MOBSF

ANDROID STATIC ANALYSIS REPORT

TraceTogether

File Name:	sg.gov.tech.bluetrace_38_apps.evozi.com.apk
Package Name:	sg.gov.tech.bluetrace
Average CVSS Score:	5.8
App Security Score:	10/100 (CRITICAL RISK)
Trackers Detection:	2/285

FILE INFORMATION

File Name: sg.gov.tech.bluetrace_38_apps.evozi.com.apk
Size: 4.09MB
MD5: a4fa09ec1c4531aa0efd3208ce38fee7
SHA1: 271841bcf6abf571e0158a246af944d480a6f734
SHA256: 1b56576aa44381b970c2685cd5e534ca7b5aa6e872ec6d356544d6f76cfa9786

APP INFORMATION

App Name: TraceTogether
Package Name: sg.gov.tech.bluetrace
Main Activity: .SplashActivity
Target SDK:
Min SDK:
Max SDK:
Android Version Name:
Android Version Code: 38

APP COMPONENTS

Activities: 17
Services: 10
Receivers: 8
Providers: 6
Exported Activities: 0
Exported Services: 2
Exported Receivers: 5
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: 2020-02-12 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

Certificate Status: Good
Description: Certificate looks good.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
	dangerous	Unknown permission from android reference	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: DETAILS Obfuscator: DexGuard Anti-VM Code: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check Anti Debug Code: Debug.isDebuggerConnected() check Anti Disassembly Code: illegal class name Compiler: dx

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
Application Data can be Backed up [android:allowBackup] flag is missing.	medium	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.

ISSUE	SEVERITY	DESCRIPTION
Broadcast Receiver () 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 () 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.
Broadcast Receiver () 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 () 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 () 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 () 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.
Broadcast Receiver () 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

ISSUE	SEVERITY	STANDARDS	FILES
			o/C2558.java o/C1821.java o/C2870.java o/C1860.java o/C2503.java o/C2892.java o/C2611.java o/C0708.java o/C1684.java o/C2196.java o/C1775.java o/C2509.java o/C2898.java o/C2162.java o/C3047.java o/C2713.java o/C2007.java o/C1914.java o/C2768.java o/C1543.java o/C1612.java o/C0500.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	o/lF.java o/C1278.java o/C0605.java o/C2507.java o/C1901.java o/C3246aa.java o/C2771.java o/C1408.java o/mM.java o/C2789.java o/C2619.java o/C2033.java o/C0798.java o/C2802.java o/C1516.java o/C2506.java o/C2793.java o/C1015.java o/C1629.java o/C1193.java o/C0444.java o/C2592.java o/C2188.java o/C3035.java o/C1205.java o/C1383.java o/C2239.java o/C2805.java o/C3557ll.java o/C0747.java o/C2490.java o/C2760.java o/C0966.java sg/gov/tech/bluetrace/fragment/UploadCompleteFragment.java sg/gov/tech/bluetrace/fragment/EnterPinFragment.java sg/gov/tech/bluetrace/fragment/ForUseFragment.java sg/gov/tech/bluetrace/fragment/VerifyCallerFragment.java
			o/C0420.java o/C2299.java o/C2923.java o/C3456hr.java o/C1708.java o/C1790.java o/C2515.java o/C2186.java o/C1745.java o/lW.java o/C0945.java o/C0729.java o/C1704.java o/C3017.java o/C2190.java o/C0457.java o/C0381.java o/C3594mv.java o/C1986.java o/C0591.java o/C1768.java o/C1142.java

ISSUE	SEVERITY	STANDARDS	FILES
			o/C2806.java o/C1396.java o/mE.java o/C1477.java o/C1836.java o/lZ.java o/kD.java o/C1461.java o/C2471.java o/C2689.java o/C1699.java o/C2670.java o/C2417.java o/C1846.java o/C2155.java o/C1796.java o/C0650.java o/C2495.java o/lQ.java o/C1128.java o/cX.java o/C2179.java o/C3466ia.java o/C0488.java o/C1299.java o/C0430.java o/C1221.java o/C1036.java o/C3609w.java o/C1098.java o/C0518.java o/fS.java o/C1866.java o/C3348dq.java o/C0667.java o/C2573.java o/C3118.java o/C1826.java o/C2135.java o/C0718.java o/C2660.java o/fG.java o/C3088.java o/C3248ac.java o/C2986.java o/C2093.java o/C3394fj.java o/C1739.java o/C3453ho.java o/C1943.java o/C2292.java o/C0755.java o/C3207.java o/C1113.java o/mC.java o/C1868.java o/C2252.java o/C2069.java o/C1829.java o/C0445.java o/C1468.java o/C1385.java o/C1690.java o/C2141.java
This App uses Java Hash Code.		CVSS V2: 2.3 (low)	

