ANDROID STATIC ANALYSIS REPORT

StopTheSpread (1.0.0)

File Name:	StopTheSpread 1.0.0.apk
Package Name:	com.virustracker.app
Average CVSS Score:	6.2
App Security Score:	60/100 (MEDIUM RISK)

FILE INFORMATION

File Name: StopTheSpread 1.0.0.apk
Size: 1.29MB
MD5: 21f5d4947c67200fd81a23caff039396
SHA1: 60ea3daf05572023debfc546da36539e2900895b
SHA256: 1510198273be009c0beff691d25e05518f9ea49bb1b5378dc2412decf71dffea

APP INFORMATION

App Name: StopTheSpread
Package Name: com.virustracker.app
Main Activity: com.virustracker.app.MainActivity
Target SDK: 28
Min SDK: 16
Max SDK:
Android Version Name: 1.0.0
Android Version Code: 1

APP COMPONENTS

Activities: 2
Services: 1
Receivers: 0
Providers: 1
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
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: 2020-03-10 00:29:02+00:00
Valid To: 2050-03-10 00:29:02+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x1273a9c6bdd487e6ea40eda78d47c2925b5debe5
Hash Algorithm: sha256
md5: ffd9bdceac8c28d737e3773bba64c909
sha1: 75f53b9affcdde8b5d1eb5feb35b27478516693e
sha256: 691bb6b32d2e4ab1a3132c146cf40798c3fb3fc5a82b6cf1d0a947179174bb3c
sha512:
8efeafeaaca576947b95d29f97651b7df8e4b34239311122e5acbf5680948d8532287527a023f6c2791830d89d4acc50a07701c32984ee608aa1d548430d3956

PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: ee945aa50449d1b700b1dafda867c1f38c72def02219617131e0a7790f9e7e80

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.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: DETAILS Anti-VM Code: Build.MANUFACTURER check 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.

CODE ANALYSIS

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	io/flutter/plugins/googlemaps/GoogleMapController.java io/flutter/plugins/firebase/cloudfirestore/a.java io/flutter/embedding/engine/f/a.java io/flutter/plugin/platform/j.java io/flutter/plugin/platform/SingleViewPresentation.java io/flutter/view/c.java io/flutter/view/AccessibilityViewEmbedder.java a/c/d/b.java a/c/e/b.java a/c/e/c.java a/d/a/b.java a/d/a/e.java a/d/a/j.java a/d/a/m.java a/d/a/a.java a/e/a/b.java c/a/a.java c/a/c/a/c.java c/a/c/a/j.java c/a/c/a/a.java c/b/m1/a.java com/baseflow/location_permissions/LocationPermissionsPlugin.java b/b/a/a/f/b/a.java b/b/a/a/c/h.java b/b/a/a/d/c/q.java b/b/a/a/e/a.java b/b/a/a/b/d.java b/b/a/a/b/i.java b/b/a/a/b/j.java b/b/a/a/b/s.java b/b/a/a/b/r.java b/b/a/a/b/n/a.java b/b/d/b.java
			io/flutter/plugins/googlemaps/GoogleMapController.java io/flutter/plugins/googlemaps/e.java io/flutter/plugins/googlemaps/GoogleMapsPlugin.java io/flutter/plugins/firebase/core/a.java io/flutter/plugins/firebase/cloudfirestore/a.java io/flutter/plugins/b/a.java io/flutter/embedding/engine/i/j.java io/flutter/embedding/engine/i/f.java io/flutter/embedding/engine/i/g.java io/flutter/embedding/engine/i/a.java io/flutter/embedding/engine/e/a.java io/flutter/plugin/platform/SingleViewPresentation.java io/flutter/view/AccessibilityViewEmbedder.java a/a/a/b/b.java a/d/a/d.java a/b/b.java a/b/d.java

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	a/b/e.java c/c/f/c.java c/c/f/d.java c/c/f/a.java c/c/f/v/a.java c/c/d/b.java c/c/d/a.java c/c/e/b.java c/c/e/c.java c/c/e/f.java c/c/e/a.java c/b/g1.java c/b/a1.java c/b/p.java c/b/o0.java c/b/x.java c/b/t0.java c/b/p1/b.java c/b/o1/r/j/d.java com/baseflow/geolocator/GeolocatorPlugin.java com/baseflow/location_permissions/LocationPermissionsPlugin.java b/c/a/c.java b/b/g/w.java b/b/g/e0.java b/b/g/c.java b/b/g/s.java b/b/g/l.java b/b/g/m.java b/b/a/a/d/c/c0.java b/b/a/a/d/c/s.java b/b/c/c/a.java b/b/c/b/b.java b/b/c/b/d.java b/b/c/b/e.java b/b/c/b/l.java b/b/c/b/m.java b/b/d/b.java b/b/d/h/a/c.java b/b/d/h/a/e.java b/b/d/m/a.java
This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	CVSS V2: 0 (info) OWASP MASVS: MSTG-STORAGE-10	io/flutter/plugin/platform/c.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	c/b/n1/i2.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	c/b/n1/d0.java c/b/n1/f0.java c/b/n1/w1.java c/b/s1/a.java c/b/o1/h.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
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
virus-tracker-bef7e.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

URLS

URL	FILE
https://github.com/flutter/flutter/issues/2897).It	io/flutter/plugin/platform/j.java
https://github.com/grpc/grpc-java/issues/5015	c/b/n1/d1.java
https://virus-tracker-bef7e.firebaseio.com	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://virus-tracker-bef7e.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	b/b/a/a/b/x.java

PLAYSTORE INFORMATION

Title: StopTheSpread COVID-19

Score: 0.0 **Installs:** 100+ **Price:** 0 **Android Version Support:** 4.1 and up **Category:** Medical **Play Store URL:** com.virustracker.app

Developer Details: Binary Mango, Binary+Mango, None, https://www.virus-tracker.com, jacobo@binarymango.com,

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

Description:

An orderly way to allow users to send reports to relevant Governments in the UK, Public Health England and in the US, the CDC with emphasis on the current coronavirus crisis. We show and share locations with the government agencies and provide the ability for users to donate to the Government toward finding the cure and preventing the spread of viruses.

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.