metadata.java com/imagepicker/VideoMetadata.java com/ketomojo/sdk/device/taidoc/parsers/TaiDocRecordsParser.java com/ketomojo/sdk/device/vivachek/parsers/VivaCheckRecordsParser.java com/launchdarkly/sdk/android/LDAndroidLogging.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/RNInstallReferrerClient.java com/learnium/RNDeviceInfo/resolver/DeviceIdResolver.java com/lugg/RNCConfig/RNCConfigModule.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/RxBleAdapterState

NO	ISSUE	SEVERITY	STANDARDS	FILES
				Observable.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 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

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	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/UUIDUtil.java com/proyecto26/inappbrowser/RNInAppBrowser.java com/reactcommunity/rndatetimepicker/MinuteIntervalSnappableTimePickerDialog.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/reactnativecommunity/cookies/CookieManagerModule.java com/reactnativecommunity/webview/RNCWebViewManager.java com/reactnativelocationenabler/LocationEnablerModule$requestDeviceResolutionLocationSettings$1.java com/reactnativenavigation/react/DevPermissionRequest.java com/reactnativenavigation/react/events/EventEmitter.java com/reactnativenavigation/utils/LogKt.java com/reactnativenavigation/utils/Time.java com/reactnativenavigation/utils/WindowInsetsUtils.java com/reactnativenavigation/viewcontrollers/stac

