ANDROID STATIC ANALYSIS REPORT

HearMax (1.37.1)

File Name:	com.beltone.hearmax_40075.apk
Package Name:	com.beltone.hearmax
Scan Date:	Aug. 29, 2025, 8:08 p.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	18	4	2	3

FILE INFORMATION

File Name: com.beltone.hearmax_40075.apk
Size: 110.74MB
MD5: 22ce5e743456d416345c45352efb26e3
SHA1: 98b210d978507a117f16596bd6fb2c6cd2ab110f
SHA256: ddcb509e8772c812b933508cc9f38bdacd714f20b5431e94c3932f0289ddfb91

APP INFORMATION

App Name: HearMax
Package Name: com.beltone.hearmax
Main Activity: crc6424c5bdc6993db472.SplashScreenActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 1.37.1

Android Version Code: 40075

APP COMPONENTS

Activities: 36
Services: 19
Receivers: 18
Providers: 7
Exported Activities: 0
Exported Services: 4
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=dk, ST=Unknown, L=Unknown, O=GN Resound A/S, OU=Unknown, CN=Unknown
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-08-10 15:00:04+00:00
Valid To: 2039-12-27 15:00:04+00:00
Issuer: C=dk, ST=Unknown, L=Unknown, O=GN Resound A/S, OU=Unknown, CN=Unknown
Serial Number: 0x502521f4
Hash Algorithm: sha1
md5: 883957838ae5e467e98b52b4f976849f
sha1: 4ffc7baee0ea8e76f415c6db26cc09f7377f7841
sha256: a78521a0902bd8f95209048599621bb89709aee4233f5b944a3e6df7401944ae
sha512: fb69049bee7727a424ae2663f256c6c1d11c0a09aef4d35716c97a3dc2b73b28fad3fd848fcab47668c8f2965e04324f7d2643a02efb2fb11e79ee8463179597
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: c0a8cba5dee14194b50f5903aca8ad4118a9774402fa5ab64aee075b85e02889
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.

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.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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.MANAGE_OWN_CALLS	normal	enables a calling app to manage its own calls.	Allows a calling application which manages it own calls through the self-managed ConnectionService APIs.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
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.ANSWER_PHONE_CALLS	dangerous	permits an app to answer incoming phone calls.	Allows the app to answer an incoming phone call.

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.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.READ_PHONE_NUMBERS	dangerous	allows reading of the device's phone number(s).	Allows read access to the device's phone number(s). This is a subset of the capabilities granted by READ_PHONE_STATE but is exposed to instant applications.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.BATTERY_STATS	signature	modify battery statistics	Allows the modification of collected battery statistics. Not for use by common applications.
android.permission.FOREGROUND_SERVICE_CONNECTED_DEVICE	normal	enables foreground services with connected device use.	Allows a regular application to use Service.startForeground with the type "connectedDevice".
android.permission.FOREGROUND_SERVICE_LOCATION	normal	allows foreground services with location use.	Allows a regular application to use Service.startForeground with the type "location".
android.permission.FOREGROUND_SERVICE_PHONE_CALL	normal	enables foreground services during phone calls.	Allows a regular application to use Service.startForeground with the type "phoneCall".
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.beltone.hearmax.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>22ce5e743456d416345c45352efb26e3.apk</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>possible VM check</td></tr></table></td></tr>
<tr><td>classes.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.HARDWARE check</td></tr><tr><td>Compiler</td><td>r8</td></tr></table></td></tr>
<tr><td>classes2.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
network operator name check
possible VM check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table></td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
crc6424c5bdc6993db472.SplashScreenActivity	Schemes: hearmaxcfg://, Hosts: dk.gnresound.gandalf.bt.config, Path Prefixes: /configuration,

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: **0** | 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	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	Broadcast Receiver (crc6446b4299145116f28.PackageReplaceReceiver) 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.
4	Service (crc64cef9ffdba4b18365.VoipCallConnectionService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_TELECOM_CONNECTION_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
5	Service (crc6409c5ccb2024a175c.RegistrationScheduler) 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.
6	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.
7	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected. [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.
8	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
9	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.

