MOBSF

ANDROID STATIC ANALYSIS REPORT

CoronaReport (2.9.5)

File Name:	CoronaReport 2.9.5.apk
Package Name:	com.spotteron.coronareport
Average CVSS Score:	6.6
App Security Score:	55/100 (MEDIUM RISK)
Trackers Detection:	1/285

FILE INFORMATION

File Name: CoronaReport 2.9.5.apk
Size: 16.74MB
MD5: 43a5bbe365e511bb4888d62a9f91ef63
SHA1: 7417e031744fdf1545b84c291938609722201b35
SHA256: d948a52831d6891f9bbedd1a6802310eb684674694fa86f1028a081aa0e55f59

APP INFORMATION

App Name: CoronaReport
Package Name: com.spotteron.coronareport
Main Activity: com.spotteron.coronareport.CoronaReport
Target SDK: 28
Min SDK: 19
Max SDK:
Android Version Name: 2.9.5
Android Version Code: 20905

APP COMPONENTS

Activities: 3
Services: 5
Receivers: 4
Providers: 3
Exported Activities: 1
Exported Services: 4
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-04-02 22:56:10+00:00
Valid To: 2042-08-18 22:56:10+00:00
Issuer: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Serial Number: 0x41ca06c5
Hash Algorithm: sha256
md5: 3c8344d2664c9d2fb8b0c2264d8786ca
sha1: 55a65780a6d05660fc9519e9476455f1988a735a
sha256: 349b5c8f34705d3591ffca661a6d9d022a21c74c25648cd0ec9c7266b710fac7
sha512:
3840f0ed1e6eebcb3b3a3004b16980de4ba02b9c827542e167d74bbfb37772bf638c4c2eab28f2d0e7f336a560506217ea86402bebfc70665085a1c2564153a4

PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: aa558640bf5c9f6879f0118427db08c9bacc702c2b457c3fe2125eff6a077964

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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
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.
android.permission.WAKE_LOCK	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.spotteron.coronareport.permission.C2D_MESSAGE	signature	Allows cloud to device messaging	Allows the application to receive push notifications.
com.sec.android.provider.badge.permission.READ	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.sec.android.provider.badge.permission.WRITE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.htc.launcher.permission.READ_SETTINGS	dangerous	Unknown permission from android reference	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
com.htc.launcher.permission.UPDATE_SHORTCUT	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.sonyericsson.home.permission.BROADCAST_BADGE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.anddoes.launcher.permission.UPDATE_COUNT	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.majeur.launcher.permission.UPDATE_BADGE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.huawei.android.launcher.permission.CHANGE_BADGE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.huawei.android.launcher.permission.READ_SETTINGS	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.huawei.android.launcher.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
android.permission.READ_APP_BADGE	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.oppo.launcher.permission.READ_SETTINGS	dangerous	Unknown permission from android reference	Unknown permission from android reference
com.oppo.launcher.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
me.everything.badger.permission.BADGE_COUNT_READ	dangerous	Unknown permission from android reference	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	dangerous	Unknown permission from android reference	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	<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 possible Build.SERIAL check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>dx</td></tr></table>

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.
Broadcast Receiver (nl.xservices.plugins.ShareChooserPendingIntent) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
Activity (com.adobe.phonegap.push.PushHandlerActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.spotteron.coronareport.permission.PushHandlerActivity [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. 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.
Service (com.adobe.phonegap.push.FCMService) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Service is explicitly exported.
Service (com.adobe.phonegap.push.PushInstanceIDListenerService) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Service is explicitly exported.

ISSUE	SEVERITY	DESCRIPTION
Service (com.google.firebase.messaging.FirebaseMessagingService) 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.
Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [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.
Service (com.google.firebase.iid.FirebaseInstanceIdService) 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

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/sqlc/SQLiteAndroidDatabase.java io/sqlc/SQLitePlugin.java me/leolin/shortcutbadger/ShortcutBadger.java com/adobe/phonegap/push/PushPlugin.java com/adobe/phonegap/push/FCMService.java com/adobe/phonegap/push/PushDismissedHandler.java com/adobe/phonegap/push/PushInstanceIDListenerService.java com/adobe/phonegap/push/BackgroundActionButtonHandler.java com/adobe/phonegap/push/PushHandlerActivity.java
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.	high	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	io/sqlc/SQLiteAndroidDatabase.java
App can read/write to External Storage. Any App can read data written to External Storage.	high	CVSS V2: 5.5 (medium) CWE: CWE-276 - Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	nl/xservices/plugins/SocialSharing.java

ISSUE	SEVERITY	STANDARDS	FILES
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	nl/xservices/plugins/SocialSharing.java com/verso/cordova/clipboard/Clipboard.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	com/adobe/phonegap/push/FCMService.java com/adobe/phonegap/push/PushConstants.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
api.whatsapp.com	good	**IP:** 157.240.8.53 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map
spotteron-382a0.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
data:image/ https://api.whatsapp.com/send?phone=	nl/xservices/plugins/SocialSharing.java
https://spotteron-382a0.firebaseio.com	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS

FIREBASE URL	DETAILS
https://spotteron-382a0.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
someone@domain.com	nl/xservices/plugins/SocialSharing.java

TRACKERS

TRACKER	URL
Google Firebase Analytics	https://reports.exodus-privacy.eu.org/trackers/49

PLAYSTORE INFORMATION

Title: CoronaReport - COVID-19 reports for Social Science

Score: 0.0 **Installs:** 100+ **Price:** 0 **Android Version Support:** 4.4 and up **Category:** Health & Fitness **Play Store URL:** com.spotteron.coronareport

Developer Details: SPOTTERON, SPOTTERON, Faßziehergasse 5, 1070 Wien, https://www.spotteron.net, office@spotteron.net,

Release Date: Mar 23, 2020 **Privacy Policy:** Privacy link

Description:

CoronaReport is a citizen science project developed by the Scottish Collaboration for Public Health Research and Policy (SCPHRP), and the University of Edinburgh. Citizens can record their experiences of the disease, and the effects on their lives. The app is not intended to be used for/in emergencies or for diagnostics/medical purposes. Coronavirus (COVID-19) is the viral pandemic affecting communities worldwide. The pandemic's impacts are varied and substantial. CoronaReport is a citizen science project which democratizes the reporting on the Coronavirus, and makes these reports accessible to other citizens. You can create public reports about your experiences, including how the virus is affecting your area and the way your community functions (e.g., schools, nursing homes, and businesses). About the project The collected and anonymized data from the reports will then be shared on the CoronaReport platform enabling you and other citizens to see first-hand accounts about how people are feeling and experiencing the impact of coronavirus. You can choose how much information you want to contribute to your reports and if you want to connect with others to share experiences. By working together citizens can build a real-time and vivid picture of how coronavirus is influencing the way people live and work. For example, we do not know the extent to which countermeasures like social distancing are being practised and how this, and other countermeasures, are affecting people's well-being. Find out more about the project on the website: www.coronareport.global The project is running on the SPOTTERON Citizen Science Platform.

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.