MOBSF

ANDROID STATIC ANALYSIS REPORT

Avaz (6.6.7)

File Name:	Avaz AAC_6.6.7_APKPure.xapk
Package Name:	com.avazapp.international.lite
Scan Date:	Nov. 17, 2024, 8:51 p.m.
App Security Score:	50/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	28	4	3	1

FILE INFORMATION

File Name: Avaz AAC_6.6.7_APKPure.xapk
Size: 20.28MB
MD5: 032cdd867b95a1702e7185e69c102182
SHA1: 37838122b94923705f7ce254a4e9bda90cf3ac97
SHA256: e9cc9a7f638aba1f3d42c7b43fc0dae6882b8c002fc41ed0b43fa194943342d9

APP INFORMATION

App Name: Avaz
Package Name: com.avazapp.international.lite
Main Activity: com.avazapp.avaz_app.MainActivity
Target SDK: 33
Min SDK: 23
Max SDK:
Android Version Name: 6.6.7

Android Version Code: 199

APP COMPONENTS

Activities: 14
Services: 18
Receivers: 17
Providers: 4
Exported Activities: 5
Exported Services: 3
Exported Receivers: 6
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
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: 2018-06-06 07:51:35+00:00
Valid To: 2048-06-06 07:51:35+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x9a16c530c0eadedcd306abb2eb4fbcc1112f2d98
Hash Algorithm: sha256
md5: e8e03c877a7814cb87964cbc5e5033b9
sha1: 0680e00e2f9839975ab183b3ee5ac9723070d4fb
sha256: bc6931b618498cba130bf6178d5a551e43c0997732637cb349888ec11ff26d43
sha512: 4eee09cc678aeeacea853648f5abab2521c5e4fe9d9b2571fc3ae3d54b561d8d3ad9a7e31aee279bcb83200cf8b9b4e597f4bc0afc32818013d84a4188fd0935
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: deb16330bd066ee117e59e83f62825b194914bb34a440aa5fb03074486e0a9ea
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.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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
com.avazapp.international.lite.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
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.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
com.sec.android.provider.badge.permission.READ	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	show notification count on app	Show notification count or badge on application launch icon for sony phones.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
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

PERMISSION	STATUS	INFO	DESCRIPTION
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.avazapp.international.lite.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.

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>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
Build.TAGS check
SIM operator check
network operator name check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.avazapp.avaz_app.MainActivity	Schemes: content://, file://, db-jo6q2x4jwtx06v7://, Hosts: *, Mime Types: */*, Path Patterns: .*\\.avt, .*\\.avc, .*\\.avz,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 16 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Broadcast Receiver (com.onesignal.FCMBroadcastReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Activity (com.onesignal.NotificationOpenedActivityHMS) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Broadcast Receiver (com.onesignal.NotificationDismissReceiver) 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.onesignal.BootUpReceiver) 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.
7	Broadcast Receiver (com.onesignal.UpgradeReceiver) 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.
8	Activity (com.onesignal.NotificationOpenedReceiver) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Activity (com.onesignal.NotificationOpenedReceiverAndroid22AndOlder) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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.
11	Activity (com.google.firebase.auth.internal.RecaptchaActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
12	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.
13	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.
14	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.

NO	ISSUE	SEVERITY	DESCRIPTION
15	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
16	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.
17	High Intent Priority (999) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

HIGH: 3 | WARNING: 9 | INFO: 3 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a3/a.java a3/d.java b3/i.java b9/b.java c6/l.java ca/a.java com/acapelagroup/android/tts/acattsandroid.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/avazapp/avaz_app/MainActivity.java com/eyetechds/quicklink/ETClient.java com/eyetechds/quicklink/EyeOnAirCommand.java com/eyetechds/quicklink/QLDevice.java com/eyetechds/quicklink/ReadPipeData.java com/eyetechds/quicklink/ReadPipeVideo.java com/eyetechds/quicklink/eyetechAPI.java com/mr/flutter/plugin/filepicker/b.java com/mr/flutter/plugin/filepicker/c.java com/onesignal/JobIntentService.java com/onesignal/d3.java com/onesignal/f.java com/onesignal/flutter/f.java com/parse/ConnectivityNotifier.java com/parse/InstallationId.java com/parse/ManifestInfo.java com/parse/NetworkQueryController.java com/parse/Parse.java com/parse/ParseDateFormat.java com/parse/ParseImpreciseDateFormat.java com/parse/ParseInstallation.java com/parse/ParseKeyValueCache.java com/parse/ParseObject.java com/parse/ParsePinningEventuallyQueue.java com/parse/ParseRequest.java com/yalantis/ucrop/UCropActivity.