CODE ANALYSIS

HIGH: **1** | WARNING: **7** | INFO: **3** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/baidu/android/pushservice/d/f.java com/microsoft/appcenter/AppCenter.java com/microsoft/appcenter/Constants.java com/microsoft/appcenter/channel/DefaultChannel.java com/microsoft/appcenter/crashes/utils/ErrorLogHelper.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 com/opentok/android/DefaultAudioDevice.java
				com/baidu/android/pushservice/PushManager.java com/baidu/android/pushservice/f/a.java com/baidu/android/pushservice/h/m.java com/baidu/android/pushservice/jni/PushSocket.java com/baidu/push/cid/cesium/c.java com/baidu/push/cid/cesium/f.java com/microsoft/appcenter/AbstractAppCenterService.java com/microsoft/appcenter/AppCenter.java com/microsoft/appcenter/Constants.java com/microsoft/appcenter/Flags.java

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	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/OneCollectorChannelListener.java com/microsoft/appcenter/crashes/Crashes.java com/microsoft/appcenter/crashes/WrapperSdkExceptionManager.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/ErrorLogHelper.java com/microsoft/appcenter/http/AbstractAppCallTemplate.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				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/one/CommonSchemaDataUtils.java com/microsoft/appcenter/ingestion/models/one/CommonSchemaLog.java com/microsoft/appcenter/persistence/DatabasePersistence.java com/microsoft/appcenter/utils/AppCenterLog.java com/microsoft/appcenter/utils/AsyncTaskUtils.java com/microsoft/appcenter/utils/DeviceInfoHelper.java com/microsoft/appcenter/utils/IdHelper.java com/microsoft/appcenter/utils/NetworkStateHelper.java com/microsoft/appcenter/utils/context/SessionContext.java com/microsoft/appcenter/utils/context/UserIdContext.java com/microsoft/appcenter/utils/crypto/CryptoUtils.java com/microsoft/appcenter/utils/storage/DatabaseManager.java com/microsoft/appcenter/utils/storage/FileManager.java com/opentok/android/BaseVideoCapturer.java com/opentok/android/OtLog.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				mono/MonoPackageManager_Resources.java mono/android/incrementaldeployment/IncrementalClassLoader.java
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/baidu/android/pushservice/e.java com/baidu/android/pushservice/h.java com/baidu/android/pushservice/h/m.java com/baidu/push/cid/cesium/f.java
4	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/baidu/android/pushservice/c/a.java com/baidu/android/pushservice/c/c.java com/microsoft/appcenter/persistence/DatabasePersistence.java com/microsoft/appcenter/utils/storage/DatabaseManager.java
5	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	mono/android/content/ClipboardManager_OnPrimaryClipChangedListenerImplementor.java
6	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/baidu/android/pushservice/h/k.java
7	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	com/baidu/android/pushservice/e/b.java
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/baidu/android/pushservice/e/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/baidu/android/pushservice/h/f.java
10	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/baidu/android/pushservice/h.java
11	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/baidu/android/pushservice/b/d.java com/baidu/push/cid/cesium/j/b/b.java com/microsoft/appcenter/http/HttpClientRetryer.java
12	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

