ANDROID STATIC ANALYSIS REPORT

Bluezone (1.0.1)

File Name:	Bluezone 1.0.1.apk
Package Name:	com.mic.bluezone
Average CVSS Score:	5.9
App Security Score:	15/100 (CRITICAL RISK)
Trackers Detection:	1/285

FILE INFORMATION

File Name: Bluezone 1.0.1.apk
Size: 7.33MB
MD5: deb6e51d0ec8b4a85f0a83683eecf20b
SHA1: 6140da4cc39289c66a586991235bbde038881beb
SHA256: ac872004b78d6ad5fec65b899285011b3e8e80d4f0ecfa7e12b063bd8315436f

APP INFORMATION

App Name: Bluezone
Package Name: com.mic.bluezone
Main Activity: com.cpmsmobileapp.MainActivity
Target SDK: 28
Min SDK: 21
Max SDK:
Android Version Name: 1.0.1
Android Version Code: 10

APP COMPONENTS

Activities: 3
Services: 13
Receivers: 10
Providers: 3
Exported Activities: 0
Exported Services: 1
Exported Receivers: 7
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: 2020-04-16 17:38:33+00:00
Valid To: 2050-04-16 17:38:33+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x9de1b27b42fd598736a1e8b5eb985595b7d442be
Hash Algorithm: sha256
md5: f17d0c15a83d3ab5949b34c1b7dfff10
sha1: 38fb5aaa4815ae761acb3277d406920ff6291327
sha256: ba0c6ebeb664d9971cc3b857ef2ff2c9915c2cb503a40af23ca5255b98ae853a
sha512:
e77e2eaeda3a18439b36a220958670434c5310e9fe833e4d6f95a84a170afa9dddd49a0728976176876742faa2525568799da157e2f548e23dc34c11ccc900e2

PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 4956b667d8a8fd9bff6c036b3b93ee26997df1f9a179e72acb6bb8fbb6c4133d

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.BLUETOOTH_ADMIN	dangerous	bluetooth administration	Allows an application to configure the local Bluetooth phone and to discover and pair with remote devices.
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.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal		Permission an application must hold in order to use
android.permission.READ_EXTERNAL_STORAGE	dangerous	read SD card contents	Allows an application to read from SD Card.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
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.

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.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.mic.bluezone.permission.C2D_MESSAGE	signature	Allows cloud to device messaging	Allows the application to receive push notifications.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.
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
com.sec.android.provider.badge.permission.READ	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.sec.android.provider.badge.permission.WRITE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.htc.launcher.permission.READ_SETTINGS	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.htc.launcher.permission.UPDATE_SHORTCUT	dangerous	Unknown permission from android reference	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.sonyericsson.home.permission.BROADCAST_BADGE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.anddoes.launcher.permission.UPDATE_COUNT	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.majeur.launcher.permission.UPDATE_BADGE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.huawei.android.launcher.permission.CHANGE_BADGE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.huawei.android.launcher.permission.READ_SETTINGS	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.huawei.android.launcher.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.READ_APP_BADGE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.oppo.launcher.permission.READ_SETTINGS	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.oppo.launcher.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
me.everything.badger.permission.BADGE_COUNT_READ	dangerous	Unknown permission from android reference	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	dangerous	Unknown permission from android reference	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check network operator name check possible VM check FINDINGS: Compiler — DETAILS: dx
classes2.dex	FINDINGS: Anti-VM Code — DETAILS: Build.MANUFACTURER check FINDINGS: Compiler — DETAILS: dx

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.cpmsmobileapp.MainActivity	Schemes: mic.bluezone://,

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
Broadcast Receiver (com.google.android.gms.gcm.GcmReceiver) 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.dieam.reactnativepushnotification.modules.RNPushNotificationBootEventReceiver) 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.
Service (com.scan.ServiceTraceCovid) 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 (com.cpmsmobileapp.BootStartReceiver) 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.
Broadcast Receiver (io.invertase.firebase.messaging.ReactNativeFirebaseMessagingReceiver) 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.learnium.RNDeviceInfo.RNDeviceReceiver) is not Protected. [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.