NO	ISSUE	SEVERITY	STANDARDS	FILES
				k/topbar/button/IconResolver.java com/reactnativenavigation/views/sidemenu/SideMenu.java com/rnketomojo/DeviceManagerModule.java com/rnketomojo/EventEmitter.java com/swmansion/gesturehandler/react/RNGestureHandlerRootHelper.java com/swmansion/gesturehandler/react/RNGestureHandlerRootView.java com/swmansion/reanimated/NativeMethodsHelper.java com/swmansion/reanimated/NativeProxy.java com/swmansion/reanimated/ReanimatedJSIModulePackage.java com/swmansion/reanimated/ReanimatedModule.java com/swmansion/reanimated/layoutReanimation/AnimationsManager.java com/swmansion/reanimated/layoutReanimation/ReanimatedNativeHierarchyManager.java com/swmansion/reanimated/nodes/DebugNode.java com/swmansion/reanimated/sensor/ReanimatedSensorContainer.java com/swmansion/rnscreens/ScreenStackHeaderConfigViewManager.java com/swmansion/rnscreens/ScreensModule.java com/swmansion/rnscreens/SearchBarManager.java com/th3rdwave/safeareacontext/SafeAreaView.java com/zoontek/rnpermissions/RNPermissionsModule.java de/patwoz/rn/bluetoothstatemanager/RNBluetoothStateManagerModule.java expo/modules/ExpoModulesPackage.java expo/modules/adapters/react/services/UIManagerModuleWrapper.java expo/modules/adapters/react/views/ViewManagerAdapterUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				expo/modules/application/ApplicationModule.java expo/modules/apploader/AppLoaderProvider.java expo/modules/constants/ConstantsService.java expo/modules/constants/ExponentInstallationId.java expo/modules/filesystem/FileSystemModule.java expo/modules/securestore/AuthenticationHelper.java expo/modules/securestore/SecureStoreModule.java io/invertase/firebase/RNFirebaseModule.java io/invertase/firebase/Utils.java io/invertase/firebase/admob/RNFirebaseAdMob.java io/invertase/firebase/analytics/RNFirebaseAnalytics.java io/invertase/firebase/auth/RNFirebaseAuth.java io/invertase/firebase/config/RNFirebaseRemoteConfig.java io/invertase/firebase/database/RNFirebaseDatabase.java io/invertase/firebase/database/RNFirebaseDatabaseReference.java io/invertase/firebase/database/RNFirebaseDatabaseUtils.java io/invertase/firebase/fabric/crashlytics/RNFirebaseCrashlytics.java io/invertase/firebase/firestore/FirestoreSerialize.java io/invertase/firebase/firestore/RNFirebaseFirestore.java io/invertase/firebase/firestore/RNFirebaseFirestoreCollectionReference.java io/invertase/firebase/firestore/RNFirebaseFirestoreDocumentReference.java io/invertase/firebase/functions/RNFirebaseFunctions.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				io/invertase/firebase/instanceid/RNFirebaseInstanceId.java io/invertase/firebase/links/RNFirebaseLinks.java io/invertase/firebase/messaging/RNFirebaseMessaging.java io/invertase/firebase/messaging/RNFirebaseMessagingService.java io/invertase/firebase/notifications/DisplayNotificationTask.java io/invertase/firebase/notifications/RNFirebaseNotificationManager.java io/invertase/firebase/notifications/RNFirebaseNotifications.java io/invertase/firebase/notifications/RNFirebaseNotificationsRebootReceiver.java io/invertase/firebase/perf/RNFirebasePerformance.java io/invertase/firebase/storage/RNFirebaseStorage.java io/sentry/SystemOutLogger.java io/sentry/android/core/AndroidLogger.java io/sentry/transport/StdoutTransport.java me/leolin/shortcutbadger/ShortcutBadger.java org/greenrobot/eventbus/Logger.java org/greenrobot/eventbus/util/ErrorDialogConfig.java org/greenrobot/eventbus/util/ErrorDialogManager.java org/greenrobot/eventbus/util/ExceptionToResourceMapping.java org/slf4j/helpers/Util.java timber/log/Timber.java
				android/content/SdkAuthenticationCache.java com/amplitude/reactnative/AmplitudeReactNativeModule.java com/appboy/Constants.java com/appboy/enums/CardKey.java com/appboy/models/outgoing/AttributionData.java com/appboy/models/outgoing/FacebookUser.java com/appboy/models/outgoing/TwitterUser.java com/braze/Constants.java com/braze/configuration/BrazeConfig.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/braze/models/inappmessage/InAppMessageHtml.java com/braze/push/BrazeNotificationUtils.java com/braze/push/BrazePushReceiver.java com/braze/support/StringUtils.java com/braze/ui/contentcards/ContentCardsFragment.java com/braze/ui/inappmessage/listeners/DefaultInAppMessageWebViewClientListener.java com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java com/launchdarkly/sdk/android/DiagnosticStore.java com/launchdarkly/sdk/android/LDClient.java com/launchdarkly/sdk/android/LDConfig.java com/launchdarkly/sdk/android/SharedPrefsFlagStore.java com/launchdarkly/sdk/android/SharedPrefsFlagStoreManager.java com/launchdarkly/sdk/android/SharedPrefsSummaryEventStore.java com/oblador/keychain/KeychainModule.java com/participantapp/BuildConfig.java com/reactnativenavigation/options/params/ThemeColourKt.java com/reactnativenavigation/react/Constants.java com/rnketomojo/DeviceManagerKeys.java expo/modules/adapters/react/NativeModulesProxy.java expo/modules/constants/ExponentInstallationId.java expo/modules/errorrecovery/ErrorRecoveryModuleKt.java expo/modules/filesystem/FileSystemModuleKt.java expo/modules/interfaces/permissions/PermissionsResponse.java io/invertase/firebase/functions/RNFirebaseFunctions.java io/invertase/firebase/notifications/RNFirebaseN

