ANDROID STATIC ANALYSIS REPORT

File Name:	android.zip
Package Name:	org.pathcheck.covidsafepaths
Average CVSS Score:	6.3
App Security Score:	100/100 (LOW RISK)
Scan Date:	Jan. 27, 2021, 6:23 p.m.

FILE INFORMATION

File Name: android.zip
Size: 2.53MB
MD5: 0547b0c76fdd8c12ff85cff3ed9fe715
SHA1: bc51e571571effce72f53ee90ca8691e5b7e3dae
SHA256: 118a66ebf4562d936b927b8cca197f1c14d41387023d3e651d2a75092d8b8326

APP INFORMATION

App Name:
Package Name: org.pathcheck.covidsafepaths
Main Activity: .SplashActivity
Target SDK:
Min SDK:
Max SDK:
Android Version Name:
Android Version Code:

APP COMPONENTS

Activities: 2
Services: 0
Receivers: 1
Providers: 0
Exported Activities: 1
Exported Services: 0
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

Failed to read Code Signing Certificate or none available.

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.

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
.MainActivity	Schemes: pathcheck://, https://, Hosts: exposureHistory, ${enxDomain},

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	Launch Mode of Activity (.MainActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
2	Activity (.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.
3	Broadcast Receiver (.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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CVSS V2: 7.5 None (high) CWE: CWE-532 Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	org/pathcheck/covidsafepaths/exposurenotifications/nearby/ExposureConfigurations.kt org/pathcheck/covidsafepaths/exposurenotifications/nearby/ProvideDiagnosisKeysWorker.java org/pathcheck/covidsafepaths/exposurenotifications/network/DiagnosisKeyDownloader.java org/pathcheck/covidsafepaths/exposurenotifications/network/escrowserver/EscrowVerificationClient.kt org/pathcheck/covidsafepaths/exposurenotifications/nearby/DiagnosisKeyFileSubmitter.java org/pathcheck/covidsafepaths/exposurenotifications/nearby/StateUpdatedWorker.java org/pathcheck/covidsafepaths/helpers/BluetoothHelper.kt org/pathcheck/covidsafepaths/exposurenotifications/network/Uris.java org/pathcheck/covidsafepaths/exposurenotifications/nearby/ExposureNotificationBroadcastReceiver.java org/pathcheck/covidsafepaths/exposurenotifications/storage/Migration.kt org/pathcheck/covidsafepaths/exposurenotifications/ExposureNotificationClientWrapper.java org/pathcheck/covidsafepaths/exposurenotifications/reactmodules/ExposureNotificationsModule.java org/pathcheck/covidsafepaths/exposurenotifications/reactmodules/UtilsModule.java org/pathcheck/covidsafepaths/exposurenotifications/network/escrowserver/DeviceIDHelper.kt
2	This App uses an SSL Pinning Library (org.thoughtcrime.ssl.pinning) to prevent MITM attacks in secure communication channel.	secure	CVSS V2: 0 None (info) OWASP MASVS: MSTG-NETWORK-4	org/pathcheck/covidsafepaths/exposurenotifications/network/escrowserver/EscrowVerificationClient.kt
3	Files may contain hardcoded sensitive informations like usernames, passwords, keys etc.	high	CVSS V2: 7.4 None (high) CWE: CWE-312 Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	org/pathcheck/covidsafepaths/exposurenotifications/storage/objects/KeyValues.kt org/pathcheck/covidsafepaths/exposurenotifications/storage/RealmSecureStorageBte.kt

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	App can write to App Directory. Sensitive Information should be encrypted.	info	CVSS V2: 3.9 None (low) CWE: CWE-276 Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	org/pathcheck/covidsafepaths/exposurenotifications/storage/ExposureNotificationSharedPreferences.java
5	This App use Realm Database with encryption.	secure	CVSS V2: 0 None (info) OWASP MASVS: MSTG-CRYPTO-1	org/pathcheck/covidsafepaths/exposurenotifications/storage/RealmSecureStorageBte.kt
6	This App uses SafetyNet API.	secure	CVSS V2: 0 None (info) OWASP MASVS: MSTG-RESILIENCE-7	org/pathcheck/covidsafepaths/exposurenotifications/network/escrowserver/DeviceIDHelper.kt

