ANDROID STATIC ANALYSIS REPORT

StopCovid (1.0.461)

File Name:	StopCovid 1.0.461.apk
Package Name:	gov.georgia.novid20
Average CVSS Score:	5.7
App Security Score:	60/100 (MEDIUM RISK)
Trackers Detection:	2/285

FILE INFORMATION

File Name: StopCovid 1.0.461.apk
Size: 7.49MB
MD5: 55540efa41fdb282fc05dd50e97abaa9
SHA1: 697a5d9dda0ffe86107b97fbe882b8081e86e30d
SHA256: 2d0dafd35f984c3c4a030a7709c7c34e6480ffab85d35cf03e50658de4a70f94

APP INFORMATION

App Name: StopCovid
Package Name: gov.georgia.novid20
Main Activity: org.novid20.ui.main.MainActivity
Target SDK: 29
Min SDK: 21
Max SDK:
Android Version Name: 1.0.461
Android Version Code: 461

APP COMPONENTS

Activities: 4
Services: 18
Receivers: 14
Providers: 4
Exported Activities: 1
Exported Services: 3
Exported Receivers: 5
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Novid20
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-03-16 00:28:42+00:00
Valid To: 2047-08-02 00:28:42+00:00
Issuer: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Novid20
Serial Number: 0x629d0e28
Hash Algorithm: sha256
md5: 095f617b8b3db05b321cebb4a8e1a1a6
sha1: 3d85c933b0f08a457e435d48ecd2ca9d9e3ee898
sha256: 259892fb34bf338b5dc65e12646aa559bb6efb6a7267347f4b0bdb1d96762a33
sha512:
6d96003a68f4299aba74912a2ae83160a5b47e27104c320a00a16db0b0657985a40dc452d793e48f0ce2dc5a1e67a7914d83c1dd8d13861c9747126fe6722867

Certificate Status: Good
Description: Certificate looks good.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
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.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.BLUETOOTH_ADMIN	dangerous	bluetooth administration	Allows an application to configure the local Bluetooth phone and to discover and pair with remote devices.
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.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background. If you're requesting this permission, you must also request either
com.google.android.gms.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACTIVITY_RECOGNITION	dangerous	allow application to recognize physical activity	Allows an application to recognize physical activity.
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.CHANGE_WIFI_STATE	dangerous	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal		Permission an application must hold in order to use
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground
android.permission.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	dangerous	Unknown permission from android reference	Unknown permission from android reference

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.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MODEL check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
Broadcast Receiver (org.novid20.ui.infected.VerificationSmsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.phone.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.

ISSUE	SEVERITY	DESCRIPTION
Service (org.novid20.sdk.activity.ActivityTransitionService) is not Protected. [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.
Broadcast Receiver (org.novid20.sdk.NovidBootReceiver) 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.
Activity (com.google.firebase.auth.internal.FederatedSignInActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.firebase.auth.api.gms.permission.LAUNCH_FEDERATED_SIGN_IN [android:exported=true]	high	An Activity 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 (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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 (org.altbeacon.beacon.startup.StartupBroadcastReceiver) 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.

ISSUE	SEVERITY	DESCRIPTION
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.
Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [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

ISSUE	SEVERITY	STANDARDS	FILES
This App uses Java Hash Code. It's a weak hash function and should never be used in Secure Crypto Implementation.	warning	CVSS V2: 2.3 (low) CWE: CWE-327 - Use of a Broken or Risky Cryptographic Algorithm OWASP MASVS: MSTG-CRYPTO-4	org/altbeacon/beacon/Region.java org/altbeacon/beacon/Beacon.java org/altbeacon/beacon/service/ExtraDataBeaconTracker.java org/novid20/ui/browser/BrowserFragment.java org/novid20/sdk/DetectionConfig.java org/novid20/sdk/ble/NovidBeaconManager.java org/novid20/sdk/ble/BleConfig.java org/novid20/sdk/model/AnalyticsStateEntry.java org/novid20/sdk/model/NovidRepositoryImpl.java org/novid20/sdk/model/ContactEntryEntity.java org/novid20/sdk/model/AnalyticsEventEntry.java org/novid20/sdk/model/Result.java org/novid20/sdk/model/AnalyticsEventEntryEntity.java org/novid20/sdk/api/models/Status.java org/novid20/sdk/api/models/AnalyticsEvent.java org/novid20/sdk/api/models/VerifyUserRequest.java org/novid20/sdk/api/models/AnalyticsRequest.java org/novid20/sdk/api/models/InfectionRequest.java org/novid20/sdk/api/models/ApiResponse.java org/novid20/sdk/api/models/AnalyticsState.java org/novid20/sdk/api/models/VerifyCodeRequest.java org/novid20/sdk/api/models/RegisterUserRequest.java org/novid20/sdk/api/models/RegisterUserResponse.java org/novid20/sdk/api/models/GetStatusResponse.java org/novid20/sdk/api/models/UpdateTokenRequest.java org/novid20/sdk/api/models/ApiContact.java kotlinx/coroutines/JobCancellationException.java kotlinx/coroutines/CoroutineContextKt.java kotlinx/coroutines/CoroutineName.java kotlinx/coroutines/DebugKt.java kotlinx/coroutines/internal/ThreadLocalKey.java kotlinx/coroutines/channels/ValueOrClosed.java io/michaelrocks/libphonenumber/android/Phonenumber.java com/hbb20/CCPCountry.java