ISSUE	SEVERITY	STANDARDS	FILES
It's a weak hash function and should never be used in Secure Crypto Implementation.	warning	CWE: CWE-327 - Use of a Broken or Risky Cryptographic Algorithm OWASP MASVS: MSTG-CRYPTO-4	o/C2383.java o/C1534.java o/C2927.java o/C0432.java o/C3460hv.java o/C3065.java o/C3376er.java o/C1625.java o/C2320.java o/C2160.java o/C0624.java o/C2064.java o/C0665.java o/C2463.java o/C1865.java o/C2290.java o/C1015.java o/lG.java o/C2300.java o/C1202.java o/C1701.java o/C2896.java o/C2195.java o/C2219.java o/C3074.java o/C1858.java o/C1272.java o/C3314ci.java o/C0530.java o/C1655.java o/C3054.java o/lU.java o/C1100.java o/C0992.java o/C2385.java o/C1681.java o/C2054.java o/C1879.java o/C0784.java o/C1746.java o/nm.java o/C1091.java o/C1880.java o/C3126.java o/C2737.java o/C3350ds.java o/C0419.java zendesk/core/AnonymousIdentity.java zendesk/core/ApplicationConfiguration.java zendesk/core/AccessToken.java zendesk/core/JwtIdentity.java zendesk/support/RequestDataList.java zendesk/support/SectionItem.java zendesk/support/ZendeskAvatarView.java zendesk/support/User.java zendesk/support/CategoryItem.java zendesk/support/SeeAllArticlesItem.java

ISSUE	SEVERITY	STANDARDS	FILES
			zendesk/support/RequestData.java zendesk/support/ArticleItem.java zendesk/support/requestlist/RequestListItem.java zendesk/support/requestlist/RequestInfo.java zendesk/support/request/ReducerError.java zendesk/support/request/ReducerConfiguration.java zendesk/support/request/RequestAccessibilityHerald.java zendesk/support/request/ReducerConversation.java zendesk/support/request/ReducerAttachments.java zendesk/support/request/ComponentToolbar.java zendesk/support/request/AdapterAttachmentCarousel.java zendesk/support/request/ReducerUiState.java zendesk/support/request/ReducerAndroidLifecycle.java
MD5 is a weak hash known to have hash collisions.	high	CVSS V2: 7.4 (high) CWE: CWE-327 - Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	o/C2149.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	o/C2149.java o/C3083.java o/C0315.java o/C2373.java o/lb$1.java o/C1535.java o/C3504jn.java o/C2396.java o/C3207.java o/C2160.java o/C2188.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	o/C2372.java o/C1573.java o/C2099.java o/C2440.java o/C2247.java o/C1943.java o/C2679.java o/C2624.java o/C2813.java o/C1507.java o/C1842.java o/C2127.java
IP Address disclosure	warning	CVSS V2: 4.3 (medium) CWE: CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor OWASP MASVS: MSTG-CODE-2	o/C2889.java o/C2563.java o/C3248ac.java o/C0779.java o/C0697.java

ISSUE	SEVERITY	STANDARDS	FILES
SHA-1 is a weak hash known to have hash collisions.	high	**CVSS V2:** 5.9 (medium) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-4	o/C2391.java
This App may have root detection capabilities.	secure	**CVSS V2:** 0 (info) **OWASP MASVS:** MSTG-RESILIENCE-1	o/C3271ax.java o/C2802.java
Remote WebView debugging is enabled.	high	**CVSS V2:** 5.4 (medium) **CWE:** CWE-919 - Weaknesses in Mobile Applications **OWASP Top 10:** M1: Improper Platform Usage **OWASP MASVS:** MSTG-RESILIENCE-2	zendesk/support/guide/ViewArticleActivity.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.tracetogether.gov.sg	good	**IP:** 52.84.228.58 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.28967 **Longitude:** 103.850067 **View:** Google Map
www.firebase.google.com	good	No Geolocation information available.
firebasestorage.googleapis.com	good	**IP:** 216.58.196.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
e.crashlytics.com	good	**IP:** 54.235.189.25 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.04372 **Longitude:** -77.487488 **View:** Google Map
github.com	good	**IP:** 13.237.44.5 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
goo.gl	good	**IP:** 216.58.203.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.googleadservices.com	good	**IP:** 172.217.25.130 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
govtech-tracer.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
www.google.com	good	**IP:** 216.58.196.132 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
tracetogether.zendesk.com	good	**IP:** 104.16.52.111 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
play.google.com	good	**IP:** 216.58.196.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebase.google.com	good	**IP:** 216.58.196.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
settings.crashlytics.com	good	**IP:** 216.58.196.131 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	good	No Geolocation information available.
www.zendesk.com	good	**IP:** 104.18.2.228 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.7757 **Longitude:** -122.395203 **View:** Google Map
app-measurement.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
1s-2s.cloudfunctions.net	good	**IP:** 216.239.36.54 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
google.com	good	**IP:** 216.58.200.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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

