ANDROID STATIC ANALYSIS REPORT

Speech Assistant (6.4.7)

File Name:	nl.asoft.speechassistant_149.apk
Package Name:	nl.asoft.speechassistant
Scan Date:	Sept. 1, 2025, 2:54 p.m.
App Security Score:	**54/100 (MEDIUM RISK)**
Grade:	**B**

◔ FINDINGS SEVERITY

🐞 HIGH	⚠ MEDIUM	ⓘ INFO	✔ SECURE	🔍 HOTSPOT
1	3	1	1	1

📦 FILE INFORMATION

File Name: nl.asoft.speechassistant_149.apk
Size: 54.95MB
MD5: 87ef43a887160ba68989bb51904d52d8
SHA1: 3dd8744af96ae72f7983d76ec72cbfdc360f133b
SHA256: 203e11582a95fb4bee01fa6171a7e0f7d6f8405e94afa0723673be44146a2fa1

ⓘ APP INFORMATION

App Name: Speech Assistant
Package Name: nl.asoft.speechassistant
Main Activity: nl.asoft.speechassistant.MainActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 6.4.7
Android Version Code: 149

■■ APP COMPONENTS

Activities: 18
Services: 2
Receivers: 1
Providers: 2
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

✸ CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: O=ASoft
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-06-27 09:52:40+00:00
Valid To: 2037-06-21 09:52:40+00:00
Issuer: O=ASoft
Serial Number: 0x4fead7e8
Hash Algorithm: sha1
md5: cb093ac40faff39fa5b5d95aa6cf0412
sha1: d6c6be89fe0c3da9f79e5a2b425b4f4d1597d2ce
sha256: d9d0da77585894be3ef3b8305c68fb68b03487636ab68e67a8a78cf3a04582a9
sha512: 43cfd474e88f7f165adba638e8990e3293f5180f95d499e1b1a4b3c097bf1492cf215acec89573807c200358fcebe331ad0cab887e01b29eb761ad1cfa6d488f
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 72b25ac1e7aeea007cdd814d817f8343cb68710068006ea336880bf30892baa2
Found 1 unique certificates

≔ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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.

🔍 APKID ANALYSIS

FILE	DETAILS
classes.dex	

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check
Compiler	r8 without marker (suspicious)

🔒 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: **2** | 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	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.

</> CODE ANALYSIS

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	A0/u.java D/b.java J/k.java M/a.java W/d.java W/g.java W/h.java W/k.java W/r.java W/v.java Y/u.java Z/A.java Z/AbstractBinderC0088a.java Z/AbstractC0090c.java Z/AbstractC0110x.java Z/S.java Z/V.java Z/W.java Z/X.java Z/Z.java Z/f0.java Z/j0.java c0/b.java k0/a.java l/k.java n/f.java p/C0337b.java t/C0365a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	B0/b.java Q/M.java Q/U.java