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/yalantis/ucrop/view/b.java d0/a.java d2/b.java e2/a.java e8/c.java f0/c.java f0/d.java f0/e.java g0/a.java g8/a.java h3/g.java h8/a.java h8/b.java io/flutter/plugins/firebase/crashlytics/n.java io/flutter/plugins/imagepicker/b.java io/flutter/plugins/imagepicker/g.java j0/c.java j2/a.java j3/b.java j3/d.java j3/h.java j3/r.java j3/s.java j3/u.java j3/x.java j3/y.java j5/a.java j5/b.java j5/c.java k0/a.java k3/b0.java k3/e.java k3/g0.java k3/j.java k3/k.java k3/l0.java k3/o.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	k3/x.java k8/c0.java k8/e0.java k8/i.java kr/co/voiceware/java/vtapi/VoiceText.java kr/co/voiceware/vtlicensemodule/VtLicenseDownloadThread.java kr/co/voiceware/vtlicensemodule/VtLicenseSetting.java kr/co/voiceware/vtlicensemodule/VwCertificateBySoap.java l1/e.java l1/f.java l3/k.java l4/a.java m/g.java m1/a.java m3/j0.java m4/a.java n/c.java o1/a.java o2/k.java o3/a.java o3/c.java o3/d0.java o3/d1.java o3/g0.java o3/g1.java o3/h1.java o3/i.java o3/i1.java o3/k0.java o3/k1.java o3/q1.java o3/t1.java p1/a.java p1/b.java p7/a.java p7/e.java q0/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				q7/h.java r1/a.java r3/a.java r8/a.java r8/b.java s2/a.java s3/a.java s5/e.java s8/a.java s8/c.java s8/f.java t0/a.java t1/a.java t1/c.java t1/d.java t3/h.java t3/p.java t3/q.java u0/e0.java u1/d.java u4/a.java u7/a.java u7/b.java v9/l.java w0/j.java w1/c.java w5/c.java w5/c0.java w5/i1.java w5/j0.java w5/k0.java w5/r0.java w5/u0.java w5/y.java w5/z.java w5/z0.java w7/c.java w9/i.java x1/b.java x3/b.java x5/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				x5/o.java x6/b.java x9/i.java y1/a.java y1/n.java y1/o.java y1/p.java y6/c.java y9/l.java z5/f.java z9/i.java
2	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/onesignal/OSUtils.java com/parse/LocalIdManager.java r1/a.java ua/a.java ua/b.java ub/b.java va/a.java z3/c.java
3	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	x6/b.java z8/a.java
4	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	io/flutter/plugins/imagepicker/e.java j4/b.java jc/a.java mc/c.java u7/c.java x6/c.java
5	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/onesignal/f4.java com/onesignal/h1.java com/onesignal/p1.java e6/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/onesignal/o4.java
7	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/onesignal/o4.java
8	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	c8/k.java com/onesignal/k3.java com/parse/OfflineSQLiteOpenHelper.java com/parse/ParseSQLiteDatabase.java k8/i.java r0/a.java t1/c.java v7/g.java w2/m0.java w2/t0.java
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/parse/ParseDigestUtils.java com/parse/ParseRESTCommand.java
10	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/mr/flutter/plugin/filepicker/b.java com/mr/flutter/plugin/filepicker/c.java jc/a.java n8/h.java x9/h.java x9/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	kr/co/voiceware/java/vtapi/BuildConfig.java
12	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	kr/co/voiceware/java/vtapi/VoiceText.java kr/co/voiceware/vtlicensemodule/VwCertificateBySoap.java
13	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	q7/h.java
14	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	c6/g.java u4/r.java
15	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	xb/c.java
16	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	l1/e.java
17	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	io/flutter/plugin/editing/b.java io/flutter/plugin/platform/b.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/acapelagroup/android/tts/acattsandroid.java com/mr/flutter/plugin/filepicker/c.java d2/b.java d6/d.java da/b.java i2/a.java io/flutter/plugins/imagepicker/e.java mc/c.java p0/a.java qb/h.java r0/b.java r1/a.java ub/a.java x9/i.java
00009	Put data in cursor to JSON object	file	com/onesignal/f0.java com/onesignal/i0.java com/onesignal/m0.java com/onesignal/r.java com/parse/OfflineStore.java t1/c.java v7/g.java
00191	Get messages in the SMS inbox	sms	com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java r1/a.java
00202	Make a phone call	control	y1/p.java

