



ANDROID STATIC ANALYSIS REPORT

No icon

 TruHearing App (2.6.80.15240)

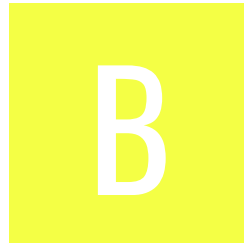
File Name: com.truhearing.rta_1524000000.apk

Package Name: com.truhearing.rta

Scan Date: Sept. 1, 2025, 10:42 a.m.






App Security Score: 47/100 (MEDIUM RISK)

Grade:



Trackers Detection: 2/432

FINDINGS SEVERITY

|  HIGH |  MEDIUM |  INFO |  SECURE |  HOTSPOT |
|--|--|--|--|---|
| 2 | 8 | 4 | 1 | 1 |

FILE INFORMATION

File Name: com.truhearing.rta_1524000000.apk

Size: 163.96MB

MD5: 5b20c70ee3886973d8255473a6ce0677

SHA1: 90d3b1e1c62e68e94fb6693a4d88464065787c5e

SHA256: b9dd2f783a5262ee29a2607d0144ae8410e9c7bceec5890586ed22fa00a76688

APP INFORMATION

App Name: TruHearing App

Package Name: com.truhearing.rta

Main Activity: crc64f4a174aab082e202.MainActivity

Target SDK: 34

Min SDK: 29

Max SDK:

Android Version Name: 2.6.80.15240

Android Version Code: 1524000000

APP COMPONENTS

Activities: 12

Services: 7

Receivers: 6

Providers: 6

Exported Activities: 1

Exported Services: 0

Exported Receivers: 2

Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed

v1 signature: False

v2 signature: False

v3 signature: True

v4 signature: False

X.509 Subject: C=DE, ST=Bavaria, L=Erlangen, O=Sivantos GmbH, OU=Unknown, CN=Code Signing Sivantos GmbH

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2015-09-24 11:34:54+00:00

Valid To: 2070-06-27 11:34:54+00:00

Issuer: C=DE, ST=Bavaria, L=Erlangen, O=Sivantos GmbH, OU=Unknown, CN=Code Signing Sivantos GmbH

Serial Number: 0x5603dfde

Hash Algorithm: sha1

md5: 6c68174d47edd8bdae5273d36de2d89a

sha1: c24a9888aef54ce2070234e9763bfb59d2a4dab6

sha256: 9b2eb7ce3b3b2cee3fe7b06d2d40da8ffae9c772d135eb887bd321cfe7be21ce

sha512: cd240e0b4a0ff45b11ceb5bfa7a357c0ac06e469a44c7c5cf73f7e5108cd856d0b918d06cca5f4717e9f731f702d182d9e40067fb38f6bac17d7aab6643baf3b

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 841360f54e4c36825eaecad39dcf2e8b509e1a1241de4e7e820f29fd167338d0

Found 1 unique certificates

☰ APPLICATION PERMISSIONS

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|-----------|--|--|
| android.permission.ACCESS_COARSE_LOCATION | dangerous | coarse (network-based) location | Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are. |
| android.permission.ACCESS_FINE_LOCATION | dangerous | fine (GPS) location | Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power. |
| android.permission.ACTIVITY_RECOGNITION | dangerous | allow application to recognize physical activity | Allows an application to recognize physical activity. |
| android.permission.ACCESS_NETWORK_STATE | normal | view network status | Allows an application to view the status of all networks. |
| android.permission.INTERNET | normal | full Internet access | Allows an application to create network sockets. |
| android.permission.READ_PHONE_STATE | dangerous | read phone state and identity | Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|-----------|---|--|
| android.permission.MODIFY_AUDIO_SETTINGS | normal | change your audio settings | Allows application to modify global audio settings, such as volume and routing. |
| android.permission.BLUETOOTH | normal | create Bluetooth connections | Allows applications to connect to paired bluetooth devices. |
| android.permission.BLUETOOTH_ADMIN | normal | bluetooth administration | Allows applications to discover and pair bluetooth devices. |
| android.permission.BLUETOOTH_SCAN | dangerous | required for discovering and pairing Bluetooth devices. | Required to be able to discover and pair nearby Bluetooth devices. |
| android.permission.BLUETOOTH_CONNECT | dangerous | necessary for connecting to paired Bluetooth devices. | Required to be able to connect to paired Bluetooth devices. |
| android.permission.USE_FULL_SCREEN_INTENT | normal | required for full screen intents in notifications. | Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents. |
| android.permission.WAKE_LOCK | normal | prevent phone from sleeping | Allows an application to prevent the phone from going to sleep. |
| android.permission.VIBRATE | normal | control vibrator | Allows the application to control the vibrator. |
| android.permission.CAMERA | dangerous | take pictures and videos | Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time. |
| android.permission.RECORD_AUDIO | dangerous | record audio | Allows application to access the audio record path. |

