MOBSF

ANDROID STATIC ANALYSIS REPORT

CoronaVirus Algérie (1.0.3)

File Name:	CoronaVirus Algérie 1.0.3.apk
Package Name:	com.covid19_algeria
Average CVSS Score:	6.0
App Security Score:	30/100 (HIGH RISK)
Trackers Detection:	1/285

FILE INFORMATION

File Name: CoronaVirus Algérie 1.0.3.apk
Size: 4.56MB
MD5: c854f177adf98457525c8601794a1ab4
SHA1: 9b19d24285e20e4a012ff58309fb010da6d04644
SHA256: 2ed816c3bad3dff96a1d323704b747ecf4066fc989fe1d21cd67f0ce0e4e8ded

APP INFORMATION

App Name: CoronaVirus Algérie
Package Name: com.covid19_algeria
Main Activity: com.covid19_algeria.MainActivity
Target SDK: 28
Min SDK: 16
Max SDK:
Android Version Name: 1.0.3
Android Version Code: 3145731

APP COMPONENTS

Activities: 3
Services: 6
Receivers: 6
Providers: 1
Exported Activities: 0
Exported Services: 0
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
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: 2020-03-19 11:11:13+00:00
Valid To: 2050-03-19 11:11:13+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x2cbe68bb9e473b64edd1f41f65251f3783a43155
Hash Algorithm: sha256
md5: 2185765f77855b65fcb94188a502c2a1
sha1: 3a9f75c9c11f6f9af01d1730a193b5ff5e54b7d7
sha256: 563307738e4cc488ef6872c0b4a2cf53553fc24e24a11cf76068ddf5abcc62a5
sha512:
9398a00b71365f2a80b1c26f866b4cc9cf738e3d9b95a2c2d15a39e01e9457eae05624e04e3dba80dd7998c524c4abe9e784ae666f7adcb922b59d13cf152195

PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 6036412971a36bee3c4b69b63ec0e6c6c9f4af0cdd7e2e029e37b31fc47089a7

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.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.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.covid19_algeria.permission.C2D_MESSAGE	signature	Allows cloud to device messaging	Allows the application to receive push notifications.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	dangerous	Unknown permission from android reference	Unknown permission from android reference
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read SD card contents	Allows an application to read from SD Card.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.sec.android.provider.badge.permission.READ	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.sec.android.provider.badge.permission.WRITE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.htc.launcher.permission.READ_SETTINGS	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.htc.launcher.permission.UPDATE_SHORTCUT	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.sonyericsson.home.permission.BROADCAST_BADGE	dangerous	Unknown permission from android reference	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.anddoes.launcher.permission.UPDATE_COUNT	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.majeur.launcher.permission.UPDATE_BADGE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.huawei.android.launcher.permission.CHANGE_BADGE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.huawei.android.launcher.permission.READ_SETTINGS	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.huawei.android.launcher.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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check network operator name check possible VM check FINDINGS: Compiler — DETAILS: dx

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
Launch Mode of Activity (com.covid19_algeria.MainActivity) 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.
Broadcast Receiver (com.google.android.gms.gcm.GcmReceiver) 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.
Broadcast Receiver (com.dieam.reactnativepushnotification.modules.RNPushNotificationBootEventReceiver) 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.
Broadcast Receiver (com.learnium.RNDeviceInfo.RNDeviceReceiver) is not Protected. [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.
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
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	me/leolin/shortcutbadger/ShortcutBadger.java me/leolin/shortcutbadger/impl/HuaweiHomeBadger.java com/dieam/reactnativepushnotification/modules/RNPushNotification.java com/dieam/reactnativepushnotification/modules/RNPushNotificationListenerService.java com/dieam/reactnativepushnotification/modules/RNPushNotificationConfig.java com/dieam/reactnativepushnotification/modules/RNPushNotificationBootEventReceiver.java com/dieam/reactnativepushnotification/modules/RNPushNotificationRegistrationService.java com/dieam/reactnativepushnotification/modules/RNPushNotificationPublisher.java com/dieam/reactnativepushnotification/modules/RNPushNotificationListenerServiceGcm.java com/dieam/reactnativepushnotification/modules/RNPushNotificationAttributes.java com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java com/dieam/reactnativepushnotification/helpers/ApplicationBadgeHelper.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/swmansion/reanimated/nodes/DebugNode.java com/swmansion/gesturehandler/react/RNGestureHandlerRootHelper.java com/swmansion/gesturehandler/react/RNGestureHandlerRootView.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/resolver/DeviceIdResolver.java com/agontuk/RNFusedLocation/RNFusedLocationModule.java com/agontuk/RNFusedLocation/SingleLocationUpdate.java
The App uses an insecure Random Number Generator.	high	CVSS V2: 7.5 (high) CWE: CWE-330 - Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/dieam/reactnativepushnotification/modules/RNPushNotification.java com/dieam/reactnativepushnotification/modules/RNPushNotificationListenerService.java com/dieam/reactnativepushnotification/modules/RNPushNotificationListenerServiceGcm.java

ISSUE	SEVERITY	STANDARDS	FILES
Files may contain hardcoded sensitive informations like usernames, passwords, keys etc.	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-312 - Cleartext Storage of Sensitive Information **OWASP Top 10:** M9: Reverse Engineering **OWASP MASVS:** MSTG-STORAGE-14	com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java
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	com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java com/reactcommunity/rnlocalize/RNLocalizeModule.java com/oblador/vectoricons/VectorIconsModule.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	com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.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	com/learnium/RNDeviceInfo/RNDeviceModule.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
c19-algeria.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
https://c19-algeria.firebaseio.com	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://c19-algeria.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

TRACKER	URL
Google Firebase Analytics	https://reports.exodus-privacy.eu.org/trackers/49

PLAYSTORE INFORMATION

Title: Coronavirus Algérie

Score: 3.1 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** 4.1 and up **Category:** Health & Fitness **Play Store URL:** com.covid19_algeria

Developer Details: Algerian Ministry of Startups, Algerian+Ministry+of+Startups, None, None, algerianministryofstartups@gmail.com,

Release Date: Mar 20, 2020 **Privacy Policy:** Privacy link

Description:

Application officielle pour lutter contre le coronavirus en Algérie, installez l'application pour rester au courant de l'évolution de la maladie, envoyez des alertes aux structures de santé de proximité si vous présentez des symptômes de la maladie, et recevez des notifications si une personne dans votre entourage est porteuse du virus

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.