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

RULE ID	BEHAVIOUR	LABEL	FILES
00132	Query The ISO country code	telephony collection	com/microsoft/appcenter/utils/DeviceInfoHelper.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/baidu/android/pushservice/PushServiceReceiver.java com/baidu/android/pushservice/h/m.java com/baidu/android/pushservice/message/PublicMsg.java com/baidu/android/pushservice/message/a/c.java
00022	Open a file from given absolute path of the file	file	com/baidu/android/pushservice/c/c.java com/baidu/android/pushservice/h/m.java com/baidu/push/cid/cesium/f.java com/microsoft/appcenter/crashes/Crashes.java com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java com/microsoft/appcenter/utils/storage/FileManager.java org/tensorflow/lite/Interpreter.java org/tensorflow/lite/InterpreterImpl.java
00036	Get resource file from res/raw directory	reflection	com/baidu/android/pushservice/CustomPushNotificationBuilder.java com/baidu/android/pushservice/c/c.java com/baidu/android/pushservice/h/m.java com/baidu/android/pushservice/message/a/c.java
00056	Modify voice volume	control	org/otwebrtc/audio/WebRtcAudioTrack.java org/otwebrtc/voiceengine/WebRtcAudioTrack.java org/otwebrtc/voiceengine61/WebRtcAudioTrack.java
00013	Read file and put it into a stream	file	com/baidu/android/pushservice/b/a.java com/baidu/android/pushservice/e.java com/baidu/android/pushservice/h.java com/baidu/push/cid/cesium/l/a.java com/microsoft/appcenter/utils/storage/FileManager.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/baidu/android/pushservice/PushServiceReceiver.java com/baidu/android/pushservice/message/PublicMsg.java com/baidu/android/pushservice/message/a/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/baidu/android/pushservice/e/b.java
00089	Connect to a URL and receive input stream from the server	command network	com/baidu/android/pushservice/e/b.java
00163	Create new Socket and connecting to it	socket	com/baidu/android/pushservice/e/b.java
00030	Connect to the remote server through the given URL	network	com/baidu/android/pushservice/e/b.java
00109	Connect to a URL and get the response code	network command	com/baidu/android/pushservice/e/b.java
00153	Send binary data over HTTP	http	com/baidu/android/pushservice/e/b.java
00094	Connect to a URL and read data from it	command network	com/baidu/android/pushservice/e/b.java
00108	Read the input stream from given URL	network command	com/baidu/android/pushservice/e/b.java
00189	Get the content of a SMS message	sms	com/baidu/android/pushservice/c/c.java com/baidu/android/pushservice/c/d.java
00188	Get the address of a SMS message	sms	com/baidu/android/pushservice/c/c.java com/baidu/android/pushservice/c/d.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/baidu/android/pushservice/c/c.java com/baidu/android/pushservice/c/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	com/baidu/android/pushservice/c/c.java com/baidu/android/pushservice/c/d.java
00200	Query data from the contact list	collection contact	com/baidu/android/pushservice/c/c.java com/baidu/android/pushservice/c/d.java
00201	Query data from the call log	collection calllog	com/baidu/android/pushservice/c/c.java com/baidu/android/pushservice/c/d.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/baidu/android/pushservice/c/c.java com/baidu/android/pushservice/c/d.java
00102	Set the phone speaker on	command	com/opentok/android/DefaultAudioDevice.java
00005	Get absolute path of file and put it to JSON object	file	com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java
00004	Get filename and put it to JSON object	file collection	com/microsoft/appcenter/crashes/utils/ErrorLogHelper.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	com/baidu/android/pushservice/c/c.java
00208	Capture the contents of the device screen	collection screen	org/otwebrtc/ScreenCapturerAndroid.java
00183	Get current camera parameters and change the setting.	camera	com/opentok/android/DefaultVideoCapturer.java org/otwebrtc/Camera1Session.java
00091	Retrieve data from broadcast	collection	com/baidu/android/pushservice/PushMessageReceiver.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://gandalf1-1385.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/371253658916/namespaces/firebase:fetch?key=AIzaSyDcIQ8vxrB6QkrOEHlUUTcboPLy3WR5OnM. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/25	android.permission.INTERNET, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK, android.permission.SYSTEM_ALERT_WINDOW, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.READ_PHONE_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.VIBRATE
Other Common Permissions	7/44	android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.FOREGROUND_SERVICE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.BATTERY_STATS, 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
180.76.76.112	IP: 180.76.76.112 Country: China Region: Beijing City: Beijing
api.tuisong.baidu.com	IP: 45.113.194.87 Country: China Region: Beijing City: Beijing

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
in.appcenter.ms	ok	**IP:** 4.152.45.235 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.opentok.com	ok	**IP:** 168.100.106.108 **Country:** United States of America **Region:** New Jersey **City:** Holmdel **Latitude:** 40.383961 **Longitude:** -74.170563 **View:** Google Map
mobile.events.data.microsoft.com	ok	**IP:** 52.178.17.2 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
180.76.76.112	ok	**IP:** 180.76.76.112 **Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map
10.95.41.15	ok	**IP:** 10.95.41.15 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
gandalf1-1385.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
api.tuisong.baidu.com	ok	**IP:** 45.113.194.87 **Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map

TRACKERS

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://gandalf1-1385.firebaseio.com"
"google_api_key" : "AIzaSyDcIQ8vxrB6QkrOEHlUUTcboPLy3WR5OnM"
"google_crash_reporting_api_key" : "AIzaSyDcIQ8vxrB6QkrOEHlUUTcboPLy3WR5OnM"
"ll_app_key" : "34c55b0b6e99152e61ff8be-1ed5e1fa-bd8b-11e7-bcda-007c928ca240"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
686479766013060971498190079908139321726943530014330540939446345918554318339765605212255964066145455497729631139148085803712198799971664381257402829111505715 1
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
a3084803c0efede7ed87b12e1c7e005ecea6540c
ae2044fb577e65ee8bb576ca48a2f06e
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

POSSIBLE SECRETS
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
115792089210356248762697446949407573530086143415290314195533631308867097853951
5181942b9ebc31ce68dacb56c16fd79f
686479766013060971498190079908139321726943530014330540939446345918554318339765539424505774633321719753296399637136332111386476861244038034037280889270700 5449
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
115792089210356248762697446949407573529996955224135760342422259061068512044369

