



ANDROID STATIC ANALYSIS REPORT



 Covid19Verify (1.3.10)

File Name: lv.verification.dgc.apk

Package Name: lv.verification.dgc





Scan Date: May 9, 2022, 6:03 a.m.

App Security Score: 61/100 (LOW RISK)

Grade:



FINDINGS SEVERITY

 HIGH	 WARNING	 INFO	 SECURE
1	5	2	2

FILE INFORMATION

File Name: lv.verifikation.dgc.apk

Size: 3.08MB

MD5: d849fd4987423f57a216c5a1edea5b3a

SHA1: 3a9b3cfbeb856bd9f3ff85042f3b4a84240f3ed3

SHA256: 074cd4b8b92e871b61f9aa815f2c907f2d29b1f05ca40bc215d74591dbb06097

APP INFORMATION

App Name: Covid19Verify

Package Name: lv.verifikation.dgc

Main Activity: lv.verifikation.dgc.MainActivity

Target SDK: 30

Min SDK: 21

Max SDK:

Android Version Name: 1.3.10

Android Version Code: 36

APP COMPONENTS

Activities: 4

Services: 3

Receivers: 0

Providers: 1

Exported Activities: 0

Exported Services: 1

Exported Receivers: 0

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: 2021-06-01 04:59:45+00:00

Valid To: 2051-06-01 04:59:45+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0xe9e61a7dac1c89dea394deab636defdd41eb581c

Hash Algorithm: sha256

md5: 32873f6f62bcc72f700acda19b95ef8e

sha1: 1ab1383632e4282dc1f0023a554a0be6332c989

sha256: 74f10864e1a5baf78f1e76a5529eb8745fe25832bb062f0809ff3bd4ca9c531a

sha512: 10e05053dc462f44907b40d30c3fa791e695f7ed024c106041ed7000e2ec2f71add4315cd98c009df1491f22d5b29c2721d5c3b0fe2f162d47fc662cca223b63

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 859e24b7735b728bc55255cd04c978072aa703d50fe71c55d0a220bcf1be5db7

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.TAGS check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	unknown (please file detection issue!)



NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------



MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) 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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				net/sqlcipher/database/SQLiteQuery.java com/getcapacitor/community/databases/sqlite/e/c/e.java a/e/j/b0/b.java net/sqlcipher/database/SQLiteQueryBuilder.java net/sqlcipher/database/SQLiteCompiledSql.java b/a/b/a/v/a/a.java com/getcapacitor/community/databases/sqlite/CapacitorSQLitePlugin.java com/journeyapps/barcodescanner/java net/sqlcipher/database/SqliteWrapper.java com/journeyapps/barcodescanner/java a/j/a/b.java net/sqlcipher/database/SQLiteProgram.java net/sqlcipher/database/SQLiteContentHelper.java b/a/b/a/v/a/b.java a/e/j/b.java net/sqlcipher/database/SQLiteOpenHelper.java a/a/n/g.java com/journeyapps/barcodescanner/xp.java a/a/k/a/a.java b/a/c/s/a/n/a.java com/getcapacitor/community/databases/sqlite/e/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	c/sqlcipher/c/a.java com/journeyapps/barcodescanner/x/g.java net/sqlcipher/AbstractCursor.java net/sqlcipher/database/SQLiteDatabase.java net/sqlcipher/BulkCursorToCursorAdapter.java net/sqlcipher/DefaultDatabaseErrorHandler.java net/sqlcipher/database/SQLiteDebug.java a/e/d/g.java b/a/c/s/a/n/b/a.java com/whitestain/securestorage/a.java com/getcapacitor/community/databases/sqlite/e/e.java a/e/d/c.java com/getcapacitor/community/databases/sqlite/d.java net/sqlcipher/DatabaseUtils.java a/n/a/a/h.java b/a/a/a/a/b/y.java a/e/j/a0.java com/getcapacitor/I0.java b/a/b/a/v/a/c.java com/journeyapps/barcodescanner/x/m.java a/e/j/v.java b/a/c/s/a/d.java a/e/j/f.java a/m/a.java a/e/j/t.java com/journeyapps/barcodescanner/x/e.java a/e/d/e.java com/journeyapps/barcodescanner/x/f.java b/a/c/s/a/f.java com/getcapacitor/community/databases/sqlite/e/h.java com/journeyapps/barcodescanner/x/i