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|-----------|--|---|
| android.permission.SET_ALARM | normal | set alarm in alarm clock | Allows the application to set an alarm in an installed alarm clock application. Some alarm clock applications may not implement this feature. |
| android.permission.GET_ACCOUNTS | dangerous | list accounts | Allows access to the list of accounts in the Accounts Service. |
| android.permission.FOREGROUND_SERVICE | normal | enables regular apps to use Service.startForeground. | Allows a regular application to use Service.startForeground. |
| android.permission.FOREGROUND_SERVICE_CONNECTED_DEVICE | normal | enables foreground services with connected device use. | Allows a regular application to use Service.startForeground with the type "connectedDevice". |
| android.permission.POST_NOTIFICATIONS | dangerous | allows an app to post notifications. | Allows an app to post notifications |
| com.google.android.c2dm.permission.RECEIVE | normal | recieve push notifications | Allows an application to receive push notifications from cloud. |
| com.truhearing.rta.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION | unknown | Unknown permission | Unknown permission from android reference |



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

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

| ACTIVITY | INTENT |
|--|--|
| crc648316b0a9aa8cfd61.BrowserTabActivity | Schemes: msal47a2ba70-6bd4-4599-8244-a3b814796770://, msalf38d888f-1965-4894-ad5d-be1cdb5eec5d://, Hosts: auth, |

NETWORK SECURITY

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

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 3 | INFO: 0 | SUPPRESSED: 0

| NO | ISSUE | SEVERITY | DESCRIPTION |
|----|-------|----------|-------------|
|----|-------|----------|-------------|

| NO | ISSUE | SEVERITY | DESCRIPTION |
|----|--|----------|--|
| 1 | 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. |
| 2 | 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. |
| 3 | Activity (crc648316b0a9aa8cfd61.BrowserTabActivity) 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 (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true] | warning | A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission. |

</> CODE ANALYSIS

HIGH: 0 | WARNING: 3 | INFO: 3 | SECURE: 0 | SUPPRESSED: 0

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|--|----------|------------------------------|---|
| 1 | This app listens to Clipboard changes. Some malware also listen to Clipboard changes. | info | OWASP MASVS: MSTG-PLATFORM-4 | mono/android/content/ClipboardManager_OnPrimaryClipChangeListenerImplementor.java |
| | | | | com/aigestudio/wheelpicker/WheelPicker.java com/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/Utils/LogcatLogger.java com/microsoft/appcenter/AbstractAppCenterService.java com/microsoft/appcenter/AppCenter.java com/microsoft/appcenter/Constants.java com/microsoft/appcenter/Flags.java com/microsoft/appcenter/ServiceInstrumentationUtils.java com/microsoft/appcenter/UncaughtExceptionHandler.java com/microsoft/appcenter/analytics/Analytics.java com/microsoft/appcenter/analytics/AnalyticsTransmissionTarget.java com/microsoft/appcenter/analytics/AuthenticationProvider.java com/microsoft/appcenter/analytics/EventProperties.java com/microsoft/appcenter/analytics/channel/AnalyticsValidator.java com/microsoft/appcenter/analytics/channel/SessionTracker.java com/microsoft/appcenter/analytics/ingestion/models/EventLog.java com/microsoft/appcenter/analytics/ingestion/models/json/EventLogFactory.java com/microsoft/appcenter/channel/DefaultChannel.java com/microsoft/appcenter/channel/OneColle |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|---|----------|---|--|
| 2 | The App logs information. Sensitive information should never be logged. | info | CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3 | ctorChannelListener.java com/microsoft/appcenter/crashes/Crashes.java com/microsoft/appcenter/crashes/WrapperSdkExceptionHandler.java com/microsoft/appcenter/crashes/ingestion/models/AbstractErrorLog.java com/microsoft/appcenter/crashes/ingestion/models/ErrorAttachmentLog.java com/microsoft/appcenter/crashes/ingestion/models/HandledErrorLog.java com/microsoft/appcenter/crashes/ingestion/models/ManagedErrorLog.java com/microsoft/appcenter/crashes/utils/ErrorHandlerHelper.java com/microsoft/appcenter/http/AbstractAppCallTemplate.java com/microsoft/appcenter/http/DefaultHttpClient.java com/microsoft/appcenter/http/DefaultHttpClientCallTask.java com/microsoft/appcenter/http/HttpClientNetworkStateHandler.java com/microsoft/appcenter/http/HttpClientRetryer.java com/microsoft/appcenter/ingestion/OneCollectorIngestion.java com/microsoft/appcenter/ingestion/models/AbstractLog.java com/microsoft/appcenter/ingestion/models/StartServiceLog.java com/microsoft/appcenter/ingestion/models/one/CommonSchemaDataUtils.java com/microsoft/appcenter/ingestion/models/one/CommonSchemaLog.java com/microsoft/appcenter/ingestion/models/one/PartAUtils.java com/microsoft/appcenter/persistence/DatabasePersistence.java com/microsoft/appcenter/utils/AppCenterLo |

