MOBSF

ANDROID STATIC ANALYSIS REPORT

CoughDrop (2023.11.01)

File Name:	CoughDrop.apk
Package Name:	com.mycoughdrop.coughdrop
Scan Date:	Nov. 17, 2024, 8:10 p.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	8	3	1	1

FILE INFORMATION

File Name: CoughDrop.apk
Size: 19.48MB
MD5: bf12c9f163008eb01b62480f57dc51b5
SHA1: 51b53721c0787b2fb6343c7bd1e1af9bbb35f6f7
SHA256: a30cd8ceab6cb5328d3c9915dd2c9ee51bb071527d656a57fae8a8c49258a3f6

APP INFORMATION

App Name: CoughDrop
Package Name: com.mycoughdrop.coughdrop
Main Activity: com.mycoughdrop.coughdrop.MainActivity
Target SDK: 33
Min SDK: 19
Max SDK:
Android Version Name: 2023.11.01
Android Version Code: 202311010

APP COMPONENTS

Activities: 5
Services: 1
Receivers: 1
Providers: 1
Exported Activities: 0
Exported Services: 1
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=Utah, L=South Jordan, O=CoughDrop, Inc., OU=CoughDrop, CN=Brian Whitmer
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-07-22 19:14:03+00:00
Valid To: 2042-12-07 19:14:03+00:00
Issuer: C=US, ST=Utah, L=South Jordan, O=CoughDrop, Inc., OU=CoughDrop, CN=Brian Whitmer
Serial Number: 0x55afeb7b
Hash Algorithm: sha1
md5: d12560ee38352293a327ed60dbb3a26e
sha1: 47b9de200d71041064b599d64d5fb7d4c5c5b22e
sha256: bcdb42ccfb55d98153f8b49075657516089bf15d635224075748c5947c4d4a2e
sha512: 6c7bf8df9f269233c128c4361b8bba151dcf7583037e3206aa8d9939a8fffef7f64b33c3ea9e4e1666d436cb3add332aa6dc73ad9e2b1f24d709de7d387dd8be
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 56b4aff5467bbaa0dc52e227f6bbdf3a5d5736ada14165c0697814b80dcad331
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.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.RECORD_VIDEO	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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
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.webkit.PERMISSIONREQUEST	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.

APKID ANALYSIS

FILE	DETAILS
classes.dex	<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 possible Build.SERIAL check Build.TAGS check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>r8</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 2 | 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.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 4.4-4.4.4, [minSdk=19]	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] 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.
3	Launch Mode of activity (com.google.android.play.core.missingsplits.PlayCoreMissingSplitsActivity) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

NO	ISSUE	SEVERITY	DESCRIPTION
4	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.

</> CODE ANALYSIS

HIGH: 0 | WARNING: 3 | INFO: 3 | 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	com/acapelagroup/android/tts/acattsandroid.java com/chariotsolutions/nfc/plugin/NfcPlugin.java com/chariotsolutions/nfc/plugin/Util.java com/hutchind/cordova/plugins/launcher/Launcher.java com/mycoughdrop/coughdrop/ExtraTTS.java io/sqlc/SQLiteAndroidDatabase.java io/sqlc/SQLiteConnectorDatabase.java io/sqlc/SQLitePlugin.java org/openaac/cordova_face/CordovaFragment.java uk/co/workingedge/phonegap/plugin/LaunchReview.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	com/verso/cordova/clipboard/Clipboard.java nl/xservices/plugins/SocialSharing.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/mycoughdrop/coughdrop/ExtraTTS.java nl/xservices/plugins/SocialSharing.java
4	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/virtuoworks/cordova/plugin/canvascamera/CanvasCamera.java
5	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	name/ratson/cordova/plugin/SharedPreferencesPlugin.java
6	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	io/sqlc/SQLiteAndroidDatabase.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/mycoughdrop/coughdrop/CoughDropMisc.java com/mycoughdrop/coughdrop/ExtraTTS.java io/sqlc/SQLiteConnectorDatabase.java io/sqlc/SQLitePlugin.java
00005	Get absolute path of file and put it to JSON object	file	com/mycoughdrop/coughdrop/CoughDropMisc.java com/mycoughdrop/coughdrop/ExtraTTS.java io/sqlc/SQLiteConnectorDatabase.java io/sqlc/SQLitePlugin.java
00004	Get filename and put it to JSON object	file collection	com/mycoughdrop/coughdrop/CoughDropMisc.java com/mycoughdrop/coughdrop/ExtraTTS.java com/virtuoworks/cordova/plugin/canvascamera/CanvasCamera.java
00056	Modify voice volume	control	com/mycoughdrop/coughdrop/CoughDropMisc.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/chariotsolutions/nfc/plugin/NfcPlugin.java com/hutchind/cordova/plugins/launcher/Launcher.java nl/xservices/plugins/SocialSharing.java uk/co/workingedge/phonegap/plugin/LaunchReview.java
00091	Retrieve data from broadcast	collection	com/hutchind/cordova/plugins/launcher/Launcher.java org/openaac/cordova_face/CordovaFragment.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/hutchind/cordova/plugins/launcher/Launcher.java nl/xservices/plugins/SocialSharing.java
00015	Put buffer stream (data) to JSON object	file	com/mycoughdrop/coughdrop/ExtraTTS.java