NO	ISSUE	SEVERITY	STANDARDS	FILES
				otificationManager.java io/invertase/firebase/notifications/RNFirebaseNotifications.java io/reactivex/internal/schedulers/SchedulerPoolFactory.java io/sentry/Baggage.java io/sentry/RequestDetailsResolver.java io/sentry/TraceContext.java io/sentry/protocol/User.java
3	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	android/content/a0.java android/content/a5.java android/content/c6.java android/content/e.java android/content/e1.java android/content/j1.java android/content/k0.java android/content/k6.java android/content/l.java android/content/l0.java android/content/l4.java android/content/m.java android/content/m0.java android/content/n6.java android/content/r1.java android/content/t6.java android/content/v3.java android/content/x0.java com/braze/configuration/RuntimeAppConfigurationProvider.java expo/modules/adapters/react/permissions/PermissionsService.java expo/modules/constants/ExponentInstallationId.java expo/modules/errorrecovery/ErrorRecoveryModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/RNFetchBlob/RNFetchBlobFS.java com/RNFetchBlob/Utils/PathResolver.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/reactnativecommunity/webview/RNCWebViewModule.java io/invertase/firebase/storage/RNFirebaseStorage.java io/sentry/android/core/DefaultAndroidEventProcessor.java
5	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/DefaultAndroidEventProcessor.java io/sentry/android/core/internal/util/RootChecker.java
6	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/RNFetchBlob/RNFetchBlobBody.java com/reactnativecommunity/webview/RNCWebViewModule.java
7	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	io/sentry/android/core/internal/util/RootChecker.java
8	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/braze/support/StringUtils.java expo/modules/filesystem/FileSystemModule.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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	android/content/d1.java com/braze/support/IntentUtils.java
10	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/RNFetchBlob/RNFetchBlobReq.java com/launchdarkly/eventsource/EventSource.java
11	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/RNFetchBlob/RNFetchBlob.java com/RNFetchBlob/RNFetchBlobReq.java com/braze/Braze.java com/braze/push/BrazeNotificationUtils.java com/braze/ui/support/UriUtils.java com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java com/proyecto26/inappbrowser/RNInAppBrowser.java expo/modules/adapters/react/permissions/PermissionsService.java expo/modules/filesystem/FileSystemModule.java io/invertase/firebase/links/RNFirebaseLinks.java io/invertase/firebase/notifications/RNFirebaseNotificationManager.java me/leolin/shortcutbadger/impl/OPPOHomeBader.java me/leolin/shortcutbadger/impl/SonyHomeBadger.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/proyecto26/inappbrowser/RNInAppBrowser.java expo/modules/adapters/react/permissions/PermissionsService.java
00036	Get resource file from res/raw directory	reflection	com/braze/push/BrazeNotificationUtils.java com/braze/ui/support/UriUtils.java com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java com/proyecto26/inappbrowser/RNInAppBrowser.java expo/modules/adapters/react/permissions/PermissionsService.java expo/modules/filesystem/FileSystemModule.java io/invertase/firebase/notifications/RNFirebaseNotificationManager.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

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	android/content/c6.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/braze/Braze.java com/braze/images/DefaultBrazeImageLoader.java com/braze/support/BrazeFileUtils.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java com/launchdarkly/sdk/android/HttpFeatureFlagFetcher.java com/launchdarkly/sdk/android/SharedPrefsFlagStore.java expo/modules/filesystem/FileSystemModule.java io/invertase/firebase/storage/RNFirebaseStorage.java io/sentry/DirectoryProcessor.java io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/SentryOptions.java io/sentry/android/core/AndroidOptionsInitializer.java io/sentry/android/core/DefaultAndroidEventProcessor.java io/sentry/android/core/cache/AndroidEnvelopeCache.java io/sentry/cache/CacheStrategy.java io/sentry/cache/EnvelopeCache.java io/sentry/instrumentation/file/FileIOSpanManager.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	android/content/n0.java com/RNFetchBlob/RNFetchBlobBody.java com/RNFetchBlob/RNFetchBlobFS.java com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/braze/support/BrazeImageUtils.java com/braze/support/WebContentUtils.java com/imagepicker/VideoMetadata.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java expo/modules/filesystem/FileSystemModule.java io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/SentryEnvelopeItem.java io/sentry/cache/CacheStrategy.java io/sentry/cache/EnvelopeCache.java io/sentry/config/FilesystemPropertiesLoader.java io/sentry/instrumentation/file/FileInputStreamInitData.java io/sentry/instrumentation/file/SentryFileInputStream.java okio/Okio__JvmOkioKt.java
00091	Retrieve data from broadcast	collection	com/braze/push/BrazeNotificationUtils.java com/dieam/reactnativepushnotification/modules/RNPushNotification.java com/dieam/reactnativepushnotification/modules/RNPushNotificationPublisher.java io/invertase/firebase/notifications/RNFirebaseBackgroundNotificationActionReceiver.java io/invertase/firebase/notifications/RNFirebaseNotifications.java