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 generate no asymmetric cryptographic keys.
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 does not encrypt files in non-volatile memory.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 not encrypt any data in traffic or does not transmit any data between itself and another trusted IT product.
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using 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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.apache.org	good	**IP:** 95.216.26.30 **Country:** Finland **Region:** Uusimaa **City:** Helsinki **Latitude:** 60.169521 **Longitude:** 24.93545 **View:** Google Map
developers.google.com	good	**IP:** 172.217.12.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

URLS

URL	FILE
https://developers.google.com/android/exposure-notifications/exposure-notifications-api#methods	org/pathcheck/covidsafepaths/exposurenotifications/ExposureNotificationClientWrapper.java
https://www.apache.org/licenses/LICENSE-2.0	org/pathcheck/covidsafepaths/exposurenotifications/network/DiagnosisKeys.java
https://www.apache.org/licenses/LICENSE-2.0	org/pathcheck/covidsafepaths/exposurenotifications/network/DiagnosisKeyDownloader.java
https://www.apache.org/licenses/LICENSE-2.0	org/pathcheck/covidsafepaths/exposurenotifications/network/DiagnosisKey.java
https://www.apache.org/licenses/LICENSE-2.0	org/pathcheck/covidsafepaths/exposurenotifications/network/Uris.java
https://www.apache.org/licenses/LICENSE-2.0	org/pathcheck/covidsafepaths/exposurenotifications/network/KeyFileBatch.java
https://www.apache.org/licenses/LICENSE-2.0	org/pathcheck/covidsafepaths/exposurenotifications/network/RequestQueueSingleton.java
https://www.apache.org/licenses/LICENSE-2.0	org/pathcheck/covidsafepaths/exposurenotifications/storage/ExposureNotificationSharedPreferences.java
https://www.apache.org/licenses/LICENSE-2.0	org/pathcheck/covidsafepaths/exposurenotifications/storage/objects/ExposureEntity.java
https://www.apache.org/licenses/LICENSE-2.0	org/pathcheck/covidsafepaths/exposurenotifications/nearby/DiagnosisKeyFileSubmitter.java
https://www.apache.org/licenses/LICENSE-2.0 https://developers.google.com/android/exposure-notifications/implementation-guide#workmanager	org/pathcheck/covidsafepaths/exposurenotifications/nearby/ProvideDiagnosisKeysWorker.java
https://www.apache.org/licenses/LICENSE-2.0	org/pathcheck/covidsafepaths/exposurenotifications/nearby/StateUpdatedWorker.java
https://developers.google.com/android/exposure-notifications/exposure-notifications-api#broadcast-receivers	org/pathcheck/covidsafepaths/exposurenotifications/nearby/ExposureNotificationBroadcastReceiver.java
https://www.apache.org/licenses/LICENSE-2.0	org/pathcheck/covidsafepaths/exposurenotifications/common/AppExecutors.java
https://www.apache.org/licenses/LICENSE-2.0	org/pathcheck/covidsafepaths/exposurenotifications/common/TaskToFutureAdapter.java

PLAYSTORE INFORMATION

Title: SafePlaces

Score: 4.1486487 **Installs:** 10,000+ **Price:** 0 **Android Version Support:** 5.0 and up **Category:** Tools **Play Store URL:** org.pathcheck.covidsafepaths

Developer Details: Path Check, Inc, Path+Check,+Inc, None, https://pathcheck.org, support@pathcheck.org,

Release Date: Apr 15, 2020 **Privacy Policy:** Privacy link

Description:

PathCheck (formerly COVID Safe Paths) can privately save the places you visit and store them on your phone. Subscribe to Healthcare Authorities in your area for information about COVID-19 near you, where available. Receive alerts from your local Healthcare Authority with information about potential exposure to COVID-19. We are a global movement to develop free, open-source, privacy-by-design tools for residents, public health officials, and larger communities. The PathCheck program has spun out of initial privacy-first research conducted by MIT and TripleBlind, into a newly created non-profit called PathCheck Foundation, established with the initial purpose of supporting global rollout of the PathCheck app and associated tools for contact tracers and healthcare authorities. The goal of PathCheck is to help enable the reemergence and re-opening of economies and communities. Through global partnerships, we are prepared to support public health officials everywhere in the effort to slow the spread of COVID-19.

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 v3.2.5 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.