MOBSF

ANDROID STATIC ANALYSIS REPORT

GreenCheck (1.18)

File Name:	at.itsv.mobile.cochap.apk
Package Name:	at.itsv.mobile.cochap
Scan Date:	May 7, 2022, 1:29 p.m.
App Security Score:	53/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	WARNING	INFO	SECURE
2	9	1	2

FILE INFORMATION

File Name: at.itsv.mobile.cochap.apk
Size: 10.74MB
MD5: 06e10ff1865763772823caefb9522a3f
SHA1: 804e59f4fd35bc7db3f9cc433c2f9d44d91e0caa
SHA256: 6739b36398149c367ac4a4524eaed6948e3d53e02df411b6ba73a9060f3f7876

APP INFORMATION

App Name: GreenCheck
Package Name: at.itsv.mobile.cochap
Main Activity: at.itsv.mobile.cochap.SplashActivity
Target SDK: 30
Min SDK: 21
Max SDK:
Android Version Name: 1.18
Android Version Code: 251

APP COMPONENTS

Activities: 3
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 1
Exported Services: 0
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: 2021-07-22 12:24:58+00:00
Valid To: 2051-07-22 12:24:58+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xf50689b0617a82ce083eb3a27b141c95b20e771a
Hash Algorithm: sha256
md5: 745928c831857eeb8025fa25c61df04a
sha1: ae5b4acb7c3293ea19870d6dd70dbb91e862d17c
sha256: e200d2ce7bad4a61bb29b69beb13fb0e56b9f363c6d8588cd05cf99fc806f32d
sha512: 1d37ddce3e7b558135a898dd24899f57704f7b2a4c13888e92052615d1decfbbd013c4adab5f0c9d2c45547da1013a0796dae434af4e47fb2540b7f74c1dcd08
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 190a0872f3f53978ee477a4d7fb58b041c3d834deaee73b16bf5bf5705ded1b4

