MOBSF

ANDROID STATIC ANALYSIS REPORT

TraceTogether (2.11.1)

File Name: TraceTogether_v2.11.1_apkpure.com.xapk

Package Name:	sg.gov.tech.bluetrace
Average CVSS Score:	0
App Security Score:	100/100 (LOW RISK)
Trackers Detection:	3/421
Scan Date:	Feb. 20, 2022, 7:24 p.m.

FILE INFORMATION

File Name: TraceTogether_v2.11.1_apkpure.com.xapk
Size: 14.75MB
MD5: 33b7b0af69d3254fef9c32f0a2217691
SHA1: e119571501fba4d388405eb0015bc8d1ae117f82
SHA256: 09c651d568bbfae6b7169a260f495b0d8af6086ff74f9a5c5019c724378023a8

APP INFORMATION

App Name: TraceTogether
Package Name: sg.gov.tech.bluetrace
Main Activity: sg.gov.tech.bluetrace.revamp.splash.SplashActivity
Target SDK: 30
Min SDK: 22
Max SDK:
Android Version Name: 2.11.1
Android Version Code: 132

APP COMPONENTS

Activities: 29
Services: 18
Receivers: 18
Providers: 14
Exported Activities: 3
Exported Services: 2
Exported Receivers: 6
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: 2020-02-12 11:50:19+00:00
Valid To: 2050-02-12 11:50:19+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xc2d173b0a2872598a57a7fe14b74294c0325c277
Hash Algorithm: sha256

md5: 2fc04293ab64be7f6f42fa9077e71e4d
sha1: ade172997a5b7bd188d3f21a163916ee413233db
sha256: c874d784acdaecf15194a56c37210ea7a397ea582ed435e86c840f1359ef804c
sha512: be7fcbdc5f6671fdcd7e36e24773464c153d79d2db4159e6f67c9523f6ce26075a0aa4d5782b4e5591ca15717fee9f26e5480acf1573e6f6abceedca6d316a25
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: ed41b1ec0534bd70fa774cf80f1031042dd8483027bfc6a70cff47f90864f467

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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.INTERNET	normal	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.
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	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
sg.gov.tech.bluetrace.permission.PROCESS_PUSH_MSG	unknown	Unknown permission	Unknown permission from android reference
sg.gov.tech.bluetrace.permission.PUSH_PROVIDER	unknown	Unknown permission	Unknown permission from android reference
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.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.DEVICE check Build.HARDWARE check Build.TAGS check
Compiler	r8