▤ NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

⛓ BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	A0/u.java W/e.java nl/asoft/speechassistant/FullScreen.java nl/asoft/speechassistant/MainActivity.java nl/asoft/speechassistant/SpeechPreferences.java
00013	Read file and put it into a stream	file	A0/u.java A0/v.java l/o.java nl/asoft/speechassistant/BackupPreferences.java nl/asoft/speechassistant/MainActivity.java nl/asoft/speechassistant/n.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	A0/u.java W/e.java nl/asoft/speechassistant/SpeechPreferences.java
00022	Open a file from given absolute path of the file	file	nl/asoft/speechassistant/BackupPreferences.java nl/asoft/speechassistant/FullScreen.java nl/asoft/speechassistant/MainActivity.java
00192	Get messages in the SMS inbox	sms	nl/asoft/speechassistant/SpeechPreferences.java
00091	Retrieve data from broadcast	collection	nl/asoft/speechassistant/FullScreen.java
00056	Modify voice volume	control	nl/asoft/speechassistant/FullScreen.java nl/asoft/speechassistant/SeekBarPreference.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	q/C0358o.java
00036	Get resource file from res/raw directory	reflection	W/e.java
00054	Install other APKs from file	reflection	nl/asoft/speechassistant/MainActivity.java
00080	Save recorded audio/video to a file	record file	nl/asoft/speechassistant/MainActivity.java
00101	Initialize recorder	record	nl/asoft/speechassistant/MainActivity.java
00195	Set the output path of the recorded file	record file	nl/asoft/speechassistant/MainActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00199	Stop recording and release recording resources	record	nl/asoft/speechassistant/MainActivity.java
00198	Initialize the recorder and start recording	record	nl/asoft/speechassistant/MainActivity.java
00136	Stop recording	record command	nl/asoft/speechassistant/MainActivity.java
00194	Set the audio source (MIC) and recorded file format	record	nl/asoft/speechassistant/MainActivity.java
00090	Set recroded audio/video file format	record	nl/asoft/speechassistant/MainActivity.java
00197	Set the audio encoder and initialize the recorder	record	nl/asoft/speechassistant/MainActivity.java
00007	Use absolute path of directory for the output media file path	file	nl/asoft/speechassistant/MainActivity.java
00138	Set the audio source (MIC)	record	nl/asoft/speechassistant/MainActivity.java
00196	Set the recorded file format and output path	record file	nl/asoft/speechassistant/MainActivity.java
00125	Check if the given file path exist	file	nl/asoft/speechassistant/MainActivity.java
00133	Start recording	record command	nl/asoft/speechassistant/MainActivity.java
00191	Get messages in the SMS inbox	sms	nl/asoft/speechassistant/MainActivity.java
00104	Check if the given path is directory	file	nl/asoft/speechassistant/MainActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00041	Save recorded audio/video to file	record	nl/asoft/speechassistant/MainActivity.java

⠿ ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	3/25	android.permission.RECORD_AUDIO, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET
Other Common Permissions	0/44	

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
www.asoft.app	ok	No Geolocation information available.
schemas.android.com	ok	No Geolocation information available.

✉ EMAILS

EMAIL	FILE
android@asoft.nl	B0/b.java
android@asoft.nl	A0/u.java
u0013android@android.com0 u0013android@android.com	W/q.java
android@asoft.nl	nl/asoft/speechassistant/MainActivity.java
android@asoft.nl	nl/asoft/speechassistant/SpeechPreferences.java
android@asoft.nl	Android String Resource

▷ PLAYSTORE INFORMATION

Title: Speech Assistant AAC

Score: 4.45 **Installs:** 500,000+ **Price:** 0 **Android Version Support: Category:** Communication **Play Store URL:** nl.asoft.speechassistant

Developer Details: A-Soft-nl, A-Soft-nl, None, http://www.asoft.nl, android@asoft.nl,

Release Date: Jun 27, 2012 **Privacy Policy:** [Privacy link](#)

Description:

