MOBSF

ANDROID STATIC ANALYSIS REPORT

COVID Defense (1.9.1)

File Name:	base.apk
Package Name:	org.pathcheck.la.bt
Average CVSS Score:	6.8
App Security Score:	65/100 (MEDIUM RISK)
Trackers Detection:	2/408
Scan Date:	Feb. 4, 2022, 1:48 a.m.

FILE INFORMATION

File Name: base.apk
Size: 7.37MB
MD5: bb4ed4340ca7683797f55d4651913cee
SHA1: af9e6c731d559e7f83091f9edb5d6012223ecedd
SHA256: 31d1742cd986d67cc788e08bd8a8e3a32f6ea3be9d7b327b182b7e8ff3e523a0

APP INFORMATION

App Name: COVID Defense
Package Name: org.pathcheck.la.bt
Main Activity: org.pathcheck.covidsafepaths.SplashActivity
Target SDK: 30
Min SDK: 23
Max SDK:
Android Version Name: 1.9.1
Android Version Code: 2661

APP COMPONENTS

Activities: 3
Services: 5
Receivers: 10
Providers: 1
Exported Activities: 1
Exported Services: 2
Exported Receivers: 3
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: 2020-08-19 16:53:47+00:00
Valid To: 2050-08-19 16:53:47+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x5c0ddeb0e391f69b39df3a4cdb22bde27d76dc12
Hash Algorithm: sha256

md5: 0146b0937373daff29c353c3cb2ea4da
sha1: aeb36f335826cd5f11d2426b1863694a6f549437
sha256: 5836fe0251e77d8c44818ef7d1e0b9980346072187191a18259648de788fe775
sha512: 52379f08f1753d9fedfe73c927f76dca715dc87a5a8f9c593fe375ab52508453b3ba05c144ff640100b36a4385317a7934d97a1d42bdc9c60317ed7524e7b560
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 07a749fd00217b095db29c84bcabb2e8572954659f64528d950f7398e2d1ab93

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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.ACCESS_NETWORK_STATE	normal	view network	Allows an application to view the status of all networks.

		status	
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.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check possible Build.SERIAL check Build.TAGS check network operator name check FINDINGS: Compiler — DETAILS: r8

BROWSABLE ACTIVITIES

ACTIVITY	INTENT

org.pathcheck.covidsafepaths.MainActivity	Schemes: pathcheck://, https://, Hosts: exposureHistory, us-la.en.express,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Activity (org.pathcheck.covidsafepaths.MainActivity) 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.
2	Broadcast Receiver (org.pathcheck.covidsafepaths.exposurenotifications.nearby.ExposureNotificationBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.nearby.exposurenotification.EXPOSURE_CALLBACK [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.

3	Service (com.google.android.gms.nearby.exposurenotification.WakeUpService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.nearby.exposurenotification.EXPOSURE_CALLBACK [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.
4	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.
5	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.
6	Broadcast Receiver (org.matomo.sdk.extra.InstallReferrerReceiver) 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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/horcrux/svg/LinearGradientView.java org/pathcheck/covidsafepaths/exposurenotifications/reactmodules/$$Lambda$ExposureNotificationsModule$fq6jUIhTgXtqXKNpq33_h3vKswk.java com/swmansion/gesturehandler/react/RNGestureHandlerRootView.java com/bottlerocketstudios/vault/keys/wrapper/ObfuscatingSecretKeyWrapper.java com/horcrux/svg/VirtualView.java com/th3rdwave/safeareacontext/SafeAreaView.java com/bottlerocketstudios/vault/keys/storage/SharedPrefKeyStorage.java com/horcrux/svg/RenderableView.java org/pathcheck/covidsafepaths/exposurenotifications/network/escrowserver/EscrowVerificationClient$refresh$2.java io/realm/Realm.java com/horcrux/svg/PatternView.java org/pathcheck/covidsafepaths/exposurenotifications/network/DiagnosisKeyDownloader.java com/horcrux/svg/ClipPathView.java org/pathcheck/covidsafepaths/exposurenotifications/network/Uris.java com/bottlerocketstudios/vault/keys/storage/hardware/An