RULE ID	BEHAVIOUR	LABEL	FILES
00203	Put a phone number into an intent	control	y1/p.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/mr/flutter/plugin/filepicker/b.java com/onesignal/OSUtils.java com/onesignal/d0.java com/onesignal/shortcutbadger/impl/SonyHomeBadger.java io/flutter/plugins/imagepicker/e.java k3/f.java y1/a.java y1/n.java y1/p.java z9/h.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/onesignal/OSUtils.java com/onesignal/d0.java k3/f.java y1/a.java y1/n.java y1/p.java z9/h.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	c6/u.java com/acapelagroup/android/tts/acattsandroid.java com/mr/flutter/plugin/filepicker/c.java com/parse/ParseCountingFileHttpBody.java com/parse/ParseFileHttpBody.java com/parse/ParseFileUtils.java d2/b.java d6/d.java h6/e.java j6/a.java kr/co/voiceware/vtlicensemodule/VtLicenseDownloadThread.java m1/a.java oa/l.java oa/n.java p0/c.java p4/e.java r7/a.java s8/e.java ub/a.java vb/b.java x6/c.java
00162	Create InetSocketAddress object and connecting to it	socket	dc/b.java dc/g.java
00163	Create new Socket and connecting to it	socket	dc/b.java dc/g.java
00189	Get the content of a SMS message	sms	com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00188	Get the address of a SMS message	sms	com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java

RULE ID	BEHAVIOUR	LABEL	FILES
00200	Query data from the contact list	collection contact	com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00187	Query a URI and check the result	collection sms calllog calendar	com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00201	Query data from the call log	collection calllog	com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java
00036	Get resource file from res/raw directory	reflection	com/onesignal/OSUtils.java com/onesignal/d0.java com/onesignal/shortcutbadger/impl/EverythingMeHomeBadger.java com/onesignal/shortcutbadger/impl/HuaweiHomeBadger.java com/onesignal/shortcutbadger/impl/NovaHomeBadger.java com/onesignal/shortcutbadger/impl/SamsungHomeBadger.java com/onesignal/shortcutbadger/impl/SonyHomeBadger.java k3/f.java y1/a.java y1/n.java
00078	Get the network operator name	collection telephony	com/onesignal/OSUtils.java v7/n.java
00091	Retrieve data from broadcast	collection	com/onesignal/FCMBroadcastReceiver.java com/onesignal/PermissionsActivity.java com/onesignal/t1.java
00109	Connect to a URL and get the response code	network command	a3/d.java com/onesignal/o3.java h3/f.java w7/b.java y6/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	com/onesignal/o3.java w7/b.java y6/c.java
00089	Connect to a URL and receive input stream from the server	command network	com/onesignal/o3.java w7/b.java y6/c.java
00056	Modify voice volume	control	j8/b.java t7/d.java
00094	Connect to a URL and read data from it	command network	g6/a.java w7/b.java
00108	Read the input stream from given URL	network command	w7/b.java
00161	Perform accessibility service action on accessibility node info	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java io/flutter/view/c.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	io/flutter/view/AccessibilityViewEmbedder.java
00012	Read data and put it into a buffer stream	file	com/mr/flutter/plugin/filepicker/c.java
00092	Send broadcast	command	com/onesignal/i0.java
00102	Set the phone speaker on	command	j8/b.java kc/m.java

RULE ID	BEHAVIOUR	LABEL	FILES
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	h2/a.java
00014	Read file into a stream and put it into a JSON object	file	d6/d.java j6/a.java x6/c.java
00192	Get messages in the SMS inbox	sms	jc/a.java
00209	Get pixels from the latest rendered image	collection	io/flutter/embedding/android/g.java
00210	Copy pixels from the latest rendered image into a Bitmap	collection	io/flutter/embedding/android/g.java
00005	Get absolute path of file and put it to JSON object	file	d6/d.java
00199	Stop recording and release recording resources	record	u7/b.java
00198	Initialize the recorder and start recording	record	u7/b.java
00194	Set the audio source (MIC) and recorded file format	record	u7/b.java
00197	Set the audio encoder and initialize the recorder	record	u7/b.java
00196	Set the recorded file format and output path	record file	u7/b.java

RULE ID	BEHAVIOUR	LABEL	FILES
00128	Query user account information	collection account	com/acapelagroup/android/tts/acattsandroid.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://avaz-for-android-5e583.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/451653437887/namespaces/firebase:fetch?key=AIzaSyCx1c-NT7deE4WgzSqHxwEcSMDjusSr8e4. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.INTERNET, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.GET_ACCOUNTS, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.VIBRATE, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	6/44	android.permission.FOREGROUND_SERVICE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.CHANGE_WIFI_STATE, com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.

