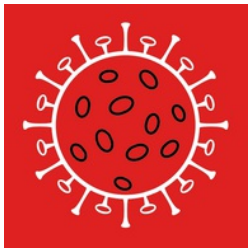
MOBSF

ANDROID STATIC ANALYSIS REPORT



COVID-19! (0.9.4)

File Name:	COVID-19! 0.9.4.apk
Package Name:	cz.nmbbrno.covid
Average CVSS Score:	6.7
App Security Score:	85/100 (LOW RISK)

FILE INFORMATION

File Name: COVID-19! 0.9.4.apk
Size: 20.82MB
MD5: c7813b2f24f48169138c272898d3b494
SHA1: 3cf30eb0bb6ebd9b427388c40c4d2de24275eb58
SHA256: 98ef69a94dbf6d7d59dcd61b5acfdec957a725c856ebcb2630e66f4802fe8f77

APP INFORMATION

App Name: COVID-19!
Package Name: cz.nmbbrno.covid
Main Activity: cz.nmbbrno.covid.MainActivity
Target SDK: 28
Min SDK: 19
Max SDK:
Android Version Name: 0.9.4
Android Version Code: 904

APP COMPONENTS

Activities: 1
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=CZ, ST=Moravskoslezsky kraj, L=Frydek-Mistek, O=Emglare Technologies, OU=HQ, CN=Matej Bacik
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-09-06 07:26:59+00:00
Valid To: 2038-08-31 07:26:59+00:00
Issuer: C=CZ, ST=Moravskoslezsky kraj, L=Frydek-Mistek, O=Emglare Technologies, OU=HQ, CN=Matej Bacik
Serial Number: 0x522983c3
Hash Algorithm: sha1
md5: 83e59006639700410bb090dc9d828816
sha1: bc0274d33d4b3db5694da06361cb9706dd0ac592
sha256: 525c15934e337ab5cecee177bf958e43cae7c1a4079feab3e346d043ece800d6
sha512:
0ef36899928157ce5d9aa5f3500919e53c6d249857052e9a90f7fdf09a009e4f3be4eb8ebc7d9a2f2ebbbf8a6f3838e45ce3dcf1c0d15024b438113b3e8e9a13

Certificate Status: Bad
Description: The app is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible Build.SERIAL check FINDINGS: Anti Debug Code — DETAILS: Debug.isDebuggerConnected() check FINDINGS: Compiler — DETAILS: dx

MANIFEST ANALYSIS

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.

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	io/sqlc/SQLiteAndroidDatabase.java io/sqlc/SQLiteConnectorDatabase.java io/sqlc/SQLitePlugin.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

URLS

URL	FILE
javascript:(function()	com/ionicframework/cordova/webview/IonicWebViewEngine.java

PLAYSTORE INFORMATION

Title: COVID-19! - The current spread of disease

Score: 3.375 **Installs:** 10,000+ **Price:** 0 **Android Version Support:** 4.4 and up **Category:** Medical **Play Store URL:** cz.nmbbrno.covid

Developer Details: Nemocnice Milosrdnych bratri, p.o., Nemocnice+Milosrdnych+bratri,+p.o., Polni 553/3 639 00 Brno Czech Republic, https://nmbbrno.cz, info@nmbbrno.cz,

Release Date: Mar 28, 2020 **Privacy Policy:** Privacy link

Description:

Applications COVID-19 helps to obtain basic information about the disease, how to prevent and how to defend against it. Also bring you news from home and around the world. With the app, you have all the basic information you need to know about the infection on your phone. The Brothers of Charity Hospital, p.o. in Brno. Under the auspices of expertise we have gained information about the disease, how to identify it and how to defend it. The app contains constant up-to-date information about the infection in numbers, both worldwide and within the selected country. These basic numerical information is supplemented with the latest information and news. You will find a map of the occurrence of COVID-19 and within the map you can display information about a specific country throughout the world.

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.