MOBSF

ANDROID STATIC ANALYSIS REPORT

COVID Alert (1.5.3)

File Name:	ca.gc.hcsc.canada.stopcovid.apk
Package Name:	ca.gc.hcsc.canada.stopcovid
Average CVSS Score:	0
App Security Score:	100/100 (LOW RISK)
Scan Date:	June 3, 2022, 2:55 a.m.

FILE INFORMATION

File Name: ca.gc.hcsc.canada.stopcovid.apk
Size: 8.71MB
MD5: a7b9ed08b05a99e6cb5d41f179fef23a
SHA1: 82396fe4f7f8b1537fcf3c9fb536944f2ef1ef13
SHA256: 180a1a9db2d2e71fb83764d045eec80f099404077b916960ce34ae95b12138bf

APP INFORMATION

App Name: COVID Alert
Package Name: ca.gc.hcsc.canada.stopcovid
Main Activity: app.covidshield.MainActivity
Target SDK: 29
Min SDK: 23
Max SDK:
Android Version Name: 1.5.3
Android Version Code: 380

APP COMPONENTS

Activities: 2
Services: 6
Receivers: 11
Providers: 1
Exported Activities: 0
Exported Services: 3
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: 2020-06-23 00:32:33+00:00
Valid To: 2050-06-23 00:32:33+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x9a7e1336651ebe93279047642065917514 79bd55
Hash Algorithm: sha256
md5: b92a1e088a4bb045cbad7d20f3d80325
sha1: c54d96c4dbcfb1eba8dd939bae8106a143a96433
sha256: f166bc40b72ba26aa6b02f7ee977637cb1a3585550227d95ea2b22896a999222
sha512: 2942bd5ec2ac36df7026ba28ef198841bd53ae98f59a1acf85563176957f6ba4ddad9bb14d0d66aa7cc7a300eccc0164fdde986acf4e8b0577854f1d7ce7b5fa
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: e691fb1a290aaa28dd1f29dd3a574493c80db725759e76bce279b68ca46248c1

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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.
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.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.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.

APKID ANALYSIS

FILE	DETAILS

<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.MANUFACTURER check
Build.HARDWARE check
possible Build.SERIAL check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
app.covidshield.MainActivity	Schemes: https://, Hosts: alpha.canada.ca, Paths: /covid-alert.html,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Broadcast Receiver (app.covidshield.receiver.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.
2	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
3	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.
4	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.
5	Service (com.transistorsoft.tsbackgroundfetch.FetchJobService) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Broadcast Receiver (com.transistorsoft.tsbackgroundfetch.BootReceiver) 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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
retrieval.covid-notification.alpha.canada.ca	good	**IP:** 65.8.66.87 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
submission.covid-notification.alpha.canada.ca	good	**IP:** 3.96.70.219 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map
github.com	good	**IP:** 140.82.113.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
metrics.covid-notification.alpha.canada.ca	good	**IP:** 3.98.190.83 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map

URLS

URL	FILE
https://retrieval.covid-notification.alpha.canada.ca/exposure-configuration/1.2.6/CA.json https://metrics.covid-notification.alpha.canada.ca/save-metrics https://retrieval.covid-notification.alpha.canada.ca/exposure-configuration/notifications-1.2.6.json https://retrieval.covid-notification.alpha.canada.ca/exposure-configuration/region.json https://retrieval.covid-notification.alpha.canada.ca https://submission.covid-notification.alpha.canada.ca	app/covidshield/BuildConfig.java
https://retrieval.covid-notification.alpha.canada.ca/exposure-configuration/1.2.6/CA.json	app/covidshield/services/metrics/DebugMetricsHelper.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
https://retrieval.covid-notification.alpha.canada.ca/exposure-configuration/1.2.6/CA.json https://metrics.covid-notification.alpha.canada.ca/save-metrics https://retrieval.covid-notification.alpha.canada.ca/exposure-configuration/notifications-1.2.6.json https://retrieval.covid-notification.alpha.canada.ca/exposure-configuration/region.json https://retrieval.covid-notification.alpha.canada.ca https://submission.covid-notification.alpha.canada.ca	Android String Resource

HARDCODED SECRETS

POSSIBLE SECRETS
"EN_API_VERSION" : "1"

POSSIBLE SECRETS
"HMAC_KEY" : "3631313045444b345742464633504e44524a3457494855505639593136464a3846584d4c59334d30"
"METRICS_API_KEY" : "7uueCf8Kiv2JaeasGEaPN2Ij9LJ5qicM6I8nsOOU"
"OUTBREAK_PUBLIC_KEY" : "MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE8oM6jlEslwzTG+sbdkBJwVnRj176nBHvMR66Fqjchohs7sBE+Mlxe6l3O3yHvREn9Nn9yEJcnEYvgFLuyUj/vQ=="
"QR_CODE_PUBLIC_KEY" : "VDWmIAzG9E6DHI4Hm4oGpLN4B51z/nmqKt81GgOR6GQ="

PLAYSTORE INFORMATION

Title: COVID Alert - Let’s protect each other

Score: 3.81 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** ca.gc.hcsc.canada.stopcovid

Developer Details: Health Canada | Santé Canada, Health+Canada+%7C+Sant%C3%A9+Canada, None, https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert/help.html, hc.AlerteCOVIDAlert.sc@canada.ca,

Release Date: Jul 29, 2020 **Privacy Policy:** Privacy link

Description:

Together, let’s slow the spread of COVID-19. Canada's COVID Alert app notifies you if someone you were near in the past 14 days tells the app they tested positive. COVID Alert uses Bluetooth to exchange random codes with nearby phones. It does not use or access any location data. COVID Alert works by determining how far away other phones are by the strength of their Bluetooth signal. Several times a day, COVID Alert checks a list of codes from people who tell the app they tested positive. You’ll get a notification if a code you received matches one of the positive codes. If you test positive for COVID-19 you’ll receive a one-time key with your diagnosis to enter into COVID Alert. The app asks permission to share your random codes from the last 14 days with a central server. Other phones using COVID Alert check the central server periodically throughout the day. If they recorded any codes that match the codes in the central server, their user will be notified that they were exposed. COVID Alert has no way of knowing: -your location - COVID Alert does not use GPS or location services -your name or address -the place or time you were near someone -if you're currently near someone who was previously diagnosed Provincial and territorial governments are working to support COVID Alert across Canada. In some places, people cannot yet report a COVID-19 diagnosis through this app. It’s still helpful to keep COVID Alert on, no matter where you are. That way, when people are able to report a diagnosis, you’ll find out if you were near them. COVID Alert was built by Health Canada with the Canadian Digital Service on the private exposure notification framework by Apple and Google.

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.