| NO | ISSUE | SEVERITY | STANDARDS | g.java FILES com/microsoft/appcenter/utis/AsyncTaskUtil s.java com/microsoft/appcenter/utis/DeviceInfoHe lper.java com/microsoft/appcenter/utis/IdHelper.java com/microsoft/appcenter/utis/NetworkStat eHelper.java com/microsoft/appcenter/utis/context/Sessi onContext.java com/microsoft/appcenter/utis/context/User IdContext.java com/microsoft/appcenter/utis/crypto/Crypt oUtils.java com/microsoft/appcenter/utis/storage/Data baseManager.java com/microsoft/appcenter/utis/storage/File Manager.java mono/MonoPackageManager_Resources.jav a mono/android/incrementaldeployment/Incr ementalClassLoader.java |
|----|-------|----------|-----------|--|
| | | | | |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|--|----------|--|---|
| 3 | Files may contain hardcoded sensitive information like usernames, passwords, keys etc. | warning | CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14 | com/microsoft/appcenter/AppCenter.java com/microsoft/appcenter/Constants.java com/microsoft/appcenter/channel/DefaultChannel.java com/microsoft/appcenter/crashes/utils/ErrorHandlerHelper.java com/microsoft/appcenter/http/DefaultHttpClient.java com/microsoft/appcenter/ingestion/OneCollectorIngestion.java com/microsoft/appcenter/ingestion/models/WrapperSdk.java com/microsoft/appcenter/ingestion/models/one/CommonSchemaLog.java com/microsoft/appcenter/persistence/DatabasePersistence.java com/microsoft/appcenter/utils/context/SessionContext.java com/microsoft/appcenter/utils/storage/DatabaseManager.java |
| 4 | This App uses SQL Cipher. Ensure that secrets are not hardcoded in code. | info | OWASP MASVS: MSTG-CRYPTO-1 | com/microsoft/appcenter/utils/storage/DatabaseManager.java |
| 5 | 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/microsoft/appcenter/persistence/DatabasePersistence.java com/microsoft/appcenter/utils/storage/DatabaseManager.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|----|---|----------|--|---|
| 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/microsoft/appcenter/http/HttpClientRet ryer.java |