classes.dex

FILE	DETAILS
classes2.dex	<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.BOARD check possible Build.SERIAL check Build.TAGS check possible ro.secure check possible VM check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>
classes3.dex	<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 ro.kernel.qemu check possible VM check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
sg.gov.tech.bluetrace.revamp.splash.SplashActivity	Schemes: https://, Hosts: www.tracetogether.gov.sg, Path Prefixes: /openapp,
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Broadcast Receiver (sg.gov.tech.bluetrace.boot.StartOnBootReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Activity (sg.gov.tech.bluetrace.onboarding.newOnboard.MainOnboardingActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
3	Broadcast Receiver (sg.gov.tech.bluetrace.receivers.UpgradeReceiver) 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.
4	Broadcast Receiver (sg.gov.tech.bluetrace.receivers.UnpauseAlarmReceiver) 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.
5	Broadcast Receiver (sg.gov.tech.bluetrace.widget.SafeEntryWidgetProvider) 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.
6	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.
7	Activity (com.google.firebase.auth.internal.GenericIdpActivity) is not Protected. [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.
8	Activity (com.google.firebase.auth.internal.RecaptchaActivity) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
9	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.
10	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.
11	Broadcast Receiver (com.huawei.hms.support.api.push.PushMsgReceiver) is Protected by a permission. Permission: sg.gov.tech.bluetrace.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	info	A Broadcast Receiver is found to be exported, but is protected by permission.
12	Broadcast Receiver (com.huawei.hms.support.api.push.PushReceiver) is Protected by a permission. Permission: sg.gov.tech.bluetrace.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	info	A Broadcast Receiver is found to be exported, but is protected by permission.
13	Service (com.huawei.hms.support.api.push.service.HmsMsgService) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
14	Content Provider (com.huawei.hms.support.api.push.PushProvider) is Protected by a permission. Permission: sg.gov.tech.bluetrace.permission.PUSH_PROVIDER protectionLevel: signature [android:exported=true]	info	A Content Provider is found to be exported, but is protected by permission.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.tracetogether.gov.sg	good	**IP:** 65.8.68.111 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
tools.android.com	good	**IP:** 142.250.69.211 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
tracetogether.zendesk.com	good	**IP:** 104.16.51.111 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.zendesk.com	good	**IP:** 104.18.3.228 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
staging.temperaturepass.ndi-api.gov.sg	good	**IP:** 13.224.14.39 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sgcovidcheck.gov.sg	good	**IP:** 13.229.33.127 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
tracetogether.gov.sg	good	**IP:** 75.2.116.251 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
eservices.healthhub.sg	good	**IP:** 45.60.105.222 **Country:** United States of America **Region:** Colorado **City:** Greenwood Village **Latitude:** 39.617210 **Longitude:** -104.950813 **View:** Google Map
sso.agc.gov.sg	good	**IP:** 199.184.145.21 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xml.org	good	**IP:** 104.239.240.11 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
schemas.android.com	good	No Geolocation information available.
store.hispace.hicloud.com	good	**IP:** 159.138.90.99 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
support.tracetogether.gov.sg	good	**IP:** 104.16.51.111 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
hive.tech.gov.sg	good	**IP:** 104.198.14.52 **Country:** United States of America **Region:** Oregon **City:** The Dalles **Latitude:** 45.594559 **Longitude:** -121.178680 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.safeentry-qr.gov.sg	good	**IP:** 52.84.159.109 **Country:** Germany **Region:** Berlin **City:** Berlin **Latitude:** 52.524368 **Longitude:** 13.410530 **View:** Google Map
www.tech.gov.sg	good	**IP:** 51.222.8.159 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map
cdn.plot.ly	good	**IP:** 151.101.54.217 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	good	**IP:** 140.82.114.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
safetravel.ica.gov.sg	good	**IP:** 51.222.8.159 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map
govtech-tracer.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
appgallery.cloud.huawei.com	good	**IP:** 159.138.86.75 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
play.google.com	good	**IP:** 142.250.69.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
staging.safeentry-qr.gov.sg	good	**IP:** 65.8.68.91 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
xmlpull.org	good	**IP:** 74.50.61.58 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.814899 **Longitude:** -96.879204 **View:** Google Map

URLS

URL	FILE
file:///android_res/	com/huawei/secure/android/common/util/UrlUtil.java
http://xml.org/sax/features/namespaces http://xml.org/sax/features/validation	com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java
http://xml.org/sax/features/namespaces http://xml.org/sax/features/namespace-prefixes http://xml.org/sax/features/validation http://xml.org/sax/features/external-general-entities http://xml.org/sax/features/external-parameter-entities http://xml.org/sax/features/string-interning	com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java

URL	FILE
http://xmlpull.org/v1/doc/features.html#process-namespaces http://xmlpull.org/v1/doc/features.html#report-namespace-prefixes http://xmlpull.org/v1/doc/features.html#process-docdecl http://xmlpull.org/v1/doc/features.html#validation	com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	io/reactivex/exceptions/UndeliverableException.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://localhost/	retrofit2/Response.java

URL	FILE
https://support.tracetogether.gov.sg/hc/en-sg/articles/1500006031601 https://sgcovidcheck.gov.sg/ https://eservices.healthhub.sg/covid/records https://support.tracetogether.gov.sg/hc/en-sg/sections/4404517990553-COVID-Health-Status https://hive.tech.gov.sg https://support.tracetogether.gov.sg/hc/en-sg/articles/360053464873-How-are-my-possible-exposures-determined-COVID-19 https://play.google.com/store/apps/details?id=sg.gov.tech.bluetrace https://support.tracetogether.gov.sg/hc/en-sg/articles/4404515077273 https://www.tracetogether.gov.sg/common/privacystatement/ https://tracetogether.gov.sg/common/privacystatement https://www.tech.gov.sg/report_vulnerability/ https://safetravel.ica.gov.sg/ https://sso.agc.gov.sg/Act/COVID19TMA2020?ProvIds=P111-#P111- https://support.tracetogether.gov.sg/hc/en-sg/articles/4408401969433 https://www.safeentry-qr.gov.sg/termsofuse https://staging.temperaturepass.ndi-api.gov.sg/login/ https://staging.safeentry-qr.gov.sg/login/ https://www.tracetogether.gov.sg/common/terms-of-use/ https://support.tracetogether.gov.sg/hc/en-sg/articles/360057640753 https://support.tracetogether.gov.sg/hc/en-sg/sections/360007409114-If-you-had-possible-exposure-to-COVID-19 https://support.tracetogether.gov.sg/hc/en-sg/articles/360056446054-I-can-t-activate-my-TraceTogether-App-What-should-I-do- https://support.tracetogether.gov.sg/hc/en-sg/articles/360050088633-I-m-home-alone-why-are-there-Bluetooth-exchanges-with-other-TraceTogether-users-What-does-that-mean- https://support.tracetogether.gov.sg/hc/en-sg/articles/360058601893-Why-can-t-I-use-the-SafeEntry-feature-in-my-app- https://tracetogether.zendesk.com	sg/gov/tech/bluetrace/BuildConfig.java
https://www.tracetogether.gov.sg/	sg/gov/tech/bluetrace/ErrorHandler.java
https://cdn.plot.ly/plotly-latest.min.js'	sg/gov/tech/bluetrace/debugger/PlotActivity.java
https://support.tracetogether.gov.sg/	sg/gov/tech/bluetrace/healthStatus/HealthStatusDetailFragment.java
https://support.tracetogether.gov.sg/hc/en-sg/articles/360058601893-Why-can-t-I-use-the-SafeEntry-feature-in-my-app-	sg/gov/tech/bluetrace/passport/PassportProfileBlockedFragment.java