RULE ID	BEHAVIOUR	LABEL	FILES
00012	Read data and put it into a buffer stream	file	expo/modules/filesystem/FileSystemModule.java io/sentry/EnvelopeSender.java io/sentry/OutboxSender.java io/sentry/SentryEnvelopeItem.java io/sentry/cache/CacheStrategy.java io/sentry/cache/EnvelopeCache.java io/sentry/config/FilesystemPropertiesLoader.java
00078	Get the network operator name	collection telephony	android/content/l0.java com/amplitude/experiment/reactnative/AndroidContextProvider.java com/amplitude/reactnative/AndroidContextProvider.java com/learnium/RNDeviceInfo/RNDeviceModule.java
00137	Get last known location of the device	location collection	com/amplitude/experiment/reactnative/AndroidContextProvider.java
00115	Get last known location of the device	collection location	com/amplitude/experiment/reactnative/AndroidContextProvider.java
00132	Query The ISO country code	telephony collection	com/amplitude/experiment/reactnative/AndroidContextProvider.java com/amplitude/reactnative/AndroidContextProvider.java
00033	Query the IMEI number	collection	android/content/l0.java
00083	Query the IMEI number	collection telephony	android/content/l0.java
00175	Get notification manager and cancel notifications	notification	com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java io/invertase/firebase/notifications/RNFirebaseNotificationManager.java
00189	Get the content of a SMS message	sms	com/RNFetchBlob/Utils/PathResolver.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java

RULE ID	BEHAVIOUR	LABEL	FILES
00192	Get messages in the SMS inbox	sms	com/RNFetchBlob/Utils/PathResolver.java io/invertase/firebase/notifications/RNFirebaseNotificationManager.java
00188	Get the address of a SMS message	sms	com/RNFetchBlob/Utils/PathResolver.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 me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00200	Query data from the contact list	collection contact	com/RNFetchBlob/Utils/PathResolver.java me/leolin/shortcutbadger/impl/SamsungHomeBadger.java
00201	Query data from the call log	collection calllog	com/RNFetchBlob/Utils/PathResolver.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
00043	Calculate WiFi signal strength	collection wifi	com/reactnativecommunity/netinfo/ConnectivityReceiver.java
00147	Get the time of current location	collection location	android/content/o.java
00075	Get location of the device	collection location	android/content/o.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/learnium/RNDeviceInfo/RNDeviceModule.java

RULE ID	BEHAVIOUR	LABEL	FILES
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
00009	Put data in cursor to JSON object	file	com/amplitude/reactnative/LegacyDatabaseStorage.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java
00024	Write file after Base64 decoding	reflection file	com/RNFetchBlob/RNFetchBlobBody.java com/RNFetchBlob/RNFetchBlobFS.java expo/modules/filesystem/FileSystemModule.java
00096	Connect to a URL and set request method	command network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java io/sentry/transport/HttpConnection.java
00089	Connect to a URL and receive input stream from the server	command network	io/invertase/firebase/notifications/DisplayNotificationTask.java io/sentry/transport/HttpConnection.java
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java io/invertase/firebase/notifications/DisplayNotificationTask.java io/sentry/transport/HttpConnection.java
00109	Connect to a URL and get the response code	network command	io/sentry/transport/HttpConnection.java
00123	Save the response to JSON after connecting to the remote server	network command	android/content/t1.java

