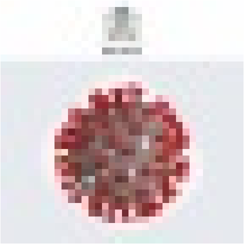
ANDROID STATIC ANALYSIS REPORT



Bolivia Segura (1.3)

File Name:	Bolivia Segura 1.3.apk
Package Name:	com.agetic.coronavirusapp
Average CVSS Score:	5.9
App Security Score:	10/100 (CRITICAL RISK)
Trackers Detection:	1/285

FILE INFORMATION

File Name: Bolivia Segura 1.3.apk

Size: 10.59MB

MD5: 2eba0cb988d96d1f8da365833cd59e25

SHA1: 8804483d1adfec3d44382d2e525d57516de1849f

SHA256: b687e22197dbbe768d04e044279159558353f2bdd83795576efc32253280bad9

APP INFORMATION

App Name: Bolivia Segura

Package Name: com.agetic.coronavirusapp

Main Activity: com.tns.NativeScriptActivity

Target SDK: 29

Min SDK: 17

Max SDK:

Android Version Name: 1.3

Android Version Code: 5

APP COMPONENTS

Activities: 3

Services: 6

Receivers: 2

Providers: 1

Exported Activities: 0

Exported Services: 2

Exported Receivers: 1

Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed

v1 signature: True

v2 signature: True

v3 signature: False

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: 2020-03-12 20:32:30+00:00

Valid To: 2050-03-12 20:32:30+00:00

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

Serial Number: 0x3864ed214ce83fcc3d7ca549b61f64ce1bfa5bb3

Hash Algorithm: sha256

md5: ef45787006af0e1b7c883994c6e74f7b

sha1: eec98cb82a5b9580a37c98308eecbd61d3885d9f

sha256: af7f0f8bcd4d08a1ab60894e72f2ad65d1013ca3a2bfae816661165e9696e09d

sha512:

a34f2a8f18bbe876dc7d5f700041632d837df47df836846382182c6bf434a1c0e8e4d992e46471f708b24ef6d1fced60d9daa91c6a3b97aa5141c113eccdcd24

PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 85a54842c1d03603ddce67a789c4175fbd2e4643cbf9a36e6fda4523675a03d6

Certificate Status: Good
Description: Certificate looks good.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read SD card contents	Allows an application to read from SD Card.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
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.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead
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.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
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.

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</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
Application Data can be Backed up [android:allowBackup=true]	medium	This flag 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 (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 (org.nativescript.plugins.firebase.MyFirebaseMessagingService) 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 (org.nativescript.plugins.firebase.MyFirebaseInstanceIDService) 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.

CODE ANALYSIS

ISSUE	SEVERITY	STANDARDS	FILES

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	org/nativescript/Process.java org/nativescript/plugins/firebase/FirebasePluginLifecycleCallbacks.java org/nativescript/plugins/firebase/FirebasePlugin.java org/nativescript/widgets/Async.java org/nativescript/widgets/CommonLayoutParams.java org/nativescript/widgets/StackLayout.java org/nativescript/widgets/image/Cache.java org/nativescript/widgets/image/Fetcher.java org/nativescript/widgets/image/AsyncTask.java org/nativescript/widgets/image/Worker.java org/ow2/asmdex/util/AsmDexifierApplicationVisitor.java com/tns/NativeScriptUncaughtExceptionHandler.java com/tns/AndroidJsV8Inspector.java com/tns/AssetExtractor.java com/tns/LogcatLogger.java com/tns/ManualInstrumentation.java com/tns/DexFactory.java com/tns/AppConfig.java com/tns/Runtime.java com/tns/RuntimeHelper.java com/tns/bindings/ProxyGenerator.java com/jesusm/kfingerprintmanager/base/FingerprintAssetsManager.java com/jesusm/kfingerprintmanager/base/keystore/KeyStoreManager.java
			org/nativescript/widgets/ViewHelper.java org/nativescript/widgets/BorderDrawable.java org/nativescript/widgets/image/Cache.java org/ow2/asmdex/encodedValue/EncodedValueArray.java org/ow2/asmdex/encodedValue/EncodedValueEnum.java org/ow2/asmdex/encodedValue/EncodedValueField.java org/ow2/asmdex/encodedValue/EncodedValueAnnotation.java org/ow2/asmdex/encodedValue/EncodedValueString.java org/ow2/asmdex/encodedValue/EncodedValueType.java org/ow2/asmdex/encodedValue/EncodedValueMethod.java org/ow2/asmdex/structureWriter/AnnotationDirectoryItem.java org/ow2/asmdex/structureWriter/ClassDefinitionItem.java org/ow2/asmdex/structureWriter/Method.java org/ow2/asmdex/structureWriter/ExceptionHandler.java org/ow2/asmdex/structureWriter/Prototype.java org/ow2/asmdex/structureWriter/AnnotationItem.java org/ow2/asmdex/structureWriter/AnnotationSetItem.java