DOMAIN	STATUS	GEOLOCATION
pagead2.googlesyndication.com	good	**IP:** 172.217.167.66 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
cdn.plot.ly	good	**IP:** 151.101.82.217 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.7757 **Longitude:** -122.395203 **View:** Google Map
tracetogether.gov.sg	good	**IP:** 99.83.159.5 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

URLS

URL	FILE
www.google.com https://www.google.com https://goo.gl/NAOOOI. https://goo.gl/NAOOOI https://www.googleadservices.com/pagead/conversion/app/deeplink?id_type=adid&sdk_version=%s&rdid=%s&bundleid=%s&retry=%s	o/C2149.java
https://google.com/search?	o/C0637.java
http://schemas.android.com/apk/res/android	o/C2411.java
http://schemas.android.com/apk/res/android	o/C2169.java
https://%s/%s/%s?key=%s	o/C0380.java
http://schemas.android.com/apk/res/android http://schemas.android.com/apk/res-auto	o/C1712.java
www.firebase.google.com/storage.	o/C0968.java
https://settings.crashlytics.com/spi/v2/platforms/android/apps/%s/settings	o/bL.java

URL	FILE
http://schemas.android.com/apk/res/android	o/C0909.java
https://tracetogether.gov.sg/common/privacystatement	o/C3560lr.java
https://app-measurement.com/a	o/C3178.java
http://schemas.android.com/apk/res/android	o/C1738.java
http://schemas.android.com/apk/res/android	o/C2587.java
https://tracetogether.zendesk.com	o/C3559lp.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	o/C3318cm.java
http://localhost	o/C1523.java
http://schemas.android.com/apk/res/android	o/C1959.java
https://firebasestorage.googleapis.com/v0	o/C3047.java
https://firebase.google.com/support/guides/disable-analytics	o/C2050.java
https://app-measurement.com/a	o/C2504.java
http://schemas.android.com/apk/res/android	o/C2663.java
https://e.crashlytics.com/spi/v2/events	o/bE.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	o/C2771.java
http://schemas.android.com/apk/res/android	o/C0921.java
http://schemas.android.com/apk/res/android	o/C2588.java
http://schemas.android.com/apk/res/android	o/C1832.java
https://tracetogether.zendesk.com	o/C3555lj.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	o/C3317cl.java
https://goo.gl/J1sWQy	o/C2188.java
https://%1$s-%2$s.cloudfunctions.net/%3$s	o/C0394.java
https://plus.google.com/	o/C1679.java
http://schemas.android.com/apk/res/android	o/C3078.java
https://cdn.plot.ly/plotly-latest.min.js'	o/C3557ll.java

URL	FILE
https://play.google.com/store/apps/details?id=sg.gov.tech.bluetrace	sg/gov/tech/bluetrace/SplashActivity.java
https://www.zendesk.com/embeddables	zendesk/support/SupportSdkSettings.java
file:///android_asset/help_center_article_style.css	zendesk/support/guide/ViewArticleActivity.java
https://govtech-tracer.firebaseio.com https://www.tracetogether.gov.sg	Android String Resource

FIREBASE DATABASES

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

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	o/C2628.java

TRACKERS

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

PLAYSTORE INFORMATION

Title: TraceTogether

Score: 3.4200914 **Installs:** 500,000+ **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, tracetogether@hive.gov.sg,

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

Description:

TraceTogether supports Singapore's efforts to mitigate the spread of COVID-19 through community-driven contact tracing. TraceTogether uses Bluetooth signals to determine if you are near another TraceTogether user. Your Bluetooth proximity data is encrypted and stored only on your phone. The Ministry of Health (MOH) will seek your consent to upload the data, if it's needed for contact tracing. If you had close contact with a COVID-19 case, TraceTogether allows the MOH call you more quickly, to provide guidance and care. TraceTogether helps us protect our loved ones and families so that we do not spread the virus to them unknowingly. It also helps us support the work of contact tracers and healthcare workers by combating the spread of COVID-19 together. TraceTogether's functionality will be suspended after the epidemic subsides.

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.