RULE ID	BEHAVIOUR	LABEL	FILES
00016	Get location info of the device and put it to JSON object	location collection	android/content/BrazeLocation.java
00121	Create a directory	file command	expo/modules/filesystem/FileSystemModule.java
00125	Check if the given file path exist	file	expo/modules/filesystem/FileSystemModule.java
00104	Check if the given path is directory	file	expo/modules/filesystem/FileSystemModule.java
00187	Query a URI and check the result	collection sms calllog calendar	me/leolin/shortcutbadger/impl/SamsungHomeBadger.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://api-5365043775856208119-921138.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/1047391090444/namespaces/firebase:fetch?key=AIzaSyDfUCBK880X2x6Ohcsf6PaFa-fhaiq_M80. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.CAMERA, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_FINE_LOCATION
Other Common Permissions	4/44	android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
mobile.launchdarkly.com	ok	**IP:** 35.153.82.190 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
android.googlesource.com	ok	**IP:** 64.233.165.82 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
virtahealth.zendesk.com	ok	**IP:** 216.198.53.6 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
www.slf4j.org	ok	**IP:** 159.100.250.151 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.braze.com	ok	**IP:** 104.17.227.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
clientsdk.launchdarkly.com	ok	**IP:** 151.101.1.55 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sdk.iad-01.braze.com	ok	**IP:** 104.18.39.68 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
api-5365043775856208119-921138.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sondheim.braze.com	ok	**IP:** 104.18.43.4 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
my.virtahealth.com	ok	**IP:** 34.120.184.98 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
clientstream.launchdarkly.com	ok	**IP:** 13.248.151.210 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
github.com	ok	**IP:** 140.82.114.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

TRACKERS

TRACKER	CATEGORIES	URL
Amplitude	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/125
Braze (formerly Appboy)	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/17
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

HARDCODED SECRETS

POSSIBLE SECRETS
"AMPLITUDE_API_KEY" : "6c1190b7d5dd6db04ec9b9608964d870"
"AMPLITUDE_EXPERIMENT_DEPLOYMENT_KEY" : "client-XO7jyByGxkCwyZiIb69yew7TYTJlO16b"
"BRAZE_API_KEY_ANDROID" : "bb5d3ae2-e275-4261-b4f2-f7ab9efedb92"
"BRAZE_API_KEY_IOS" : "2414af5d-a92b-458e-953a-542f4b178242"
"com_braze_api_key" : "bb5d3ae2-e275-4261-b4f2-f7ab9efedb92"
"com_braze_firebase_cloud_messaging_sender_id" : "1047391090444"

POSSIBLE SECRETS
"com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key"
"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"
"com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key"
"firebase_database_url" : "https://api-5365043775856208119-921138.firebaseio.com"
"google_api_key" : "AIzaSyDfUCBK880X2x6Ohcsf6PaFa-fhaiq_M80"
"google_crash_reporting_api_key" : "AIzaSyDfUCBK880X2x6Ohcsf6PaFa-fhaiq_M80"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
68647976601306097149819007990813932172694353001433054093944634591855431833976560521225596406614545549772963113914808580371219879997166438125740282911150571 51
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394 2643
00001523-1212-efde-1523-785feabcd123
37a6259cc0c1dae299a7866489dff0bd
4c6651a25ec5f03e5bd0

POSSIBLE SECRETS
00C0C101C30302C2C60607C705C5C404CC0C0DCD0FCFCE0E0ACACB0BC90908C8D81819D91BDBDA1A1EDEDF1FDD1D1CDC14D4D515D71716D6D21213D311D1D010F03031F133F3F23236F6F737F53534F43CFCFD3DFF3F3EFEFA3A3BFB39F9F83828E8E929EB2B2AEAEE2E2FEF2DEDEC2CE42425E527E7E62622E2E323E12120E0A06061A163A3A26266A6A767A56564A46CACAD6DAF6F6EAEAA6A6BAB69A9A86878B8B979BB7B7ABABE7E7FBF7DBDBC7CB47475B577B7B67672B2B373B17170B0509091519353529296565797559594549C5C5D9D5F9F9E5E5A9A9B5B99595898884849894B8B8A4A4E8E8F4F8D4D4C8C44848545874746868242438341818040
bb5d3ae2-e275-4261-b4f2-f7ab9efedb92
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
00001524-1212-efde-1523-785feabcd123
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
B3EEABB8EE11C2BE770B684D95219ECB
6c1190b7d5dd6db04ec9b9608964d870
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe814112031408f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
-efde-1523-785feabcd123
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
01360240043788015936020505