Speech Assistant AAC is a text-to-speech (TTS) app designed for people who are speech impaired, for example due to Aphasia, MND/ALS, Autism, Stroke, Cerebral Palsy or other speech problems. With the app you can create categories and phrases, which are placed on buttons. With these buttons you can create messages that can be shown or spoken (text-to-speech). It is also possible to type any text using the keyboard. Key features • Easy to use and completely customizable to your needs and preferences. • Categories to organize your phrases. • History for quick access to previously typed phrases. • Option to select photos from your Photo Library or Symbols on the buttons. • Option to record speech or use a text-to-speech voice. • Full screen button to show your message with a large font. • Auto complete feature to quickly find your phrases. • Tabs for multiple conversations (optional setting). • Designed for smartphones and tablets with portrait and landscape layout. • Backup to Mail or Google Drive. Categories and phrases • Add, change or delete your own categories and phrases. • You can create categories to organize your phrases for quick access. • Long press (optional setting) to easily edit the phrase and category buttons. • Option to Backup and Restore your categories and phrases. Fully Customizable • The size of the buttons, the textbox and the text can be adjusted. • The app has various color schemes and you can also create a personal color scheme. • Give the individual buttons with phrases different colors. Full screen • Show your message full screen with a very large font. • Useful for communicating in a noisy environment. • Button to rotate the text to show your message to the person opposite of you. Other features • Button to share your message to mail, text and social media. • Connect a bluetooth keyboard and create shortcuts for the functions Speak, Clear, Show and Attention Sound. • Option for preventing double tapping by disabling the button (for a short time) after touching. • Undo option in case of unintentionally tapping the clear button. • Attention sound button on Main and Full screen. Voices The voice is not part of the app, but the app uses the voice installed on your device. For example, you can use one of the voices from 'Speech Services by Google'. It has female and male voices in many languages. If it is not available on your device, you can download it from the Google Play Store. You can change the selected voice in the voice settings of the app. Full version The basic version of the app is free. In the settings of the app you can upgrade to the full version. This is a one-time payment for these extra features, there is no subscription. • An unlimited number of categories. • Backup and Restore option. • Option to select symbols from the set of 3400 Mulberry Symbols (mulberrysymbols.org). • Option to change the color of the individual buttons. • History for quick access to previously spoken phrases. • Create user profiles for different languages, situations or persons. • Tabs for easy switching between multiple conversations. • Option to record speech on to a button and to import voice recordings into the app. About the app • The app does not require an internet connection. • For feedback or questions, please contact: android@asoft.nl. • On www.asoft.nl you can find a user manual.

⊟ SCAN LOGS

Timestamp	Event	Error
2025-09-01 14:54:45	Generating Hashes	OK
2025-09-01 14:54:45	Extracting APK	OK

2025-09-01 14:54:45	Unzipping	OK
2025-09-01 14:54:46	Parsing APK with androguard	OK
2025-09-01 14:54:46	Extracting APK features using aapt/aapt2	OK
2025-09-01 14:54:46	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 14:54:48	Parsing AndroidManifest.xml	OK
2025-09-01 14:54:48	Extracting Manifest Data	OK
2025-09-01 14:54:48	Manifest Analysis Started	OK
2025-09-01 14:54:48	Performing Static Analysis on: Speech Assistant (nl.asoft.speechassistant)	OK
2025-09-01 14:54:50	Fetching Details from Play Store: nl.asoft.speechassistant	OK
2025-09-01 14:54:51	Checking for Malware Permissions	OK
2025-09-01 14:54:51	Fetching icon path	OK

2025-09-01 14:54:51	Library Binary Analysis Started	OK
2025-09-01 14:54:51	Reading Code Signing Certificate	OK
2025-09-01 14:54:52	Running APKiD 2.1.5	OK
2025-09-01 14:54:55	Detecting Trackers	OK
2025-09-01 14:54:55	Decompiling APK to Java with JADX	OK
2025-09-01 14:55:00	Converting DEX to Smali	OK
2025-09-01 14:55:00	Code Analysis Started on - java_source	OK
2025-09-01 14:55:01	Android SBOM Analysis Completed	OK
2025-09-01 14:55:07	Android SAST Completed	OK
2025-09-01 14:55:07	Android API Analysis Started	OK
2025-09-01 14:55:13	Android API Analysis Completed	OK

2025-09-01 14:55:14	Android Permission Mapping Started	OK
2025-09-01 14:55:19	Android Permission Mapping Completed	OK
2025-09-01 14:55:20	Android Behaviour Analysis Started	OK
2025-09-01 14:55:28	Android Behaviour Analysis Completed	OK
2025-09-01 14:55:28	Extracting Emails and URLs from Source Code	OK
2025-09-01 14:55:28	Email and URL Extraction Completed	OK
2025-09-01 14:55:28	Extracting String data from APK	OK
2025-09-01 14:55:28	Extracting String data from Code	OK
2025-09-01 14:55:28	Extracting String values and entropies from Code	OK
2025-09-01 14:55:29	Performing Malware check on extracted domains	OK
2025-09-01 14:55:40	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.