Other Common Permissions:
Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
parseapi.back4app.com	ok	**IP:** 18.67.39.120 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
accounts.google.com	ok	**IP:** 64.233.180.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebase-settings.crashlytics.com	ok	**IP:** 142.251.41.35 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.onesignal.com	ok	**IP:** 104.16.160.145 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.251.41.66 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	ok	**IP:** 140.82.114.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
avaz-for-android-5e583.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
developer.android.com	ok	**IP:** 142.251.41.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.mixpanel.com	ok	**IP:** 130.211.34.183 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
verification.voiceware.co.kr	ok	**IP:** 210.205.55.5 **Country:** Korea (Republic of) **Region:** Seoul-teukbyeolsi **City:** Seoul **Latitude:** 37.568260 **Longitude:** 126.977829 **View:** Google Map
schemas.xmlsoap.org	ok	**IP:** 13.107.246.35 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	k3/w.java

TRACKERS

TRACKER	CATEGORIES	URL
Bolts	Analytics	https://reports.exodus-privacy.eu.org/trackers/403
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
OneSignal		https://reports.exodus-privacy.eu.org/trackers/193

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "6d75ed8eafe94d7e9306187f832b1af1"
"firebase_database_url" : "https://avaz-for-android-5e583.firebaseio.com"
"google_api_key" : "AIzaSyCx1c-NT7deE4WgzSqHxwEcSMDjusSr8e4"
"google_crash_reporting_api_key" : "AIzaSyCx1c-NT7deE4WgzSqHxwEcSMDjusSr8e4"
lgOHbvYl5meun6k6kYYXa1zZWs47yxHOkTKe4b6j
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
c682b8144a8dd52bc1ad63
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66

POSSIBLE SECRETS
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
49f946663a8deb7054212b8adda248c6
VGhpcyBpcyB0aGUga2V5IGZvcihBIHNlY3XyZZBzdG9yYWdlIEFFUyBLZXkK
3qZQJAtZxjyFqa4PuIi8vf1TAa3TXzIv3iq1G58O
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBhIHNlY3VyZSBzdG9yYWdlCg
470fa2b4ae81cd56ecbcda9735803434cec591fa
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
Y29tLmFuZHJvaWQudmVuZGluZy5saWNlbnNpbmcuSUxpY2Vuc2luZ1NlcnZpY2U=
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
VGhpcyBpcyB0aGUga2V5IGZvciBhIHNlY3VyZSBzdG9yYWdlIEFFUyBLZXkK
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
b2f7f966-d8cc-11e4-bed1-df8f05be55ba
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
5eb5a37e-b458-11e3-ac11-000c2940e62c
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c103703e120ae8cc73c9248622f3cd1e
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
VGhpcyBpcyB0aGUgcHJlZml4IGZvciBCaWdJbnRlZ2Vy
85053bf24bba75239b16a601d9387e17

PLAYSTORE INFORMATION

Title: Avaz AAC

Score: 3.8658535 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Education **Play Store URL:** com.avazapp.international.lite

Developer Details: Avaz Inc., Avaz+Inc., 374 Tyrella Avenue Mountain View California 94043, http://www.avazapp.com, support@avazapp.com,

Release Date: Nov 22, 2018 **Privacy Policy:** Privacy link

Description:

Avaz AAC is an Augmentative and Alternative Communication App that empowers children & adults with Autism, Cerebral Palsy, Down Syndrome, Aphasia, Apraxia and individuals with any other condition/cause of speech delays, with a voice of their own. "My daughter has nearly mastered the navigation, so much so that one day she brought it to me to show me she wanted Taco Bell for lunch. This made me cry. My child had a voice for the first time. Thank you for being the one to give my daughter that voice". - Amy Kinderman Designed to aid language development, by presenting core words, which make up 80% of everyday speech, in a research-based order. This enables users to progress from using 1-2 word phrases to forming complete sentences. Avaz, a fully AAC text-to-speech app with over 40,000 pictures(Symbolstix) and a range of high-quality voices, enables users to quickly form sentences and express themselves with ease. Avaz is a customizable AAC app that empowers users to express themselves powerfully and connect with the world! Now available in English UK, English US, Français, Dansk, Svenska, Magyar, and Føroyskt Picture mode - Vocabulary is organized in a consistent pattern to facilitate quick access and promote motor memory in users. - Color-coded words with the Fitzgerald key allow easy correlation of part of speech with special ed classroom materials. - Enlarging words when tapped on for visual reinforcement. - Option for advanced users to hide pictures and adjust the number of displayed pictures (from 1-77). - Add and personalize multiple words and folders in an instant. - A quick search for words with path visibility. Keyboard mode - Create sentences with just a few taps with a powerful prediction system. - Prediction of words and phrases along with predicting the present and following words, as well as options for phonetically spelled words. - Favorites folder for saving frequently-used phrases. Other Key Features - Auto Backup your vocabulary in the cloud storage of your choice. - Share folders with other Avaz AAC users. - Get the caregiver's attention with the ‘mistake’ & ‘alert’ buttons. - Create a PECS book by generating a PDF file in the app and printing it. - Access FAQs and the support desk within the app. - Add a passcode to Settings & Edit mode. - Easily share messages with loved ones on email, WhatsApp, and social media. Upgrade Your Avaz Experience Introducing auto backup for worry-free vocabulary progress. Simply choose how often you want your vocabulary progress backed up with our auto-backup interval selection option. Never lose your progress again! We understand that different users have different preferences regarding cloud storage. So we’ve made it easy to back up your vocabulary to your preferred cloud storage including popular platforms like Google Drive and many more! Avaz gets a visual upgrade with new themes -Classic Light, Classic Dark (with high contrast), and Outer Space (a dark mode). The dark mode is especially useful for adult users and those using Avaz with eye-tracking devices. "We are always happy to hear from you. For any questions, support, or general, please feel free to write to us at support@avazapp.com. Note:Try Avaz AAC's free 14-day trial without adding credit card details! You can make in-app purchases and choose from our affordable monthly, yearly, and lifetime subscription plans to keep benefiting from the amazing features. Terms of Use - https://www.avazapp.com/terms-of-use/ Privacy Policy - https://www.avazapp.com/privacy-policy/

SCAN LOGS

Timestamp	Event	Error
2024-11-17 20:51:57	Generating Hashes	OK
2024-11-17 20:51:57	Extracting APK	OK

2024-11-17 20:51:57	Unzipping	OK
2024-11-17 20:51:57	Getting Hardcoded Certificates/Keystores	OK
2024-11-17 20:51:57	Parsing APK with androguard	OK
2024-11-17 20:51:58	Parsing AndroidManifest.xml	OK
2024-11-17 20:51:58	Extracting Manifest Data	OK
2024-11-17 20:51:58	Performing Static Analysis on: Avaz (com.avazapp.international.lite)	OK
2024-11-17 20:51:58	Fetching Details from Play Store: com.avazapp.international.lite	OK
2024-11-17 20:51:59	Manifest Analysis Started	OK
2024-11-17 20:51:59	Checking for Malware Permissions	OK
2024-11-17 20:51:59	Fetching icon path	OK
2024-11-17 20:51:59	Library Binary Analysis Started	OK

2024-11-17 20:51:59	Reading Code Signing Certificate	OK
2024-11-17 20:51:59	Running APKiD 2.1.5	OK
2024-11-17 20:52:01	Detecting Trackers	OK
2024-11-17 20:52:01	Decompiling APK to Java with JADX	OK
2024-11-17 20:52:07	Converting DEX to Smali	OK
2024-11-17 20:52:07	Code Analysis Started on - java_source	OK
2024-11-17 20:52:09	Android SAST Completed	OK
2024-11-17 20:52:09	Android API Analysis Started	OK
2024-11-17 20:52:10	Android API Analysis Completed	OK
2024-11-17 20:52:10	Android Permission Mapping Started	OK
2024-11-17 20:52:12	Android Permission Mapping Completed	OK

2024-11-17 20:52:13	Email and URL Extraction Completed	OK
2024-11-17 20:52:13	Android Behaviour Analysis Started	OK
2024-11-17 20:52:14	Android Behaviour Analysis Completed	OK
2024-11-17 20:52:14	Extracting String data from APK	OK
2024-11-17 20:52:14	Extracting String data from Code	OK
2024-11-17 20:52:14	Extracting String values and entropies from Code	OK
2024-11-17 20:52:15	Performing Malware check on extracted domains	OK
2024-11-17 20:52:16	Saving to Database	OK
2024-11-17 20:52:17	Unzipping	OK

Report Generated by - MobSF v4.1.9

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.