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/journeyapps/barcodescanner/m.ja a/e/d/f.java b/a/a/a/a/b/a.java com/dutchconcepts/capacitor/barcode scanner/BarcodeScanner.java a/e/j/h.java com/journeyapps/barcodescanner/x/k. java a/e/j/s.java com/getcapacitor/plugin/http/Http.java com/getcapacitor/community/databas e/sqlite/e/a.java a/e/d/j.java a/e/d/k.java
2	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/getcapacitor/b0.java com/getcapacitor/plugin/http/c.java com/capacitorjs/plugins/filesystem/a.j ava
3	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/getcapacitor/b0.java com/getcapacitor/community/databas e/sqlite/e/g.java com/journeyapps/barcodescanner/j.ja va
4	This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files.	info	OWASP MASVS: MSTG-CRYPTO-1	com/getcapacitor/community/databas e/sqlite/e/g.java com/getcapacitor/community/databas e/sqlite/e/a.java
5	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	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	net/sqlcipher/database/SQLiteDatabase.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	b/a/a/a/a/b/o.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 invoke the functionality provided by the platform to securely store 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 ['camera', 'network connectivity'].
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.

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 encrypt some transmitted data with HTTPS/TLS/SSH 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.
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 in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode or AES-GCM (as defined in NIST SP 800-38D) and cryptographic key sizes 256-bit/128-bit.
13	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1/SHA-256/SHA-384/SHA-512 and message digest sizes 160/256/384/512 bits.
14	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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
15	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.
16	FCS_CKM.1.1(2)	Optional Security Functional Requirements	Cryptographic Symmetric Key Generation	The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
github.com	ok	IP: 140.82.121.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
journeyapps.com	ok	IP: 108.156.22.6 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.zetetic.net	ok	IP: 108.156.22.129 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
capacitorjs.com	ok	IP: 76.76.21.123 Country: United States of America Region: California City: Walnut Latitude: 34.015400 Longitude: -117.858223 View: Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"
"library_zxingandroidembedded_author" : "JourneyApps"
"library_zxingandroidembedded_authorWebsite" : "https://journeyapps.com/"

PLAYSTORE INFORMATION

Title: Covid19Verify

Score: 0 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** 5.0 and up **Category:** Medical **Play Store URL:** [lv.verify.dgc](https://play.google.com/store/apps/details?id=lv.verify.dgc)

Developer Details: SPKC, SPKC, Duntes iela 22, k-5, Rīga, Latvija, LV 1005, None, covid19verify@vmnvd.gov.lv,

Release Date: Jul 1, 2021 **Privacy Policy:** [Privacy link](#)

Description:

Covid19Verify lietotne sniedz iespēju pārbaudīt atbilstoši EU regulai izsniegto Covid-19 sertifikātu derīgumu un autentiskumu, ievērojot Latvijā pieņemtos noteikumus. Pārbaude tiek veikta skenējot personas uzrādītā sertifikāta QR kodu. Lietotne ļauj noteikt derīgumu šāda veida sertifikātiem – sertifikāts par veikto vakcināciju pret Covid-19, sertifikāts par Covid-19 laboratoriskās pārbaudes rezultātiem, sertifikāts par Covid-19 izslimošanas faktu. Lietotnes izmantošana - atverot lietotni, jāizmanto ierīcē iebūvētā foto kamera un jānoskenē QR kods. Lietotne uzrāda paziņojumu par to, vai noskenētais sertifikāts ir derīgs vai nav derīgs.

Report Generated by - MobSF v3.5.1 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.

© 2022 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).