ISSUE	SEVERITY	DESCRIPTION
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
			it/innove/BleManager.java it/innove/Peripheral.java it/innove/LollipopScanManager.java it/innove/LegacyScanManager.java io/liteglue/SQLiteAndroidDatabase.java io/liteglue/SQLitePlugin.java io/invertase/firebase/app/ReactNativeFirebaseApp.java io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java io/invertase/firebase/common/RCTConvertFirebase.java io/invertase/firebase/common/SharedUtils.java io/invertase/firebase/common/ReactNativeFirebaseEventEmitter.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingReceiver.java me/leolin/shortcutbadger/ShortcutBadger.j

ISSUE	SEVERITY	STANDARDS	FILES
			ava timber/log/Timber.java cl/json/RNShareModule.java cl/json/social/SingleShareIntent.java com/dieam/reactnativepushnotification/modules/RNPushNotification.java com/dieam/reactnativepushnotification/modules/RNPushNotificationListenerService.java com/dieam/reactnativepushnotification/modules/RNPushNotificationConfig.java com/dieam/reactnativepushnotification/modules/RNPushNotificationBootEventReceiver.java com/dieam/reactnativepushnotification/modules/RNPushNotificationRegistrationService.java com/dieam/reactnativepushnotification/modules/RNPushNotificationPublisher.java com/dieam/reactnativepushnotification/modules/RNPushNotificationListenerServiceGcm.java com/dieam/reactnativepushnotification/modules/RNPushNotificationAttributes.java com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java com/dieam/reactnativepushnotification/helpers/ApplicationBadgeHelper.java com/horcrux/svg/RadialGradientView.java com/horcrux/svg/VirtualView.java com/horcrux/svg/ImageView.java com/horcrux/svg/UseView.java com/horcrux/svg/MaskView.java com/horcrux/svg/LinearGradientView.java com/horcrux/svg/Brush.java com/horcrux/svg/PatternView.java com/horcrux/svg/ClipPathView.java com/reactnativecommunity/webview/RNCWebViewModule.java com/reactnativecommunity/webview/RNCWebViewManager.java com/reactnativecommunity/geolocation/GeolocationModule.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/swmansion/reanimated/nodes/DebugNode.java com/swmansion/gesturehandler/react/RNGestureHandlerRootHelper.java com/swmansion/gesturehandler/react/RNGestureHandlerRootView.java com/ninty/system/setting/SystemSetting.java com/nineoldandroids/animation/PropertyValuesHolder.java com/rnfs/Downloader.java com/scan/AppUtils.java com/scan/TraceCovidModuleManager.java com/scan/apis/AsyncStorageApi.java com/cpmsmobileapp/BootStartReceiver.java com/bumptech/glide/Glide.java com/bumptech/glide/GeneratedAppGlide

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	ModuleImpl.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/resource/ImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java

ISSUE	SEVERITY	STANDARDS	FILES
			com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/learnium/RNDeviceInfo/resolver/DeviceIdResolver.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/liteglue/SQLiteAndroidDatabase.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/scan/AppDatabaseHelper.java
App can read/write to External Storage. Any App can read data written to External Storage.	high	**CVSS V2:** 5.5 (medium) **CWE:** CWE-276 - Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2	io/invertase/firebase/utils/ReactNativeFirebaseUtilsModule.java cl/json/ShareFiles.java cl/json/RNSharePathUtil.java cl/json/ShareFile.java com/reactnativecommunity/webview/RNCWebViewModule.java com/rnfs/RNFSManager.java com/scan/AppUtils.java com/learnium/RNDeviceInfo/RNDeviceModule.java
			io/invertase/firebase/common/RCTConvertFirebase.java io/invertase/firebase/common/SharedUtils.java cl/json/social/TargetChosenReceiver.java com/dieam/reactnativepushnotification/m

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	odules/RNPushNotificationHelper.java com/horcrux/svg/PropHelper.java com/horcrux/svg/TSpanView.java com/horcrux/svg/SVGLength.java com/oblador/vectoricons/VectorIconsModule.java com/reactnativecommunity/webview/RNCWebViewManager.java com/ninty/system/setting/SystemSetting.java com/scan/AppUtils.java com/bumptech/glide/util/Util.java com/bumptech/glide/util/MultiClassKey.java com/bumptech/glide/util/CachedHashCodeArrayMap.java com/bumptech/glide/signature/MediaStoreSignature.java com/bumptech/glide/signature/ObjectKey.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/Options.java com/bumptech/glide/load/MultiTransformation.java com/bumptech/glide/load/model/GlideUrl.java com/bumptech/glide/load/model/ModelCache.java com/bumptech/glide/load/model/LazyHeaders.java com/bumptech/glide/load/resource/bitmap/CenterInside.java com/bumptech/glide/load/resource/bitmap/CenterCrop.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/DrawableTransformation.java com/bumptech/glide/load/resource/bitmap/GranularRoundedCorners.java com/bumptech/glide/load/resource/bitmap/Rotate.java com/bumptech/glide/load/resource/bitmap/CircleCrop.java com/bumptech/glide/load/resource/bitmap/FitCenter.java com/bumptech/glide/load/resource/bitmap/RoundedCorners.java com/bumptech/glide/load/resource/bitmap/BitmapDrawableTransformation.java com/bumptech/glide/load/resource/gif/GifDrawableTransformation.java com/bumptech/glide/load/engine/EngineKey.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineJob.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/load/engine/prefill/PreFillType.java com/bumptech/glide/load/engine/bitmap_recycle/AttributeStrategy.java com/bumptech/glide/load/engine/bitmap_