POSSIBLE SECRETS
115792089210356248762697446949407573530086143415290314195533631308867097853951
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
33b1dfd615b4a7b2e66b37a153d78be28076d3289640ac19
2414af5d-a92b-458e-953a-542f4b178242
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: Virta Health

Score: 2.5643563 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.participantapp

Developer Details: Virta Health, Virta+Health, None, http://www.virtahealth.com, support@virtahealth.com,

Release Date: Jun 18, 2019 **Privacy Policy:** Privacy link

Description:

Virta is a life-changing program to lose weight and reverse type 2 diabetes. Our proven approach transforms the way your body fuels itself, using real food. Get expert care in the palm of your hand. With Virta, you can: • View a daily action plan tailored to your health goals. • Track progress with a connected weight scale and blood meter. • Message your dedicated care team anytime. • Receive all the supplies you need, shipped to your door. • Get inspired with recipes, food plans, videos, and more. • Connect with a private community for ongoing support. Not a member yet? Visit https://www.virtahealth.com/join to learn more and apply. About Virta Health: Virta empowers you with the support, tools, and knowledge needed to lose weight, reverse type 2 diabetes, and reduce unwanted medications. Our evidence-based approach resets your metabolism by changing what you eat, with a nutrition plan tailored to you by your dedicated care team. A connected weight scale and blood glucose meter make tracking your progress seamless and accessible directly on your smartphone. You'll receive continuous support and guidance from your health coach, medical provider, and comprehensive app to sustainably transform your health. Learn how our unique approach has helped thousands of members reimagine what's possible at www.virtahealth.com.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 07:04:06	Generating Hashes	OK
2025-09-01 07:04:07	Extracting APK	OK
2025-09-01 07:04:07	Unzipping	OK
2025-09-01 07:04:10	Parsing APK with androguard	OK
2025-09-01 07:04:11	Extracting APK features using aapt/aapt2	OK
2025-09-01 07:04:11	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 07:04:13	Parsing AndroidManifest.xml	OK
2025-09-01 07:04:13	Extracting Manifest Data	OK
2025-09-01 07:04:13	Manifest Analysis Started	OK

2025-09-01 07:04:14	Reading Network Security config from network_security_config.xml	OK
2025-09-01 07:04:14	Parsing Network Security config	OK
2025-09-01 07:04:14	Performing Static Analysis on: Virta (com.participantapp)	OK
2025-09-01 07:04:15	Fetching Details from Play Store: com.participantapp	OK
2025-09-01 07:04:17	Checking for Malware Permissions	OK
2025-09-01 07:04:17	Fetching icon path	OK
2025-09-01 07:04:17	Library Binary Analysis Started	OK
2025-09-01 07:04:17	Reading Code Signing Certificate	OK
2025-09-01 07:04:18	Running APKiD 2.1.5	OK
2025-09-01 07:04:20	Detecting Trackers	OK
2025-09-01 07:04:24	Decompiling APK to Java with JADX	OK

2025-09-01 07:04:43	Converting DEX to Smali	OK
2025-09-01 07:04:43	Code Analysis Started on - java_source	OK
2025-09-01 07:04:46	Android SBOM Analysis Completed	OK
2025-09-01 07:04:53	Android SAST Completed	OK
2025-09-01 07:04:53	Android API Analysis Started	OK
2025-09-01 07:04:59	Android API Analysis Completed	OK
2025-09-01 07:04:59	Android Permission Mapping Started	OK
2025-09-01 07:05:07	Android Permission Mapping Completed	OK
2025-09-01 07:05:07	Android Behaviour Analysis Started	OK
2025-09-01 07:05:14	Android Behaviour Analysis Completed	OK
2025-09-01 07:05:14	Extracting Emails and URLs from Source Code	OK

2025-09-01 07:05:18	Email and URL Extraction Completed	OK
2025-09-01 07:05:18	Extracting String data from APK	OK
2025-09-01 07:05:18	Extracting String data from Code	OK
2025-09-01 07:05:18	Extracting String values and entropies from Code	OK
2025-09-01 07:05:22	Performing Malware check on extracted domains	OK
2025-09-01 07:05:24	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.