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	com/mycoughdrop/coughdrop/ExtraTTS.java
00013	Read file and put it into a stream	file	com/acapelagroup/android/tts/acattsandroid.java com/mycoughdrop/coughdrop/ExtraTTS.java de/appplant/cordova/plugin/printer/PrintIO.java
00012	Read data and put it into a buffer stream	file	com/mycoughdrop/coughdrop/ExtraTTS.java
00028	Read file from assets directory	file	de/appplant/cordova/plugin/printer/PrintIO.java
00003	Put the compressed bitmap data into JSON object	camera	com/virtuoworks/cordova/plugin/canvascamera/CanvasCamera.java
00183	Get current camera parameters and change the setting.	camera	com/virtuoworks/cordova/plugin/canvascamera/CanvasCamera.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/virtuoworks/cordova/plugin/canvascamera/CanvasCamera.java
00128	Query user account information	collection account	com/acapelagroup/android/tts/acattsandroid.java
00009	Put data in cursor to JSON object	file	io/sqlc/SQLiteAndroidDatabase.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	12/25	android.permission.INTERNET, android.permission.WRITE_SETTINGS, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.RECORD_AUDIO, android.permission.READ_PHONE_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.CAMERA
Other Common Permissions	2/44	android.permission.MODIFY_AUDIO_SETTINGS, android.permission.FOREGROUND_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

DOMAIN	STATUS	GEOLOCATION
api.whatsapp.com	ok	**IP:** 31.13.80.53 **Country:** Canada **Region:** Ontario **City:** Toronto **Latitude:** 43.700111 **Longitude:** -79.416298 **View:** Google Map

EMAILS

EMAIL	FILE
someone@domain.com	nl/xservices/plugins/SocialSharing.java

HARDCODED SECRETS

POSSIBLE SECRETS

308203c7308202afa003020102021500dc286b43b4ea12039958a00a6655eb84720e46c9300d06092a864886f70d01010b05003074310b300906035504061302555331
1330110603550408130a43616c69666f726e6961311163014060355040713 0d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e31103
00e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3137303830343136353333375a170d3437303830343136353333375a3074
310b300906035504061302555331133011060355040813 0a43616c69666f726e6961311163014060355040713 0d4d6f756e7461696e205669657731143012060355040a1
30b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820122300d06092a864886f70d01010105000
382010f003082010a0282010100 8998646f47fc333db09644c303104ed183e904e351152aa66a603b77f63389d45d6fcffae3c94fadf1f28038e265d697fea347327f9081a7f
0b9074d5b148db5bf357c611a77f87f844a15068818bdcd5b21d187e93fa2551676170eedce04a150c35ec0a791eef507fa9b406573c36f6f207764842e5677e35a281a422
659e91e26eb4fecfb053b5c936d0976c37f8757adb57a37953da5844ea350695854d343a61ad341b63a1c425d22855af7ebfee018e1736cee98536be5b9947f288e2a26f9
9eb9f91b5de93fecc513019d2e90f12b38610d1f02eaa81deca4ce91c19cbce36d6c3025ce2432b3d178616beafaf437c08451bc469c6bc6f4517a714a5b0203010001a350
304e300c0603551d13040530030101ff301d0603551d0e0416041419a864c0f2618c67c803a23da909bc70521f269b301f0603551d2304183016801419a864c0f2618c67c8
03a23da909bc70521f269b300d06092a864886f70d01010b0500038201010054 03fc56fdefc440376a0337815002b96a15bffc2fe42de6c58f52fae4d80652e3704455b885
409eef81ffbb4c44dba104b6b8e24c9e2e0e7a04338ee73baa5b71bfb4488f8e04bef3d0eaf7d43aa42b03b278c33cc1f0dd3802571624baa161d851fab37db4bc92b9094
b6885dff62b400ecd81f069d56a1be1db46d8198c50c9628cdb6e38686ef640fd386775f50376f957e24ea45ed1942968f20c82f189607fdb22f11cfdfd0760a77a60ceb341
6cfb3f48f13f9f83f3834a01001750a7c78bc1fd81f0b53a7c41dcba9f5a0118259d083c32bb9ebb84d645d6f6b9c31923d8ab70e7f0a25940ecc9f4945144419f86e8c421d3
b99774f4b8f3d09262e7

