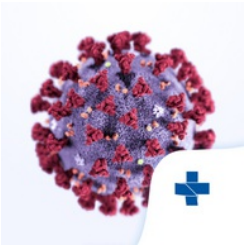
MOBSF

ANDROID STATIC ANALYSIS REPORT



Coronavírus SUS (2.0.5)

File Name:	Coronavírus SUS 2.0.5.apk
Package Name:	br.gov.datasus.guardioes
Average CVSS Score:	5.8
App Security Score:	40/100 (HIGH RISK)
Trackers Detection:	2/285

FILE INFORMATION

File Name: Coronavírus SUS 2.0.5.apk
Size: 21.89MB
MD5: a3a203ea67f8be4014156f88a9ebab44
SHA1: 9f5c11e43afffd7263df92c6c9cb5e4f6d5b3aa2
SHA256: 1a39dd147cb7afc403fa0a62ee0f4698a53de5c8690ca179057164e287c386ea

APP INFORMATION

App Name: Coronavírus SUS
Package Name: br.gov.datasus.guardioes
Main Activity: br.gov.datasus.guardioes.MainActivity
Target SDK: 28
Min SDK: 19
Max SDK:
Android Version Name: 2.0.5
Android Version Code: 20005

APP COMPONENTS

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

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=BR, ST=Distrito Federal, L=Brasilia, O=Datasus, OU=Datasus, CN=Ministerio da Saude
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-04-26 14:33:14+00:00
Valid To: 2044-09-11 14:33:14+00:00
Issuer: C=BR, ST=Distrito Federal, L=Brasilia, O=Datasus, OU=Datasus, CN=Ministerio da Saude
Serial Number: 0x4343e308
Hash Algorithm: sha256
md5: e7a4a258e3b96225466083f1ac27d381
sha1: 291c7b6162b6e6cd0659149c4c20ad1b4de21d7c
sha256: cd2455b18f3a33decec3c97cc9a1c9ab367fb5ee417fcfa37e4f282008d15617
sha512:
ae7c222905512fe3f60874a75042c7f665fd1267c00b47c42e029974064b08b4bbe74dc4f5685effd466c248d66cf750830e4db050488ed739735e536c34d02e

PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: d828551ca1609ccd14fd48f2e1693ec616ccd75bb5f1f722c848f7d7bfb5f0ce

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.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
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.
br.gov.datasus.guardioes.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

PERMISSION	STATUS	INFO	DESCRIPTION
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
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

PERMISSION	STATUS	INFO	DESCRIPTION
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

<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.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible Build.SERIAL check
Build.TAGS check
network operator name check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
App has a Network Security Configuration [android:networkSecurityConfig]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
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.
Activity (com.adobe.phonegap.push.PushHandlerActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: br.gov.datasus.guardioes.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/SQLiteConnectorDatabase.java io/sqlc/SQLitePlugin.java uk/co/workingedge/phonegap/plugin/LaunchNavigatorPlugin.java uk/co/workingedge/phonegap/plugin/CordovaLogger.java me/leolin/shortcutbadger/ShortcutBadger.java com/dynatrace/android/agent/util/Utility.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 com/ionicframework/cordova/webview/WebViewLocalServer.java com/ionicframework/cordova/webview/AndroidProtocolHandler.java com/ionicframework/cordova/webview/IonicWebViewEngine.java

ISSUE	SEVERITY	STANDARDS	FILES
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 com/dynatrace/android/agent/db/ParmDbHelper.java com/dynatrace/android/agent/db/EventsDbHelper.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	uk/co/workingedge/phonegap/plugin/LaunchNavigatorPlugin.java com/adobe/phonegap/push/FCMService.java com/adobe/phonegap/push/PushConstants.java
This App uses Java Hash Code. It's a weak hash function and should never be used in Secure Crypto Implementation.	warning	**CVSS V2:** 2.3 (low) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP MASVS:** MSTG-CRYPTO-4	com/dynatrace/android/app/LcContext.java com/dynatrace/android/agent/CalloutTable.java com/dynatrace/android/callback/OkCallback.java com/dynatrace/android/callback/OkInterceptor.java com/dynatrace/android/callback/CallbackCore.java
This App may have root detection capabilities.	secure	**CVSS V2:** 0 (info) **OWASP MASVS:** MSTG-RESILIENCE-1	com/dynatrace/android/agent/RootDetector.java com/dynatrace/android/agent/metrics/AndroidMetrics.java
IP Address disclosure	warning	**CVSS V2:** 4.3 (medium) **CWE:** CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor **OWASP MASVS:** MSTG-CODE-2	com/dynatrace/android/agent/Version.java
The App uses an insecure Random Number Generator.	high	**CVSS V2:** 7.5 (high) **CWE:** CWE-330 - Use of Insufficiently Random Values **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-6	com/dynatrace/android/agent/data/Session.java com/dynatrace/android/agent/data/RandomFactory.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
maps.google.com	good	**IP:** 216.58.196.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
share.here.com	good	**IP:** 3.86.128.108 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.04372 **Longitude:** -77.487488 **View:** Google Map
unknown.host	good	**IP:** 188.68.51.215 **Country:** Germany **Region:** Baden-Wurttemberg **City:** Karlsruhe **Latitude:** 49.004719 **Longitude:** 8.38583 **View:** Google Map
guardioes-e1626.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
live.dynatrace.com	good	No Geolocation information available.
citymapper.com	good	**IP:** 46.137.173.201 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.34399 **Longitude:** -6.26719 **View:** Google Map

URLS

URL	FILE
http://maps.google.com/maps? http://maps.google.com/maps?daddr= https://citymapper.com/directions? https://share.here.com/r/ https://maps.google.com/maps/api/geocode/json?	uk/co/workingedge/LaunchNavigator.java
https://live.dynatrace.com	com/dynatrace/android/agent/conf/DynatraceConfigurationBuilder.java
https://unknown.host	com/dynatrace/android/agent/conf/BuilderUtil.java
javascript:(function()	com/ionicframework/cordova/webview/IonicWebViewEngine.java
https://guardioes-e1626.firebaseio.com	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://guardioes-e1626.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

TRACKER	URL
Dynatrace	https://reports.exodus-privacy.eu.org/trackers/137
Google Firebase Analytics	https://reports.exodus-privacy.eu.org/trackers/49

PLAYSTORE INFORMATION

Title: Coronavírus - SUS

Score: 3.9788136 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** 4.4 and up **Category:** Health & Fitness **Play Store URL:** br.gov.datasus.guardioes

Developer Details: Governo do Brasil, 5829287075355252046, None, http://www.datasus.gov.br, mobile.datasus@saude.gov.br,

Release Date: Jul 5, 2018 **Privacy Policy:** Privacy link

Description:

O Ministério da Saúde lança o app Coronavírus-SUS com o objetivo de conscientizar a população sobre o Corona Vírus COVID-19, para isso o aplicativo conta com as seguintes funcionalidades: - Informativos de diversos tópicos como os sintomas, como se prevenir, o que fazer em caso de suspeita e infecção e etc; - Mapa indicando unidades de saúde próximas; - Em caso de suspeita de infecção, o cidadão pode conferir se os sintomas são compatíveis com o do Corona, e caso seja será instruído e encaminhado para a unidade de saúde básica mais próxima; - Área de notícias oficial do Ministério da Saúde com foco no Coronavírus.

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

APP SECURITY SCORE	RISK
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.