1	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	droidKeystoreTester.java com/swmansion/gesturehandler/react/RNGestureHandlerRootHelper.java org/pathcheck/covidsafepaths/exposurenotifications/ExposureNotificationClientWrapper.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java com/bugsnag/android/Configuration.java com/horcrux/svg/ImageView.java com/horcrux/svg/RadialGradientView.java com/horcrux/svg/UseView.java org/pathcheck/covidsafepaths/exposurenotifications/network/escrowserver/DeviceIDHelper.java org/pathcheck/covidsafepaths/exposurenotifications/nearby/ExposureConfigurations$refresh$1.java org/pathcheck/covidsafepaths/exposurenotifications/network/escrowserver/EscrowVerificationClient$postPositiveSubmission$2.java org/pathcheck/covidsafepaths/exposurenotifications/reactmodules/UtilsModule.java io/realm/RealmCache.java org/pathcheck/covidsafepaths/exposurenotifications/storage/RealmSecureStorageBte.java com/bottlerocketstudios/vault/keys/storage/CompatSharedPrefKeyStorageFactory.java io/realm/internal/OsRealmConfig.java com/horcrux/svg/MaskView.java org/pathcheck/covidsafepaths/exposurenotifications/nearby/ProvideDiagnosisKeysWorker.java org/pathcheck/covidsafepaths/exposurenotifications/network/escrowserver/EscrowVerificationClient$authenticate$2.java com/bugsnag/android/ExceptionHandler.java com/bugsnag/android/DebugLogger.java org/pathcheck/covidsafepaths/exposurenotifications/reactmodules/ExposureNotificationsModule.java org/pathcheck/covidsafepaths/exposurenotifications/nearby/StateUpdatedWorker.java io/realm/BaseRealm.java org/pathcheck/covidsafepaths/exposurenotifications/network/escrowserver/DeviceIDHelper$getDeviceID$2.java org/pathcheck/covidsafepaths/exposurenotifications/netw

				ork/escrowserver/EscrowVerificationClient$postMetaInfo$2.java
2	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CVSS V2: 5.9 (medium) CWE: CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java
3	The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CVSS V2: 5.9 (medium) CWE: CWE-327 Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	com/bottlerocketstudios/vault/keys/wrapper/ObfuscatingSecretKeyWrapper.java
4	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CVSS V2: 7.4 (high) CWE: CWE-312 Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/pedrouid/crypto/RNSCRandomBytes.java org/pathcheck/covidsafepaths/BuildConfig.java
5	The App uses an insecure Random Number Generator.	warning	CVSS V2: 7.5 (high) CWE: CWE-330 Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	org/matomo/sdk/Tracker.java
6	This App may have root detection capabilities.	secure	CVSS V2: 0 (info) OWASP MASVS: MSTG-RESILIENCE-1	com/bugsnag/android/DeviceDataCollector.java
7	This App uses SafetyNet API.	secure	CVSS V2: 0 (info) OWASP MASVS: MSTG-RESILIENCE-7	org/pathcheck/covidsafepaths/exposurenotifications/network/escrowserver/DeviceIDHelper$getDeviceID$2.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity', 'bluetooth'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
				The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using

10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys not in accordance with FCS_CKM.1.1(1) using key generation algorithm RSA schemes and cryptographic key sizes of 1024-bit or lower.
12	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption not in accordance with FCS_COP.1.1(1), AES-ECB mode is being used.
13	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
14	FCS_COP.1.1(3)	Selection-Based Security Functional Requirements	Cryptographic Operation - Signing	The application perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
15	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
16	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
17	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
18	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
apps.apple.com	good	**IP:** 104.79.84.26 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.714272 **Longitude:** -74.005966 **View:** Google Map
www.coviddefensela.com	good	**IP:** 184.73.183.75 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
prod.exposurenotification.health	good	**IP:** 13.107.213.40 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
apiserver.encv.org	good	**IP:** 34.107.223.222 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

encdn.prod.exposurenotification.health	good	IP: 104.212.67.108 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
realm.io	good	IP: 13.225.214.66 Country: United States of America Region: New Jersey City: Newark Latitude: 40.735661 Longitude: -74.172371 View: Google Map
coviddefensela.com	good	IP: 34.193.69.252 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
ldhcovid19.my.salesforce.com	good	IP: 96.43.153.40 Country: United States of America Region: California City: San Francisco Latitude: 37.788464 Longitude: -122.394608 View: Google Map
play.google.com	good	IP: 142.250.81.206 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

