



ANDROID STATIC ANALYSIS REPORT



COVID Tracker Ireland (1.0.1.44)

File Name:	com.covidtracker.hse.apk
Package Name:	com.covidtracker.hse
Average CVSS Score:	0
App Security Score:	100/100 (LOW RISK)
VirusTotal Detection:	0/62



FILE INFORMATION

File Name: com.covidtracker.hse.apk
Size: 4.25MB
MD5: ef86c01ed30b11fd45ee6307ccfb78a2
SHA1: 49e4a87daea80eb28d07b1a1be23d9e7124b1afc
SHA256: 0674b431a0524d7c744c374c5a5845935981564e599b6eb9c044911cf31a28ff

i APP INFORMATION

App Name: COVID Tracker Ireland
Package Name: com.covidtracker.hse
Main Activity: com.covidtracker.hse.MainActivity
Target SDK: 28
Min SDK: 23
Max SDK:
Android Version Name: 1.0.1.44
Android Version Code: 61



APP COMPONENTS

Activities: 3
Services: 9
Receivers: 10
Providers: 4
Exported Activities: 0
Exported Services: 2
Exported Receivers: 2
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: 2020-04-17 15:44:58+00:00
Valid To: 2050-04-17 15:44:58+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x5e78e6ce703b9d4d519ac6b7af5c135dfb4604d6
Hash Algorithm: sha256
md5: a3fda59fec7835c838108dd46ed351b4
sha1: 63cd45255d10107b4edc364cf94d3cb503c47874
sha256: 1407a740ce0ac762de781e8b2cc42cf64389a1903de4fee1a12fc19054e9058d
sha512:

df04b88e40fa1923cd059ad36d8ab747ba6416e1017e91dd5a2c8a71e6f5937315dba8b97984032387fdb329aaa7ec8d04cb63717119af11aeaab19e8257838e

PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 46e69ffd12fa7f2a449ea6558cd9a24200819bffe06f9bae5e945be765051e53

Certificate Status: Good
Description: Certificate looks good.

≡ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH	dangerous	create Bluetooth connections	Allows an application to view configuration of the local Bluetooth phone and to make and accept connections with paired devices.
android.permission.INTERNET	dangerous	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.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.

🕷 VIRUSTOTAL SCAN

0 / 62 AVs found this file Malicious!

📶 APKID ANALYSIS

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check possible Build.SERIAL check
	Compiler	dx

🔍 MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION

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.
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.
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.
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
-------	----------	-----------	-------

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

www.zetetic.net	good	IP: 52.85.104.126 Country: United States of America Region: New York City: New York City Latitude: 40.714272 Longitude: -74.005966 View: Google Map
github.com	good	IP: 140.82.118.3 Country: United States of America Region: California City: San Francisco Latitude: 37.7757 Longitude: -122.395203 View: Google Map

URLs

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

PLAYSTORE INFORMATION

Title: COVID Tracker Ireland

Score: 2.6 **Installs:** 500,000+ **Price:** Free **Android Version Support:** 6.0 and up **Category:** Medical **Play Store URL:** [com.covidtracker.hse](https://play.google.com/store/apps/details?id=com.covidtracker.hse)

Developer Details: Health Service Executive (HSE), Health Service Executive (HSE), HSE Communications 10/11 Cornmarket Dublin D08X8C6 Ireland, <https://covidtracker.ie>, digital@hse.ie,

Release Date: 2020-07-15 **Privacy Policy:** [Privacy link](#)

Description:

COVID-19 is here. The HSE and the Government of Ireland is asking everyone to help tackle coronavirus by downloading and using the COVID Tracker app every day. Using the app will give us a better picture of the spread of the virus help carry out contact tracing link you to excellent HSE health advice if you need it keep you updated with notifications you can trust How the Covid Tracker app helps us Daily health check-in The Covid Tracker app allows you to check-in every day, to let us know if you have any cold, flu or coronavirus symptoms, or if you're feeling well. This will help us map the spread of the virus in Ireland. Understanding how the virus is affecting the country will help us to manage and respond to this pandemic. Contact tracing The app uses your phone's technology to make a record of when you are close to other app users. If an app user tests positive for COVID-19, the HSE can ask them for the records on the app. This will help us to contact other people who might have been affected, and give them the advice and help they need. Your data and privacy The COVID Tracker app will not: publicly identify anyone with COVID-19 make personal data available to the HSE without your direct consent use your data for any reason other than contact tracing and anonymously reporting illness levels Be part of this national effort Use this app for 1 minute a day to make an important contribution to the fight against coronavirus. Protect yourself, your family, your community and the most vulnerable in society. Encourage everyone you know to download and use the COVID Tracker app where possible. Protection from Coronavirus. It's in our hands.

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 v3.0.9 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.

© 2020 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).