MOBSF

ANDROID STATIC ANALYSIS REPORT

BC COVID-19 (1.39.0)

File Name:	BC COVID 19 Support_v1.39.0_apkpure.com.apk
Package Name:	ca.bc.gov.health.hlbc.COVID19
Average CVSS Score:	0
App Security Score:	100/100 (LOW RISK)
Trackers Detection:	3/421
Scan Date:	Feb. 15, 2022, 1:59 a.m.

FILE INFORMATION

File Name: BC COVID 19 Support_v1.39.0_apkpure.com.apk
Size: 11.78MB
MD5: cd26d5d031cfbb0adafd02152cbea7e5

SHA1: d9765a750289111e412bfcb294b7c7141c270bb1
SHA256: 36969c140febb371f94b9f3281ce4787b020b3279182859f5635fd3d2ab26a5e

APP INFORMATION

App Name: BC COVID-19
Package Name: ca.bc.gov.health.hlbc.COVID19
Main Activity: app.health.thrive.MainActivity
Target SDK: 29
Min SDK: 21
Max SDK:
Android Version Name: 1.39.0
Android Version Code: 41

APP COMPONENTS

Activities: 2
Services: 8
Receivers: 6
Providers: 3
Exported Activities: 0
Exported Services: 1
Exported Receivers: 1
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: 2020-03-17 02:26:52+00:00
Valid To: 2050-03-17 02:26:52+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xb3019cf8afad030ab0f88f42ce25feb15d4612b4
Hash Algorithm: sha256
md5: 5b51e17a1009dacbc0a8441482ef6f7e
sha1: d5c025535150683e0dff35532a80aa626fc37348
sha256: 5e36ab1aa2add12929cd4f0ed164688b233b2310a9a0b7cc9ea09747f5f59b9b
sha512: 7c7d59e87ec5be7c4093d947c8431962f597eac85d8448d439377b39dbe99cde1e5ce5f479f3b1a29c2001868ed3e6239a56c0e01a8b6ed3ad935963a819e452
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: b5f0c897a7e52a1a70b7ae55e7effa0f488b34752cdd3c976353ac90b4c6bbe5

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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.

APKID ANALYSIS

<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.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.TAGS check
SIM operator check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
app.health.thrive.MainActivity	Schemes: ca.bc.gov.health.hlbc.COVID19://, https://, @string/custom_url_scheme://, app.health.thrive://, Hosts: location, bcseqr.app.link, bcseqr-alternate.app.link, bcseqr.test-app.link, bcseqr-alternate.test-app.link, healthyhippo.auth0.com, auth.healthyhippo.co, auth.newhippo.com, auth.wethrive.ninja, auth.thrive.health, newhippo.auth0.com, Path Prefixes: /cordova/app.health.thrive/callback,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup=true]	medium	This flag 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.
2	Service (com.getcapacitor.CapacitorFirebaseMessagingService) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Service is explicitly exported.
3	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

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
cdn.branch.io	good	**IP:** 65.8.68.79 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
health-link-bc-covid19.firebaseio.com	good	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
branch.app.link	good	**IP:** 52.84.184.91 **Country:** Korea (Republic of) **Region:** Gyeonggi-do **City:** Incheon **Latitude:** 37.279171 **Longitude:** 127.442497 **View:** Google Map
docs.branch.io	good	**IP:** 52.84.184.102 **Country:** Korea (Republic of) **Region:** Gyeonggi-do **City:** Incheon **Latitude:** 37.279171 **Longitude:** 127.442497 **View:** Google Map
capacitorjs.com	good	**IP:** 76.223.125.115 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

URLS

URL	FILE
https://capacitorjs.com/docs/apis/splash-screen#hiding-the-splash-screen	com/getcapacitor/Splash.java

URL	FILE
	com/getcapacitor/plugin/Camera.java
file:///	com/getcapacitor/plugin/util/AssetUtil.java
https://cdn.branch.io/sdk/uriskiplist_v#.json	io/branch/referral/UniversalResourceAnalyser.java
https://docs.branch.io/pages/apps/android/#load-branch https://docs.branch.io/pages/apps/android/#configure-app https://docs.branch.io/pages/dashboard/integrate/#android https://docs.branch.io/pages/deep-linking/android-app-links/#add-intent-filter-to-manifest https://branch.app.link/link-settings-page	io/branch/referral/validators/IntegrationValidator.java
https://health-link-bc-covid19.firebaseio.com	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://health-link-bc-covid19.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

TRACKER	CATEGORIES	URL
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"fileprovider_authority" : "app.health.thrive.fileprovider"
"firebase_database_url" : "https://health-link-bc-covid19.firebaseio.com"
"google_api_key" : "AIzaSyBE5FSJBAc59fP8BrdrYIq98lPXGgua2LU"
"google_crash_reporting_api_key" : "AIzaSyBE5FSJBAc59fP8BrdrYIq98lPXGgua2LU"

PLAYSTORE INFORMATION

Title: BC COVID-19 Support

Score: 0 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** 5.0 and up **Category:** Medical **Play Store URL:** ca.bc.gov.health.hlbc.COVID19

Developer Details: Province of British Columbia, Canada, Province+of+British+Columbia,+Canada, None, None, support@thrive.health,

Release Date: Apr 8, 2020 **Privacy Policy:** Privacy link

Description:

If you are a resident of British Columbia, Canada, BC COVID-19 Support is designed for you to stay informed about COVID-19 in BC and determine what actions and next

steps you should take. Recommendations are personalized and based on your personal risk factors. You will receive timely updates with important news and alerts from BC's Ministry of Health. Recommendations and content are automatically updated based on the latest BC guidelines related to COVID-19. This application has been developed in collaboration with Thrive Health, a Vancouver-based healthcare technology company. SAFETY & SECURITY: You will only be asked to provide your age, postal code, and device location. The data you provide will be combined with all user data and used to inform the provincial COVID-19 response, and to allow you to receive location-based alerts. Your data will not be sold. Your data will not be used for any purpose other than health care. We follow industry best practices for data security and privacy. The data you provide is always encrypted and is stored in Canada.

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.