MOBSF

ANDROID STATIC ANALYSIS REPORT

Talk to deaf (2.2)

File Name:	Talk to deaf_2.2_APKPure.apk
Package Name:	unique2040.com.text2speech
Scan Date:	Nov. 29, 2024, 4:46 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	2	1	1	0

FILE INFORMATION

File Name: Talk to deaf_2.2_APKPure.apk
Size: 1.27MB
MD5: f14b54c0b2f7a4f73a66037b454da758
SHA1: 89477b9813b815da359b5a4e1a4112113dc5f487
SHA256: 32dcb3d415cac2c4133e647ea30ea0959c74c1744a7c3ded2fd986cde462a565

APP INFORMATION

App Name: Talk to deaf
Package Name: unique2040.com.text2speech
Main Activity: kickdata.speech2text.MainActivity
Target SDK: 30
Min SDK: 15
Max SDK:
Android Version Name: 2.2
Android Version Code: 10

APP COMPONENTS

Activities: 2
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
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: 2018-11-29 16:44:51+00:00
Valid To: 2048-11-29 16:44:51+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xd2fa36ceea4c06be1b413d9797a6bf4c73e10477
Hash Algorithm: sha256
md5: 6bd51079a3d20c4ffdb29ca41b7db531
sha1: ff6fec80ac8067fa669bca16442f28d658164243
sha256: b117d71d1359b9356d45d2d71ad8b8b289b110116a7b12e1744d7ab1e4efb72c
sha512: 1135010c1be130ebb757b2e31b7cce0043d52fa1250f2bdf60f2ec78ce917d4ec942cefe8987fe3f4c945621011a03516b72bbe4cda041382a969258013dfca0
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 375e38d67c8a76ee3285788102e30039ae8b5ffb01da65edef1f25e456c2bdbe
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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
classes.dex	FINDINGS: Compiler DETAILS: unknown (please file detection issue!)

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
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: **1** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.0.3-4.0.4, [minSdk=15]	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.

CODE ANALYSIS

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

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	a/a/k/a/a.java a/a/m/g.java a/e/d/c/b.java a/e/d/c/f.java a/e/e/b.java a/e/e/d.java a/e/e/e.java a/e/e/f.java a/e/e/h.java a/e/e/i.java a/e/l/b.java a/e/l/b0/d.java a/e/l/f.java a/e/l/h.java a/e/l/t.java a/e/l/u.java a/e/l/v.java a/g/b/a.java a/j/a/a/i.java b/a/a/a/a/a/a.java b/a/a/b/k/h.java b/a/a/b/l/a.java kickdata/speech2text/MainActivity.java kickdata/speech2text/a.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	a/e/e/d.java a/e/e/i.java kickdata/speech2text/MainActivity.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	a/e/l/b0/d.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	kickdata/speech2text/MainActivity.java
00022	Open a file from given absolute path of the file	file	kickdata/speech2text/MainActivity.java
00091	Retrieve data from broadcast	collection	b/a/a/a/a/a/a.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	0/25	
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
schemas.android.com	ok	No Geolocation information available.
play.google.com	ok	**IP:** 216.58.211.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

EMAILS

EMAIL	FILE
talktodeafapp@gmail.com	kickdata/speech2text/MainActivity.java

PLAYSTORE INFORMATION

Title: Talk to deaf

Score: 3.99 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Communication **Play Store URL:** unique2040.com.text2speech

Developer Details: KICKDATA, KICKDATA, KICKDATA GMBH Spittelwiese 15 4020 Linz Austria, None, TalkToDeafApp@gmail.com,

Release Date: Nov 29, 2018 **Privacy Policy:** Privacy link

Description:

If one of your friends or loved ones is deaf or has a hearing impairment, it is quite difficult to communicate with them. With this app you can use your phone to translate your speech into text. The deaf person can then easily read your message. Talk to deaf contains the following functions: + Voice input and automatic translation into text + Text entry using the keyboard for entering answers + Font can be enlarged and reduced as desired + the history can be deleted

SCAN LOGS

Timestamp	Event	Error
2024-11-29 16:47:00	Generating Hashes	OK
2024-11-29 16:47:00	Extracting APK	OK
2024-11-29 16:47:00	Unzipping	OK

2024-11-29 16:47:00	Parsing APK with androguard	OK
2024-11-29 16:47:00	Extracting APK features using aapt/aapt2	OK
2024-11-29 16:47:00	Getting Hardcoded Certificates/Keystores	OK
2024-11-29 16:47:03	Parsing AndroidManifest.xml	OK
2024-11-29 16:47:03	Extracting Manifest Data	OK
2024-11-29 16:47:03	Manifest Analysis Started	OK
2024-11-29 16:47:03	Performing Static Analysis on: Talk to deaf (unique2040.com.text2speech)	OK
2024-11-29 16:47:03	Fetching Details from Play Store: unique2040.com.text2speech	OK
2024-11-29 16:47:03	Checking for Malware Permissions	OK
2024-11-29 16:47:03	Fetching icon path	OK

2024-11-29 16:47:03	Library Binary Analysis Started	OK
2024-11-29 16:47:03	Reading Code Signing Certificate	OK
2024-11-29 16:47:04	Running APKiD 2.1.5	OK
2024-11-29 16:47:05	Detecting Trackers	OK
2024-11-29 16:47:06	Decompiling APK to Java with JADX	OK
2024-11-29 16:47:15	Converting DEX to Smali	OK
2024-11-29 16:47:15	Code Analysis Started on - java_source	OK
2024-11-29 16:47:15	Android SBOM Analysis Completed	OK
2024-11-29 16:47:47	Android SAST Completed	OK
2024-11-29 16:47:47	Android API Analysis Started	OK
2024-11-29 16:48:19	Android API Analysis Completed	OK

2024-11-29 16:48:19	Android Permission Mapping Started	OK
2024-11-29 16:48:20	Android Permission Mapping Completed	OK
2024-11-29 16:48:20	Android Behaviour Analysis Started	OK
2024-11-29 16:48:22	Android Behaviour Analysis Completed	OK
2024-11-29 16:48:22	Extracting Emails and URLs from Source Code	OK
2024-11-29 16:48:22	Email and URL Extraction Completed	OK
2024-11-29 16:48:22	Extracting String data from APK	OK
2024-11-29 16:48:22	Extracting String data from Code	OK
2024-11-29 16:48:22	Extracting String values and entropies from Code	OK
2024-11-29 16:48:22	Performing Malware check on extracted domains	OK
2024-11-29 16:48:23	Saving to Database	OK

Report Generated by - MobSF v4.2.8

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.