NIAP ANALYSIS v1.3

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

BEHAVIOUR ANALYSIS

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---------|---|----------------------|---|
| 00078 | Get the network operator name | collection telephony | com/microsoft/appcenter/utils/DeviceInfoHelper.java |
| 00132 | Query The ISO country code | telephony collection | com/microsoft/appcenter/utils/DeviceInfoHelper.java |
| 00022 | Open a file from given absolute path of the file | file | com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/microsoft/appcenter/crashes/Crashes.java com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java com/microsoft/appcenter/utils/storage/FileManager.java |
| 00005 | Get absolute path of file and put it to JSON object | file | com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java |

| RULE ID | BEHAVIOUR | LABEL | FILES |
|---------|---|-----------------|--|
| 00004 | Get filename and put it to JSON object | file collection | com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java |
| 00013 | Read file and put it into a stream | file | com/airbnb/lottie/network/NetworkCache.java com/airbnb/lottie/network/NetworkFetcher.java com/microsoft/appcenter/utils/storage/FileManager.java okio/Okio.java |
| 00096 | Connect to a URL and set request method | command network | com/airbnb/lottie/network/NetworkFetcher.java |
| 00089 | Connect to a URL and receive input stream from the server | command network | com/airbnb/lottie/network/NetworkFetcher.java |
| 00030 | Connect to the remote server through the given URL | network | com/airbnb/lottie/network/NetworkFetcher.java |
| 00109 | Connect to a URL and get the response code | network command | com/airbnb/lottie/network/NetworkFetcher.java |

FIREBASE DATABASES ANALYSIS

| TITLE | SEVERITY | DESCRIPTION |
|----------------------------------|----------|---|
| App talks to a Firebase database | info | The app talks to Firebase database at https://lightcloud-1272.firebaseio.com |

| TITLE | SEVERITY | DESCRIPTION |
|---------------------------------|----------|--|
| Firebase Remote Config disabled | secure | Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/21086090395/namespaces/firebase:fetch?key=AlzaSyCLTCofHb07BffjnyKTxj3_oX44TYl8Y0 . This is indicated by the response: {'state': 'NO_TEMPLATE'} |

🚩 ABUSED PERMISSIONS

| TYPE | MATCHES | PERMISSIONS |
|--------------------------|---------|--|
| Malware Permissions | 10/25 | android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.READ_PHONE_STATE, android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.GET_ACCOUNTS |
| Other Common Permissions | 6/44 | android.permission.ACTIVITY_RECOGNITION, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.FOREGROUND_SERVICE, com.google.android.c2dm.permission.RECEIVE |

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 |
|----------------------------------|--------|--|
| mobile.events.data.microsoft.com | ok | IP: 20.189.173.9 Country: United States of America Region: California City: San Francisco Latitude: 37.774929 Longitude: -122.419418 View: Google Map |
| in.appcenter.ms | ok | IP: 132.196.225.214 Country: Sweden Region: Stockholms lan City: Stockholm Latitude: 59.332581 Longitude: 18.064899 View: Google Map |
| lightcloud-1272.firebaseio.com | ok | IP: 34.120.160.131 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map |

| TRACKER | CATEGORIES | URL |
|--|-----------------|---|
| Microsoft Visual Studio App Center Analytics | Analytics | https://reports.exodus-privacy.eu.org/trackers/243 |
| Microsoft Visual Studio App Center Crashes | Crash reporting | https://reports.exodus-privacy.eu.org/trackers/238 |

HARDCODED SECRETS

| POSSIBLE SECRETS |
|--|
| "firebase_database_url" : "https://lightcloud-1272.firebaseio.com" |
| "google_api_key" : "AlzaSyCLTCoNfHb07BffjnyKTxj3_oX44TYI8Y0" |
| "google_crash_reporting_api_key" : "AlzaSyCLTCoNfHb07BffjnyKTxj3_oX44TYI8Y0" |

PLAYSTORE INFORMATION

Title: TruHearing App

Score: 2.8247013 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** [com.truhearing.rta](https://play.google.com/store/apps/details?id=com.truhearing.rta)

Developer Details: Sivantos Pte. Ltd., Sivantos+Pte.+Ltd., None, <https://www.wsa.com>, apps@sivantos.com,

Release Date: Jul 20, 2020 **Privacy Policy:** [Privacy link](#)

Description:

The TruHearing app gives you everything you need to get the most from your hearing aids. Tailor your personal preferences discreetly on your smartphone: adjust volume and balance, change hearing programs, and monitor device connection and battery status. Get motivated to do more by seeing Health Insights about your physical and social activities. Stay in touch with your Hearing Care Professional with Virtual Appointments and TeleCare. The TruHearing app connects you with support when you need it – even when you can't make a visit in person. To enable TeleCare features, contact your Hearing Care Professional. The user guide for the app can be

accessed from the app settings menu. Alternatively, you can download the user guide in electronic form from www.wsaud.com or order a printed version from the same address. The printed version will be made available to you free of charge within 7 working days. Manufactured for TruHearing Inc. 12936 S. Frontrunner Blvd Draper, UT 84020 United States UDI-DI (01)05714880113150

SCAN LOGS

| Timestamp | Event | Error |
|---------------------|--|-------|
| 2025-09-01 10:42:51 | Generating Hashes | OK |
| 2025-09-01 10:42:51 | Extracting APK | OK |
| 2025-09-01 10:42:51 | Unzipping | OK |
| 2025-09-01 10:42:52 | Parsing APK with androguard | OK |
| 2025-09-01 10:42:52 | Extracting APK features using aapt/aapt2 | OK |
| 2025-09-01 10:42:53 | Getting Hardcoded Certificates/Keystores | OK |
| 2025-09-01 10:42:55 | Parsing AndroidManifest.xml | OK |
| 2025-09-01 10:42:55 | Extracting Manifest Data | OK |

| | | |
|---------------------|--|----|
| 2025-09-01 10:42:55 | Manifest Analysis Started | OK |
| 2025-09-01 10:42:55 | Performing Static Analysis on: TruHearing App (com.truhearing.rta) | OK |
| 2025-09-01 10:42:57 | Fetching Details from Play Store: com.truhearing.rta | OK |
| 2025-09-01 10:42:58 | Checking for Malware Permissions | OK |
| 2025-09-01 10:42:58 | Fetching icon path | OK |
| 2025-09-01 10:42:58 | Library Binary Analysis Started | OK |
| 2025-09-01 10:42:58 | Reading Code Signing Certificate | OK |
| 2025-09-01 10:42:59 | Running APKiD 2.1.5 | OK |
| 2025-09-01 10:43:02 | Detecting Trackers | OK |
| 2025-09-01 10:43:08 | Decompiling APK to Java with JADX | OK |
| 2025-09-01 10:45:02 | Decompiling with JADX failed, attempting on all DEX files | OK |

| | | |
|---------------------|--|----|
| 2025-09-01 10:45:02 | Decompiling classes2.dex with JADX | OK |
| 2025-09-01 10:45:09 | Decompiling classes.dex with JADX | OK |
| 2025-09-01 10:45:24 | Decompiling classes2.dex with JADX | OK |
| 2025-09-01 10:45:31 | Decompiling classes.dex with JADX | OK |
| 2025-09-01 10:45:47 | Decompiling with JADX failed for classes.dex | OK |
| 2025-09-01 10:45:47 | Some DEX files failed to decompile | OK |
| 2025-09-01 10:45:47 | Converting DEX to Smali | OK |
| 2025-09-01 10:45:47 | Code Analysis Started on - java_source | OK |
| 2025-09-01 10:45:49 | Android SBOM Analysis Completed | OK |
| 2025-09-01 10:45:56 | Android SAST Completed | OK |
| 2025-09-01 10:45:56 | Android API Analysis Started | OK |

| | | |
|---------------------|--|----|
| 2025-09-01 10:46:01 | Android API Analysis Completed | OK |
| 2025-09-01 10:46:02 | Android Permission Mapping Started | OK |
| 2025-09-01 10:46:09 | Android Permission Mapping Completed | OK |
| 2025-09-01 10:46:09 | Android Behaviour Analysis Started | OK |
| 2025-09-01 10:46:16 | Android Behaviour Analysis Completed | OK |
| 2025-09-01 10:46:16 | Extracting Emails and URLs from Source Code | OK |
| 2025-09-01 10:46:17 | Email and URL Extraction Completed | OK |
| 2025-09-01 10:46:17 | Extracting String data from APK | OK |
| 2025-09-01 10:46:17 | Extracting String data from Code | OK |
| 2025-09-01 10:46:17 | Extracting String values and entropies from Code | OK |
| 2025-09-01 10:46:21 | Performing Malware check on extracted domains | OK |

| | | |
|---------------------|--------------------|----|
| 2025-09-01 10:46:22 | 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.