PLAYSTORE INFORMATION

Title: CoughDrop AAC

Score: 3.863158 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Education **Play Store URL:** com.mycoughdrop.coughdrop

Developer Details: CoughDrop, Inc., CoughDrop,+Inc., 9733 Sharolyn Ln. South Jordan, UT 84009, https://www.coughdrop.com, info@coughdrop.com,

Release Date: Sep 14, 2015 **Privacy Policy:** Privacy link

Description:

CoughDrop is a simple, modern AAC communication and support tool that empowers individuals and the teams around them through a paid coughdrop.com account. It is a premium, full-featured communication app built for individuals with autism, cerebral palsy, Down syndrome, Angelman syndrome, Rett syndrome, or other complex communication needs. CoughDrop is flexible and configurable enough to work with the access and comprehension needs of many communicators. PLEASE NOTE: CoughDrop can be installed without purchasing, but a coughdrop.com account is required to log in, and functionality will become limited after the two-month trial period has ended. The app includes starter boards for different levels of communication, and boards with large or small buttons can be personalized using the rich symbol set, user-provided images or camera photos, user-recorded audio, speech synthesis, etc. CoughDrop runs on multiple devices, so you can log in on your tablet, phone and computer and have access to the same communication tools and interface. In addition, users can be linked so parents, therapists and supervisors can access a communicator's boards from their own devices to better facilitate modeling, and to make it easier to modify boards without taking away the communicator's device. The

built-in reporting and messaging tools also help the support team have a consistent strategy and know what's working across locations and times.

SCAN LOGS

Timestamp	Event	Error
2024-11-17 20:10:59	Generating Hashes	OK
2024-11-17 20:10:59	Extracting APK	OK
2024-11-17 20:10:59	Unzipping	OK
2024-11-17 20:10:59	Getting Hardcoded Certificates/Keystores	OK
2024-11-17 20:10:59	Parsing APK with androguard	OK
2024-11-17 20:11:00	Parsing AndroidManifest.xml	OK
2024-11-17 20:11:00	Extracting Manifest Data	OK
2024-11-17 20:11:00	Performing Static Analysis on: CoughDrop (com.mycoughdrop.coughdrop)	OK

2024-11-17 20:11:00	Fetching Details from Play Store: com.mycoughdrop.coughdrop	OK
2024-11-17 20:11:00	Manifest Analysis Started	OK
2024-11-17 20:11:00	Checking for Malware Permissions	OK
2024-11-17 20:11:00	Fetching icon path	OK
2024-11-17 20:11:00	Library Binary Analysis Started	OK
2024-11-17 20:11:00	Reading Code Signing Certificate	OK
2024-11-17 20:11:01	Running APKiD 2.1.5	OK
2024-11-17 20:11:02	Updating Trackers Database....	OK
2024-11-17 20:11:02	Detecting Trackers	OK
2024-11-17 20:11:02	Decompiling APK to Java with JADX	OK
2024-11-17 20:11:06	Converting DEX to Smali	OK

2024-11-17 20:11:06	Code Analysis Started on - java_source	OK
2024-11-17 20:11:06	Android SAST Completed	OK
2024-11-17 20:11:06	Android API Analysis Started	OK
2024-11-17 20:11:06	Android API Analysis Completed	OK
2024-11-17 20:11:06	Android Permission Mapping Started	OK
2024-11-17 20:11:08	Android Permission Mapping Completed	OK
2024-11-17 20:11:08	Email and URL Extraction Completed	OK
2024-11-17 20:11:08	Android Behaviour Analysis Started	OK
2024-11-17 20:11:08	Android Behaviour Analysis Completed	OK
2024-11-17 20:11:08	Extracting String data from APK	OK
2024-11-17 20:11:08	Extracting String data from Code	OK

2024-11-17 20:11:08	Extracting String values and entropies from Code	OK
2024-11-17 20:11:08	Performing Malware check on extracted domains	OK
2024-11-17 20:11:09	Saving to Database	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.