URL	FILE
https://(www	sg/gov/tech/bluetrace/qrscanner/QrScannerModel.java
https://support.tracetogether.gov.sg/hc/en-sg/articles/360058601893-Why-can-t-I-use-the-SafeEntry-feature-in-my-app-	sg/gov/tech/bluetrace/revamp/home/HomeFragmentV3.java
http://tools.android.com/tech-docs/new-build-system/user-guide/manifest-merger	zendesk/belvedere/Storage.java
https://www.zendesk.com/embeddables	zendesk/support/SupportSdkSettings.java
https://govtech-tracer.firebaseio.com https://play.google.com/store/apps/details?id= https://appgallery.cloud.huawei.com https://www.tracetogether.gov.sg https://store.hispace.hicloud.com/hwmarket/api/	Android String Resource

FIREBASE DATABASES

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

EMAILS

EMAIL	FILE
this@groupcheckinfragment.viewmodel	sg/gov/tech/bluetrace/groupCheckIn/GroupCheckInFragment$adapter$1.java

EMAIL	FILE
this@groupcheckinfragment.viewmodel	sg/gov/tech/bluetrace/groupCheckIn/GroupCheckInFragment.java
mfa_tt_queries@mfa.gov support@tracetogether.gov	Android String Resource

TRACKERS

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
Huawei Mobile Services (HMS) Core	Analytics, Advertisement, Location	https://reports.exodus-privacy.eu.org/trackers/333

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://govtech-tracer.firebaseio.com"
"google_api_key" : "AIzaSyBLG0eg8CJZb1i4Lvrmf9mmGYSMEfT5yrg"
"google_crash_reporting_api_key" : "AIzaSyBLG0eg8CJZb1i4Lvrmf9mmGYSMEfT5yrg"

PLAYSTORE INFORMATION

Title: TraceTogether

Score: 3.7 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** 5.1 and up **Category:** Medical **Play Store URL:** sg.gov.tech.bluetrace

Developer Details: Government Technology Agency, Government+Technology+Agency, None, https://tracetogether.gov.sg, support@tracetogether.gov.sg,

Release Date: Mar 9, 2020 **Privacy Policy:** Privacy link

Description:

TraceTogether supports Singapore's efforts to fight the spread of COVID-19 through community-driven contact tracing. The TraceTogether App allows you to view or present your COVID Health Status based on your vaccination and test statuses. TraceTogether notifies you quickly if you've been exposed to COVID-19 through close contact with other TraceTogether users. The app allows the Ministry of Health (MOH) to give you timely care and guidance, protecting you and those around you. The app uses Bluetooth, and your Bluetooth data is stored securely on your phone. It'll be shared with MOH if you test positive for COVID-19, for the purpose of contact tracing. Also, all Bluetooth data stored on your phone is automatically deleted after 25 days. TraceTogether helps us ensure that we don't spread the virus to our loved ones unknowingly. It also helps us support the work of contact tracers and healthcare workers by combating the spread of COVID-19 together. App functionality will cease once the outbreak ends. TraceTogether is designed for use by people in Singapore. To register, you will need a valid NRIC, FIN, or a valid document of your current stay in Singapore.

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.