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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.USE_BIOMETRIC	normal		Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.CHANGE_WIFI_MULTICAST_STATE	normal	allow Wi-Fi Multicast reception	Allows an application to receive packets not directly addressed to your device. This can be useful when discovering services offered nearby. It uses more power than the non-multicast mode.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
possible Build.SERIAL check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
network operator name check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Activity (at.itsv.mobile.cochap.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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/lwansbrough/RCTCamera/RCTCameraModule.java com/tozny/crypto/android/AesCbcWithIntegrity.java com/horcrux/svg/VirtualView.java com/learnium/RNDeviceInfo/RNInstallReferrerClient.java com/horcrux/svg/UseView.java com/securepreferences/SecurePreferencesOld.java com/koushikdutta/async/PushParser.java com/drew/imaging/ImageMetadataReader.java com/drew/tools/ExtractJpegSegmentTool.java com/koushikdutta/async/http/server/AsyncHttpServerRequestImpl.java com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/drew/tools/ProcessUrlUtility.java com/oblador/keychain/decryptionHandler/DecryptionResultHandlerInteractiveBiometric.java com/koushikdutta/async/ByteBufferList.java com/lwansbrough/RCTCamera/RCTCameraViewFinder.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	com/swmansion/reanimated/nodes/DebugNode.java com/learnium/RNDeviceInfo/RNDeviceModule.java com/horcrux/svg/Brush.java com/oblador/keychain/KeychainModule.java com/peel/react/TcpSockets.java org/reactnative/facedetector/tasks/FileFaceDetectionAsyncTask.java com/horcrux/svg/MaskView.java com/reactnativecommunity/asyncstorage/AsyncStorageExpoMigration.java com/koushikdutta/async/AsyncNetworkSocket.java com/koushikdutta/async/AsyncServer.java com/learnium/RNDeviceInfo/resolver/DeviceIdResolver.java com/oblador/keychain/cipherStorage/CipherStorageBase.java com/oblador/keychain/cipherStorage/CipherStorageFacebookConceal.java com/koushikdutta/async/http/AsyncHttpRequest.java com/horcrux/svg/LinearGradientView.java com/reactnativecommunity/asyncstorage/AsyncStorageModule.java com/swmansion/gesturehandler/react/RNGestureHandlerRootView.java com/oblador/keychain/cipherStorage/CipherStorageKeystoreRsaEcb.java com/oblador/keychain/cipherStorage/CipherStorageKeystoreAesCbc.java com/horcrux/svg/ImageView.java com/securepreferences/SecurePreferences.java com/swmansion/reanimated/NativeMethodsHelper.java com/drew/lang/CompoundException.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java com/horcrux/svg/PatternView.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/tradle/react/UdpSockets.java com/horcrux/svg/ClipPathView.java com/swmansion/gesturehandler/react/RNGestureHandlerRootHelper.java io/github/aakira/napier/DebugAntilog.java com/lugg/ReactNativeConfig/ReactNativeConfigModule.java COSE/ASN1.java com/horcrux/svg/RadialGradientView.java com/taluttasgiran/rnsecurestorage/RNKeyStore.java com/lwansbrough/RCTCamera/RCTCamera.java com/oblador/keychain/decryptionHandler/DecryptionResultHandlerInteractiveBiometricManualRetry.java com/lwansbrough/RCTCamera/MutableImage.java com/drew/tools/ProcessAllImagesInFolderUtility.java com/th3rdwave/safeareacontext/SafeAreaView.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/lwansbrough/RCTCamera/RCTCameraModule.java com/learnium/RNDeviceInfo/RNDeviceModule.java
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/lwansbrough/RCTCamera/RCTCameraModule.java
4	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/tozny/crypto/android/AesCbcWithIntegrity.java com/koushikdutta/async/http/WebSocketImpl.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	com/tectiv3/aes/RCTAes.java
6	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	com/reactnativecommunity/asyncstorage/ReactDatabaseSupplier.java com/reactnativecommunity/asyncstorage/AsyncLocalStorageUtil.java
7	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/koushikdutta/async/AsyncSSLSocketWrapper.java net/i2p/crypto/eddsa/EdDSASecurityProvider.java com/koushikdutta/async/dns/Dns.java
8	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/koushikdutta/async/AsyncSSLSocketWrapper.java
9	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	org/reactnative/facedetector/tasks/FileFaceDetectionAsyncTask.java com/bitgo/randombytes/RandomBytesModule.java
10	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	j$/util/concurrent/ThreadLocalRandom.java com/koushikdutta/async/util/FileCache.java com/koushikdutta/async/dns/Dns.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/koushikdutta/async/util/FileCache.java com/koushikdutta/async/http/spdy/ByteString.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 implement 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 ['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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.
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_CKM.1.1(3),FCS_CKM.1.2(3)	Selection-Based Security Functional Requirements	Password Conditioning	A password/passphrase shall perform [Password-based Key Derivation Functions] in accordance with a specified cryptographic algorithm..
13	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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
14	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.
15	FCS_COP.1.1(4)	Selection-Based Security Functional Requirements	Cryptographic Operation - Keyed-Hash Message Authentication	The application perform keyed-hash message authentication with cryptographic algorithm ['HMAC-SHA-256'] .
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.1.1	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The application validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates', 'The certificate path must terminate with a trusted CA certificate'].
19	FIA_X509_EXT.1.2	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.
20	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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
21	FIA_X509_EXT.2.2	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	When the application cannot establish a connection to determine the validity of a certificate, the application allow the administrator to choose whether to accept the certificate in these cases or accept the certificate ,or not accept the certificate.
22	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.
23	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
xerces.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
iptc.org	ok	**IP:** 3.64.29.21 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
pwall.net	ok	**IP:** 92.243.0.172 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map
www.w3.org	ok	**IP:** 128.30.52.100 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.365078 **Longitude:** -71.104523 **View:** Google Map
purl.org	ok	**IP:** 207.241.239.242 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.781734 **Longitude:** -122.459435 **View:** Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
drewnoakes.com	ok	**IP:** 50.17.237.32 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
cipa.jp	ok	**IP:** 118.82.81.189 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
www.aiim.org	ok	**IP:** 199.60.103.225 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.370129 **Longitude:** -71.086304 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.npes.org	ok	**IP:** 216.33.126.92 **Country:** United States of America **Region:** Virginia **City:** Vienna **Latitude:** 38.926575 **Longitude:** -77.262360 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
xml.org	ok	**IP:** 104.239.240.11 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
raw.githubusercontent.com	ok	**IP:** 185.199.111.133 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
greencheck.gv.at	ok	**IP:** 157.177.248.43 **Country:** Austria **Region:** Wien **City:** Vienna **Latitude:** 48.208488 **Longitude:** 16.372080 **View:** Google Map
ns.useplus.org	ok	**IP:** 54.83.4.77 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
json-schema.org	ok	**IP:** 172.67.130.91 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

PLAYSTORE INFORMATION

Title: GreenCheck

Score: 0 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** 5.0 and up **Category:** Medical **Play Store URL:** at.itsv.mobile.cochap

Developer Details: Österreichische Sozialversicherung, %C3%96sterreichische+Sozialversicherung, None, https://greencheck.gv.at/, greencheck@itsv.at,

Release Date: Jul 22, 2021 **Privacy Policy:** Privacy link

Description:

GreenCheck ermöglicht Ihnen die rasche und unkomplizierte Kontrolle, ob einer zu überprüfenden Person Zutritt bzw. die Einreise nach Österreich gewährt werden darf. Der Check erfolgt über den Scan des digitalen oder ausgedruckten EU-konformen QR-Codes. Schnelle Klarheit: Ist die Person, basierend auf den Regeln der COVID-19 Öffnungs- bzw. Einreiseverordnung, zutrittsberechtigt, bekommen Sie das Ergebnis „Prüfung gültig“ angezeigt. Ist dies nicht der Fall oder der gescannte QR-Code ist als Zutrittsnachweis ungeeignet, erhalten Sie das Scan-Ergebnis „Prüfung ungültig“.

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.