MOBSF

ANDROID STATIC ANALYSIS REPORT

COVID Alert NJ (1.1.4)

File Name:	COVID Alert NJ_v1.1.4_apkpure.com.xapk
Package Name:	com.nj.gov.covidalert
Average CVSS Score:	0
App Security Score:	100/100 (LOW RISK)
Scan Date:	Feb. 20, 2022, 4:58 p.m.

FILE INFORMATION

File Name: COVID Alert NJ_v1.1.4_apkpure.com.xapk
Size: 4.92MB
MD5: 3804261c16ef7c205d051632633a1c1f
SHA1: b9de351280820d858338ded3409a26a30d91353b
SHA256: e2ffb38d4b4cee57e5cf7b83db5b072f26c109dd78b5b66e2ba6cd31c91b8679

APP INFORMATION

App Name: COVID Alert NJ
Package Name: com.nj.gov.covidalert
Main Activity: com.nj.gov.covidalert.MainActivity
Target SDK: 29
Min SDK: 23
Max SDK:
Android Version Name: 1.1.4
Android Version Code: 40

APP COMPONENTS

Activities: 2
Services: 11
Receivers: 15
Providers: 4
Exported Activities: 0
Exported Services: 3
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=IE, ST=Ireland, L=Waterford, O=NearForm Ltd, OU=Ops, CN=Colm Harte
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-09-01 11:37:39+00:00
Valid To: 2045-08-26 11:37:39+00:00

Issuer: C=IE, ST=Ireland, L=Waterford, O=NearForm Ltd, OU=Ops, CN=Colm Harte
Serial Number: 0x1faffe38
Hash Algorithm: sha256
md5: b5b7b188e8eb9ffe0ef605607ec537c2
sha1: 75841b7432b7669316cd57dec3e57c4353db581f
sha256: 28da15cffb3ad39ad5841eda581306d2dcc02a21af409954100177ab93562a7f
sha512: f2085f9220e00fb9537fab00fd2960e2cbf2ebbc8b686df892d77891adc8b2903d8851be76cc432d21c8660937ea641adf01661b7d9c77e9eb4630db706f8d8c
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: b81b642162d4a56b63394e2bf639c63b000e9e3b61d08f3e9a0744c3306b0b8b

STATUS	DESCRIPTION
secure	Application is signed with a code signing certificate
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.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check possible Build.SERIAL check FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.nj.gov.covidalert.MainActivity	Schemes: com.nj.gov.covidalert://, https://, Hosts: us-nj.en.express,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Broadcast Receiver (ie.gov.tracing.nearby.ExposureNotificationBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.nearby.exposurenotification.EXPOSURE_CALLBACK [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.
3	Service (com.google.android.gms.nearby.exposurenotification.WakeUpService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.nearby.exposurenotification.EXPOSURE_CALLBACK [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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	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.
5	Service (androidx.work.impl.background.gcm.WorkManagerGcmService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.BIND_NETWORK_TASK_SERVICE [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.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [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.
7	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [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

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.zetetic.net	good	**IP:** 65.8.68.51 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
expo.io	good	**IP:** 34.132.55.135 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	good	**IP:** 140.82.112.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
schemas.android.com	good	No Geolocation information available.

URLS

URL	FILE
data:image	com/bumptech/glide/load/o/e.java
https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenFragment.java
https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenStackFragment.java
http://schemas.android.com/apk/res/android	f/h/e/e/g.java
https://expo.io	i/a/j/i.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	j/a/b.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	j/a/g/e.java

URL	FILE
https://www.zetetic.net/sqlcipher/ https://www.zetetic.net/sqlcipher/license/ https://github.com/sqlcipher/android-database-sqlcipher	Android String Resource

HARDCODED SECRETS

POSSIBLE SECRETS
"library_android_database_sqlcipher_author" : "Zetetic, LLC"
"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"

PLAYSTORE INFORMATION

Title: COVID Alert NJ

Score: 3.9705882 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** 6.0 and up **Category:** Health & Fitness **Play Store URL:** com.nj.gov.covidalert

Developer Details: State of New Jersey Applications, State+of+New+Jersey++Applications, None, https://covid19.nj.gov/index.html, COVIDapp@doh.nj.gov,

Release Date: Sep 18, 2020 **Privacy Policy:** Privacy link

Description:

COVID Alert NJ App is being made available by the New Jersey Department of Health (DOH) to complement New Jersey's comprehensive COVID-19 contact tracing effort. COVID Alert NJ is a free and secure mobile phone app that allows New Jerseyans: 1. To be alerted if they have been in close contact with another app user who has tested positive for COVID-19 – even if that person is a stranger 2. To track their symptoms and get advice on what to do to protect themselves and others 3. To be able to anonymously warn other app users whom they were in close contact with, if they tested positive for COVID-19 – especially people they do not know or remember being in close contact with (e.g., during bus/train ride, at public places) 4. To monitor the latest information and statistics related to the COVID-19 pandemic 5. To reach NJ public health representatives and be connected with support services For all this to work, all you have to do is push "Allow" COVID-19 Exposure Notification Services (ENS) on your phone within your App. You can also choose to "Allow" your phone to turn on the COVID-19 Exposure Notification Services (ENS) and also "Allow" your phone to display

notifications so that you also receive an alert that you have been exposed to someone who has tested positive for COVID-19. You can also turn off this functionality, at any time, in the Settings page of the App. In the event you receive an Exposure Notification, you may read NJ DOH advice under Exposure Notification Information or get in touch with a public health representative. It is important to note that COVID Alert NJ will never reveal the identity of any person using the app to other app users, and never reveals who has been diagnosed as positive for COVID-19. Help us Stop the Spread of COVID-19 in New Jersey. Share this app with your friends and family. The use of this App is entirely voluntary and it is available to download for free from the Google Play Store. The App runs Android phones running Android 6.0 and higher. The App is not intended for use by persons under 18 years of age, as they are considered not to have reached the digital age of consent or agreement with the State of New Jersey. You will be asked to confirm that you are 18 years or older after you download the App. View our privacy policy here:
https://www.nj.gov/health/documents/DPP_COVIDALERTNJ.pdf

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 v3.4.5 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.