github.com	good	IP: 140.82.113.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
www.cdc.gov	good	IP: 23.51.180.82 Country: United States of America Region: Pennsylvania City: Philadelphia Latitude: 39.952339 Longitude: -75.163788 View: Google Map
notify.bugsnag.com	good	IP: 35.186.205.6 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
docs.bugsnag.com	good	IP: 157.245.84.7 Country: United States of America Region: New Jersey City: North Bergen Latitude: 40.804272 Longitude: -74.012077 View: Google Map
issuetracker.google.com	good	IP: 172.217.13.238 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

ldh.la.gov	good	**IP:** 3.94.39.96 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
sessions.bugsnag.com	good	**IP:** 35.190.88.7 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
bugsnag.com	good	**IP:** 52.85.132.5 **Country:** United States of America **Region:** Virginia **City:** Dulles **Latitude:** 38.951668 **Longitude:** -77.448059 **View:** Google Map
cdn.projectaurora.cloud	good	**IP:** 35.244.172.56 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

URLS

URL	FILE

https://%s/	com/terveystalo/react_native/matomo_sdk/RNMatomoSdkModule.java
https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenStackFragment.java
https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenFragment.java
https://bugsnag.com	com/bugsnag/android/Notifier.java
https://docs.bugsnag.com/platforms/android/ndk-link-errors	com/bugsnag/android/NdkPlugin.java
https://github.com/bugsnag/bugsnag-js	com/bugsnag/android/BugsnagReactNativePlugin.java
https://notify.bugsnag.com https://sessions.bugsnag.com	com/bugsnag/android/EndpointConfiguration.java
https://realm.io/news/android-installation-change/	io/realm/RealmConfiguration.java
https://issuetracker.google.com/issues/36918154	io/realm/Realm.java
https://cdn.projectaurora.cloud/la/cfg/android/v1.6.config.json https://play.google.com/store/apps/details?id=org.pathcheck.la.bt https://cdn.projectaurora.cloud/la/cfg/ios/v1.config.json https://cdn.projectaurora.cloud/la/cfg/ios/v2.config.json https://www.cdc.gov/coronavirus/2019-ncov/if-you-are-sick/quarantine.html https://ldhcovid19.my.salesforce.com/services/data/v49.0/sobjects/PathCheck_Staging__c https://ldhcovid19.my.salesforce.com/services/oauth2/ https://ldhcovid19.my.salesforce.com https://www.cdc.gov/coronavirus/2019-ncov/if-you-are-sick/steps-when-sick.html https://www.cdc.gov/coronavirus/2019-ncov/symptoms-testing/symptoms.html https://encdn.prod.exposurenotification.health https://cdn.projectaurora.cloud/cfg https://cdn.projectaurora.cloud/cfg/v1.config.json https://cdn.projectaurora.cloud/cfg/v1.6.config.json https://ldh.la.gov/index.cfm/page/3934 https://apiserver.encv.org	org/pathcheck/covidsafepaths/BuildConfig.java

https://apps.apple.com/us/app/covid-defense/id1528363969 https://coviddefensela.com/privacy-policy https://prod.exposurenotification.health https://www.coviddefensela.com/ https://www.coviddefensela.com/faqs	
https://encdn.prod.exposurenotification.health/	org/pathcheck/covidsafepaths/exposurenotifications/nearby/DiagnosisKeyFileSubmitter.java

TRACKERS

TRACKER	CATEGORIES	URL
Bugsnag	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/207
Matomo (Piwik)	Analytics	https://reports.exodus-privacy.eu.org/trackers/138

PLAYSTORE INFORMATION

Title: COVID Defense

Score: 3.57 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** 6.0 and up **Category:** Health & Fitness **Play Store URL:** org.pathcheck.la.bt

Developer Details: State of Louisiana, 8181680172265163636, Louisiana Division of Administration 1201 N 3rd St. Baton Rouge, LA 70802-5243, https://www.coviddefensela.com/, COVIDDefenseSupport@la.gov,

Release Date: Jan 7, 2021 **Privacy Policy:** Privacy link

Description:

COVID Defense is an easy-to-use app created by the Louisiana Department of Health. COVID Defense protects your privacy while helping protect you from COVID-19. You will get an alert if you are in close contact with someone who tests positive for COVID-19. By adding this free app to your phone, you join thousands of people helping to protect one another from COVID by knowing if you've been exposed. The COVID Defense app was built using an open-source project developed by PathCheck Foundation.

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 v3.4.6 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.