ANDROID STATIC ANALYSIS REPORT

SOS CORONA (0.0.6)

File Name:	SOS CORONA 0.0.6.apk
Package Name:	io.ageticmali.soscovid
Average CVSS Score:	5.5
App Security Score:	35/100 (HIGH RISK)
Trackers Detection:	4/285

FILE INFORMATION

File Name: SOS CORONA 0.0.6.apk
Size: 12.35MB
MD5: a78f45b2d83b63c97caf7972b631b15b
SHA1: 435cd7f7d7bf118c3bc8f14ddf2c3864def84c60
SHA256: 3aaf6f8869458341003d25e5a04eb9f353165fd7676b37966baa131411c5eef1

APP INFORMATION

App Name: SOS CORONA
Package Name: io.ageticmali.soscovid
Main Activity: io.ageticmali.soscovid.MainActivity
Target SDK: 28
Min SDK: 19
Max SDK:
Android Version Name: 0.0.6
Android Version Code: 6

APP COMPONENTS

Activities: 7
Services: 7
Receivers: 5
Providers: 5
Exported Activities: 2
Exported Services: 2
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-03-18 00:46:40+00:00
Valid To: 2050-03-18 00:46:40+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x820ec7da4e93c5809816eb1a38be477d5cbd7b4e
Hash Algorithm: sha256
md5: 3695e977939690f623c931dee8b18050
sha1: 23729a8eba971ff00dbcb2d98f4ab34aaa2a9340
sha256: 5a3b4e88ed28200d1aa615805c5445f8ee41e0e8da0b46ec374dc5eba587ae98
sha512:
```

9501fe0d7492647f930170d892fd7b8850ec6febecd98d02efefcb1b3a6514bcf19bc485d43159e4545a91621c679e45fe2ecfc544cd9d89f114b7f34d2229ce

PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 8f125817a1ad7213e3ff22fa3dbf5c28555abbd902aaf166c3b42c63cd26f134

Certificate Status: Good
Description: Certificate looks good.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.MODIFY_AUDIO_SETTINGS	dangerous	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.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
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.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
com.google.android.providers.gsf.permission.READ_GSERVICES	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.

SHARED LIBRARY BINARY ANALYSIS

ISSUE	SEVERITY	DESCRIPTION	FILES
Found elf built without Position Independent Executable (PIE) flag	high	In order to prevent an attacker from reliably jumping to, for example, a particular exploited function in memory, Address space layout randomization (ASLR) randomly arranges the address space positions of key data areas of a process, including the base of the executable and the positions of the stack, heap and libraries. Built with option <strong>-pie</strong>.	lib/mips64/libtbxml.so

APKID ANALYSIS

<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
possible Build.SERIAL check
Build.TAGS 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.google.android.gms.tagmanager.TagManagerPreviewActivity	Schemes: tagmanager.c.io.ageticmali.soscovid://,

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION

ISSUE	SEVERITY	DESCRIPTION
App has a Network Security Configuration [android:networkSecurityConfig]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
Application Data can be Backed up [android:allowBackup] flag is missing.	medium	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.
Service (org.apache.cordova.firebase.FirebasePluginMessagingService) is not Protected. An intent-filter exists.	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Service is explicitly exported.
Broadcast Receiver (nl.xservices.plugins.ShareChooserPendingIntent) is not Protected. An intent-filter exists.	high	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
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]	high	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.
Activity (com.google.android.gms.tagmanager.TagManagerPreviewActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

ISSUE	SEVERITY	DESCRIPTION
Launch Mode of Activity (com.google.firebase.auth.internal.FederatedSignInActivity) is not standard.	high	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.
Activity (com.google.firebase.auth.internal.FederatedSignInActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.firebase.auth.api.gms.permission.LAUNCH_FEDERATED_SIGN_IN [android:exported=true]	high	An Activity 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.
Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	high	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.
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]	high	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

ISSUE	SEVERITY	STANDARDS	FILES
MD5 is a weak hash known to have hash collisions.	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-4	okio/Buffer.java