PLAYSTORE INFORMATION

Title: Beltone HearMax

Score: 4.4431553 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.beltone.hearmax

Developer Details: GN Hearing, GN+Hearing, None, http://www.beltone.com/hearmax, appsupport@beltone.com,

Release Date: Apr 28, 2017 **Privacy Policy:** Privacy link

Description:

The Beltone HearMax app lets you control your hearing aids directly from your mobile device. You can change programs, and make simple or more advanced sound adjustments and save them as favorites. The app helps you learn what you can do and how to do it. It can even help you find your hearing aids if you lose them. Last, but not least, you can have your hearing care professional update your hearing aid programs and send you new hearing aid software without taking a trip to the clinic. Notes: Please contact your local Beltone representative for product and feature availability in your market. We recommend that the hearing aids run the latest software version. If in doubt, please contact your hearing care professional. Beltone HearMax mobile device compatibility: Please consult the Beltone app website for up-to-date compatibility information: www.beltone.com/support/compatibility. Use the Beltone HearMax app to: • Enjoy Beltone Remote Care: Request help with your hearing aid settings from your hearing care professional and receive new settings and software updates. And use these direct control and personalization options: • Adjust volume settings on your hearing aids • Mute your hearing aids • Adjust volume of your Beltone streaming accessories • Adjust speech focus as well as noise and wind-noise levels with Sound Enhancer (feature availability depends on your hearing aid model and the fitting by your hearing care professional) • Change manual and streamer programs • Edit and personalize program names • Adjust treble, middle and bass tones to your preferences • Save your preferred settings as a Favorite – you can even tag to a location • Monitor the battery status of your rechargeable hearing aids • Help locate lost or misplaced hearing aids • Tinnitus manager: Adjust sound variation and frequency of the Tinnitus Breaker Pro. Select Nature Sounds (feature availability depends on your hearing aid model and the fitting by your hearing care professional) For more information please visit www.beltone.com/hearmax or the support site via the link in the app store.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 20:08:33	Generating Hashes	OK
2025-08-29 20:08:33	Extracting APK	OK
2025-08-29 20:08:33	Unzipping	OK
2025-08-29 20:08:33	Parsing APK with androguard	OK
2025-08-29 20:08:33	Extracting APK features using aapt/aapt2	OK

2025-08-29 20:08:33	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 20:08:35	Parsing AndroidManifest.xml	OK
2025-08-29 20:08:35	Extracting Manifest Data	OK
2025-08-29 20:08:35	Manifest Analysis Started	OK
2025-08-29 20:08:35	Performing Static Analysis on: HearMax (com.beltone.hearmax)	OK
2025-08-29 20:08:36	Fetching Details from Play Store: com.beltone.hearmax	OK
2025-08-29 20:08:37	Checking for Malware Permissions	OK
2025-08-29 20:08:37	Fetching icon path	OK
2025-08-29 20:08:37	Library Binary Analysis Started	OK
2025-08-29 20:08:37	Reading Code Signing Certificate	OK
2025-08-29 20:08:38	Running APKiD 2.1.5	OK

2025-08-29 20:08:43	Detecting Trackers	OK
2025-08-29 20:08:45	Decompiling APK to Java with JADX	OK
2025-08-29 20:08:59	Converting DEX to Smali	OK
2025-08-29 20:08:59	Code Analysis Started on - java_source	OK
2025-08-29 20:09:01	Android SBOM Analysis Completed	OK
2025-08-29 20:09:06	Android SAST Completed	OK
2025-08-29 20:09:06	Android API Analysis Started	OK
2025-08-29 20:09:10	Android API Analysis Completed	OK
2025-08-29 20:09:10	Android Permission Mapping Started	OK
2025-08-29 20:09:15	Android Permission Mapping Completed	OK

2025-08-29 20:09:16	Android Behaviour Analysis Started	OK
2025-08-29 20:09:20	Android Behaviour Analysis Completed	OK
2025-08-29 20:09:20	Extracting Emails and URLs from Source Code	OK
2025-08-29 20:09:21	Email and URL Extraction Completed	OK
2025-08-29 20:09:21	Extracting String data from APK	OK
2025-08-29 20:09:21	Extracting String data from Code	OK
2025-08-29 20:09:21	Extracting String values and entropies from Code	OK
2025-08-29 20:09:24	Performing Malware check on extracted domains	OK
2025-08-29 20:09:25	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.