ISSUE	SEVERITY	STANDARDS	FILES
			recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/SizeConfigStrategy.java com/bumptech/glide/request/SingleRequest.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	io/invertase/firebase/messaging/ReactNativeFirebaseMessagingHeadlessService.java io/invertase/firebase/messaging/ReactNativeFirebaseMessagingSerializer.java com/dieam/reactnativepushnotification/modules/RNPushNotificationHelper.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/load/engine/EngineResource.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	com/dieam/reactnativepushnotification/modules/RNPushNotification.java com/dieam/reactnativepushnotification/modules/RNPushNotificationListenerService.java com/dieam/reactnativepushnotification/modules/RNPushNotificationListenerServiceGcm.java
App creates temp file. Sensitive information should never be written into a temp file.	high	**CVSS V2:** 5.5 (medium) **CWE:** CWE-276 - Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2	com/reactnativecommunity/webview/RNCWebViewModule.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
twitter.com	good	**IP:** 104.244.42.193 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
covid19-1ffcf.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

DOMAIN	STATUS	GEOLOCATION
www.facebook.com	good	**IP:** 157.240.8.35 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map
plus.google.com	good	**IP:** 172.217.167.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pinterest.com	good	**IP:** 151.101.192.84 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.7757 **Longitude:** -122.395203 **View:** Google Map
github.com	good	**IP:** 13.236.229.21 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map

URLS

URL	FILE
https://www.facebook.com/sharer/sharer.php?u={url}	cl/json/social/FacebookPagesManagerShare.java
https://plus.google.com/share?url={url}	cl/json/social/GooglePlusShare.java
https://twitter.com/intent/tweet?text={message}&url={url}	cl/json/social/TwitterShare.java
https://www.facebook.com/sharer/sharer.php?u={url}	cl/json/social/FacebookShare.java
https://pinterest.com/pin/create/button/?url={url}&media=$media&description={message}	cl/json/social/PinterestShare.java
https://github.com/c19354837/react-native-system-setting/issues/48	com/ninty/system/setting/SystemSetting.java
file:///android_asset/	com/bumptech/glide/load/model/AssetUriLoader.java

URL	FILE
data:image	com/bumptech/glide/load/model/DataUrlLoader.java
https://covid19-1ffcf.firebaseio.com	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://covid19-1ffcf.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

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

PLAYSTORE INFORMATION

Title: Bluezone - Electronicmask

Score: 4.28 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** 5.0 and up **Category:** Health & Fitness **Play Store URL:** com.mic.bluezone

Developer Details: Cục Tin học hóa, Bộ Thông tin và Truyền thông, C%E1%BB%A5c+Tin+h%E1%BB%8Dc+h%C3%B3a,+B%E1%BB%99+Th%C3%B4ng+tin+v%C3%A0+Truy%E1%BB%81n+th%C3%B4ng, 68 Dương Đình Nghệ, Cầu Giấy, Hà Nội, None, banbientap@mic.gov.vn,

Release Date: Apr 16, 2020 **Privacy Policy:** Privacy link

Description:

Bluezone application: The app is to protect the community against COVID-19 pandemic, helping bring the life back to normal. Viet Nam's Ministry of Information and Communications and Ministry of Health, under the direction by the Prime Minister, have deployed the app called "Electronic mask Bluezone" to smartphones. Bluezone shall alert if you had close contact with people who have COVID-19, thereby minimizing the spread of the virus to the community, helping people return to their normal life. When there is a new case of infection, you can learn whether you had close contact with this case or not simply by accessing Bluezone. The more people install Bluezone, there more effective it is. Let's challenge the virus with the strength of our community. Let's try to get every smartphone around Viet Nam installed with Bluezone in a month, so that our community will be protected. With each person installing the app for themselves and getting the smartphones of 3 other people installed with Bluezone, in a month, the whole Viet Nam will get protected. The Ministry of Information and Communications and the Ministry of Health recommend that the whole country install Bluezone for themselves and for 3 others. - Data security: Bluezone stores data on your device only, it does not send such data to the system. - No location data collection: Bluezone does not collect data on your location. - Anonymity: All Bluezoners are anonymous to others. Only competent health authorities know those who are infected and those who are suspected of infection due to close contact with COVID-19 cases. - Transparency: The Project is open source under GPL 3.0. license. Users from other countries are free to learn the operations of the system at source code level, and to use, research, modify and share it.

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.