The App logs information. Sensitive information should never be logged.	info	**CVSS V2:** 7.5 (high) **CWE:** CWE-532 - Insertion of Sensitive Information into Log File **OWASP MASVS:** MSTG-STORAGE-3	io/sqlc/SQLiteAndroidDatabase.java io/sqlc/SQLiteConnectorDatabase.java io/sqlc/SQLitePlugin.java plugin/google/maps/PluginLocationService.java plugin/google/maps/MyPluginLayout.java plugin/google/maps/CordovaGoogleMaps.java plugin/google/maps/PluginEnvironment.java plugin/google/maps/PluginMap.java plugin/google/maps/MyPlugin.java plugin/google/maps/PluginMarkerCluster.java plugin/google/maps/AsyncLoadImage.java plugin/google/maps/PluginMarker.java defpackage/NativeStorage.java defpackage/Crypto.java com/rjfun/cordova/plugin/nativeaudio/NativeAudio.java com/phonegap/plugins/barcodescanner/BarcodeScanner.java com/ionicframework/cordova/webview/WebViewLocalServer.java com/ionicframework/cordova/webview/AndroidProtocolHandler.java com/ionicframework/cordova/webview/IonicWebViewEngine.java
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.	high	**CVSS V2:** 5.9 (medium) **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

ISSUE	SEVERITY	STANDARDS	FILES
This App uses Java Hash Code. It's a weak hash function and should never be used in Secure Crypto Implementation.	warning	**CVSS V2:** 2.3 (low) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP MASVS:** MSTG-CRYPTO-4	plugin/google/maps/PluginLocationService.java plugin/google/maps/PluginMap.java plugin/google/maps/PluginTileProvider.java plugin/google/maps/PluginUtil.java plugin/google/maps/AsyncLoadImage.java plugin/google/maps/PluginGroundOverlay.java plugin/google/maps/PluginMarker.java
IP Address disclosure	warning	**CVSS V2:** 4.3 (medium) **CWE:** CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor **OWASP MASVS:** MSTG-CODE-2	plugin/google/maps/PluginKmlOverlay.java plugin/google/maps/PluginTileProvider.java plugin/google/maps/AsyncLoadImage.java
App can read/write to External Storage. Any App can read data written to External Storage.	high	**CVSS V2:** 5.5 (medium) **CWE:** CWE-276 - Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2	nl/xservices/plugins/SocialSharing.java
This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	**CVSS V2:** 0 (info) **OWASP MASVS:** MSTG-STORAGE-10	nl/xservices/plugins/SocialSharing.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
127.0.0.1	good	**IP:** 127.0.0.1 **Country:** - **Region:** - **City:** - **Latitude:** 0.0 **Longitude:** 0.0 **View:** Google Map
api.whatsapp.com	good	**IP:** 157.240.8.53 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	good	**IP:** 216.58.196.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
soscovid.firebaseio.com	good	**IP:** 35.201.97.85 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

URLS

URL	FILE
data:image http://localhost http://127.0.0.1 http://.+?/ file:///android_asset/www/ file:///android_asset/	plugin/google/maps/PluginKmlOverlay.java
http://play.google.com/store/apps/details?id=com.google.android.gms	plugin/google/maps/CordovaGoogleMaps.java
http://play.google.com/store/apps/details?id=com.google.android.gms	plugin/google/maps/PluginEnvironment.java
data:image/ data:image/png;base64, javascript:if(window.cordova){cordova.fireDocumentEvent('plugin_touch', javascript:if('%s'	plugin/google/maps/PluginMap.java
javascript:if('%s'	plugin/google/maps/PluginStreetViewPanorama.java
javascript:plugin.google.maps.Map._onOverlayEvent('	plugin/google/maps/MyPlugin.java
javascript:if(window.cordova){cordova.fireDocumentEvent('%s-%s-tileoverlay', data:image/ http://localhost http://127.0.0.1 http://.+?/ file:///android_asset/www/ file:///android_asset/	plugin/google/maps/PluginTileProvider.java

URL	FILE
data:image http://localhost http://127.0.0.1 http://.+?/ file:///android_asset/www/ file:///android_asset/ data:image/	plugin/google/maps/AsyncLoadImage.java
data:image/ https://api.whatsapp.com/send?phone=	nl/xservices/plugins/SocialSharing.java
javascript:(function()	com/ionicframework/cordova/webview/IonicWebViewEngine.java
https://soscovid.firebaseio.com	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://soscovid.firebaseio.com	info App talks to a Firebase Database.

EMAILS

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

TRACKERS

TRACKER	URL
Google Analytics	https://reports.exodus-privacy.eu.org/trackers/48
Google CrashLytics	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	https://reports.exodus-privacy.eu.org/trackers/49
Google Tag Manager	https://reports.exodus-privacy.eu.org/trackers/105

PLAYSTORE INFORMATION

Title: SOS CORONA

Score: 4.1754384 **Installs:** 10,000+ **Price:** 0 **Android Version Support:** 4.4 and up **Category:** Communication **Play Store URL:** io.ageticmali.soscovid

Developer Details: AGETIC DEV, AGETIC+DEV, None, https://agetic.gouv.ml, info@agetic.gouv.ml,

Release Date: Mar 17, 2020 **Privacy Policy:** Privacy link

Description:

Cette application a été conçue par le Ministère de l'Economie Numérique et de la Prospective à travers L'AGETIC et en partenariat avec le Ministère de la Santé et des Affaires Sociales, afin d'informer et de sensibiliser la population sur les dangers du covid-19 et assurer une meilleure prise en charge des cas suspects.

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

Report Generated by - MobSF v3.0.8 Beta

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.