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	org/altbeacon/beacon/BeaconParser.java org/altbeacon/beacon/utils/EddystoneTelemetryAccessor.java org/altbeacon/beacon/service/ScanState.java org/altbeacon/beacon/logging/InfoAndroidLogger.java org/altbeacon/beacon/logging/WarningAndroidLogger.java org/altbeacon/beacon/logging/VerboseAndroidLogger.java org/novid20/sdk/Logger.java com/hbb20/CCPCountry.java com/hbb20/CountryCodePicker.java
Files may contain hardcoded sensitive informations like usernames, passwords, keys etc.	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-312 - Cleartext Storage of Sensitive Information **OWASP Top 10:** M9: Reverse Engineering **OWASP MASVS:** MSTG-STORAGE-14	org/altbeacon/beacon/service/RangingData.java org/altbeacon/beacon/service/SettingsData.java org/altbeacon/beacon/service/MonitoringData.java org/altbeacon/beacon/service/StartRMData.java
App can write to App Directory. Sensitive Information should be encrypted.	info	**CVSS V2:** 3.9 (low) **CWE:** CWE-276 - Incorrect Default Permissions **OWASP MASVS:** MSTG-STORAGE-14	org/novid20/sdk/NovidConfig.java
The App uses an insecure Random Number Generator.	high	**CVSS V2:** 7.5 (high) **CWE:** CWE-330 - Use of Insufficiently Random Values **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-6	kotlinx/coroutines/scheduling/CoroutineScheduler.java com/codesgood/views/JustifiedTextView.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
api.novid20.app	good	**IP:** 216.58.199.51 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.stopcov.ge	good	**IP:** 37.46.105.200 **Country:** Georgia **Region:** Tbilisi **City:** Tbilisi **Latitude:** 41.694111 **Longitude:** 44.833679 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
s3.amazonaws.com	good	IP: 52.216.97.45 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.04372 Longitude: -77.487488 View: Google Map
novid.org	good	IP: 52.85.43.245 Country: Australia Region: Victoria City: Melbourne Latitude: -37.813999 Longitude: 144.963318 View: Google Map
schemas.android.com	good	No Geolocation information available.
novid20.firebaseio.com	good	IP: 35.201.97.85 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
stopcov.ge	good	IP: 37.46.105.200 Country: Georgia Region: Tbilisi City: Tbilisi Latitude: 41.694111 Longitude: 44.833679 View: Google Map
api.perkonigg.at	good	IP: 95.216.215.253 Country: Finland Region: Uusimaa City: Helsinki Latitude: 60.169521 Longitude: 24.93545 View: Google Map
novid20.org	good	IP: 13.35.126.86 Country: United States of America Region: California City: San Francisco Latitude: 37.774929 Longitude: -122.419418 View: Google Map

DOMAIN	STATUS	GEOLOCATION
track.customer.io	good	**IP:** 35.244.218.227 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

URLS

URL	FILE
https://s3.amazonaws.com/android-beacon-library/android-distance.json	org/altbeacon/beacon/BeaconManager.java
https://www. http://www.	org/altbeacon/beacon/utils/UrlBeaconUrlCompressor.java
https://api.novid20.app/api/v1	org/novid20/BuildConfig.java
https://novid.org/your/api/	org/novid20/sdk/BuildConfig.java
https://track.customer.io/push/events	org/novid20/sdk/api/CustomClientImpl.java
http://schemas.android.com/apk/res/android	com/hbb20/CountryCodePicker.java
https://novid20.firebaseio.com https://stopcov.ge/ https://NoVid20.org https://api.novid20.app/api/v1/mobile/about https://api.perkonigg.at/api/v1/mobile/more https://api.novid20.app/api/v1/mobile/more https://api.perkonigg.at/api/v1/mobile/privacy https://novid20.org/ www.stopcov.ge https://api.perkonigg.at/api/v1/mobile/terms_and_conditions	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://novid20.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

TRACKER	URL
AltBeacon	https://reports.exodus-privacy.eu.org/trackers/219
Google Firebase Analytics	https://reports.exodus-privacy.eu.org/trackers/49

PLAYSTORE INFORMATION

Title: Stop Covid - let's fight this together

Score: 3.98 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** 5.0 and up **Category:** Health & Fitness **Play Store URL:** gov.georgia.novid20

Developer Details: Ministry of IDPs, Labour, Health, Social Affairs, Ministry+of+IDPs,+Labour,+Health,+Social+Affairs, None, http://www.stopcov.ge, stopcovid@moh.gov.ge,

Release Date: Apr 5, 2020 **Privacy Policy:** Privacy link

Description:

The great danger with COVID-19 is the long incubation period and the fact that many infected people do not experience any symptoms. Our goal is to inform people who have had contact with another infected person at an early stage and thus prevent them from unknowingly spreading the virus further. The Stop Covid app anonymously determines social interactions with other app users. Encounters that have a certain intensity in terms of time and proximity are stored locally by both apps in an encrypted form. If someone tests positive for COVID-19, people who may have had contact with the infected person within the last few days will receive a warning with instructions to contact the local governmental authority.

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.