ISSUE	SEVERITY	STANDARDS	FILES
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	org/ow2/asmdex/structureWriter/EncodedCatchHandler.java org/ow2/asmdex/structureWriter/AnnotationElement.java org/ow2/asmdex/structureWriter/Field.java org/ow2/asmdex/structureWriter/DebugInfoItem.java org/ow2/asmdex/structureWriter/TypeList.java com/tns/FragmentClass.java com/tns/NativeScriptWeakHashMap.java com/tns/NativeScriptActivity.java com/tns/AndroidJsV8Inspector.java com/tns/ManualInstrumentation.java com/tns/NativeScriptHashMap.java com/tns/NativeScriptAbstractMap.java com/tns/gen/org/nativescript/plugins/firebase/FirebasePluginListener.java com/tns/gen/org/nativescript/widgets/FragmentBase_script_37_1471960_n.java com/tns/gen/org/nativescript/widgets/Async_CompleteCallback.java com/tns/gen/org/nativescript/widgets/TabsBar_script_37_1475653_r.java com/tns/gen/org/nativescript/widgets/FragmentBase_script_37_1378639_n.java com/tns/gen/org/nativescript/widgets/FragmentBase_script_37_1247350_n.java com/tns/gen/org/nativescript/widgets/BottomNavigationBar_script_37_1380117_r.java com/tns/gen/java/lang/Object_script_37_764167_r.java com/tns/gen/java/lang/Object_script_37_1086373_n.java com/tns/gen/java/lang/Object_script_37_710371_r.java com/tns/gen/java/lang/Object_script_37_2343119_r.java com/tns/gen/java/lang/Object_script_37_1429700_r.java com/tns/gen/java/lang/Object_script_37_2467791_r.java com/tns/gen/java/lang/Object_script_37_1244713_r.java com/tns/gen/java/lang/Object_script_37_624767_r.java com/tns/gen/java/lang/Object_script_37_1095211_r.java com/tns/gen/java/lang/Object_script_37_2348740_r.java com/tns/gen/java/lang/Object_script_37_1245031_r.java com/tns/gen/java/lang/Object_script_37_1450793_r.java com/tns/gen/java/lang/Object_script_37_1450251_r.java com/tns/gen/java/lang/Object_script_37_1380753_r.java com/tns/gen/java/lang/Object_script_37_1462543_r.java com/tns/gen/java/lang/Object_script_37_858187_r.java com/tns/gen/java/lang/Object_script_37_1429433_r.java com/tns/gen/java/lang/Object_script_37_1404957_r.

ISSUE	SEVERITY	STANDARDS	FILES
			java com/tns/gen/java/lang/Object_script_37_1458758_r.java com/tns/gen/java/lang/Object_script_37_1495805_r.java com/tns/gen/java/lang/Object_script_37_1231168_r.java com/tns/gen/java/lang/Runnable.java com/tns/gen/java/lang/Object_script_37_1490318_r.java com/tns/gen/android/webkit/WebViewClient_script_37_1485550_r.java com/tns/gen/android/hardware/Camera_PreviewCallback.java com/tns/gen/android/app/Application_ActivityLifecycleCallbacks.java com/tns/gen/android/app/Dialog_script_37_619566_r.java com/tns/gen/android/app/DatePickerDialog_OnDateSetListener.java com/tns/gen/android/app/TimePickerDialog_OnTimeSetListener.java com/tns/gen/android/widget/BaseAdapter_script_37_2465843_r.java com/tns/gen/android/widget/Spinner_script_37_2464692_r.java com/tns/gen/android/widget/TabHost_script_37_1245450_r.java com/tns/gen/android/widget/BaseAdapter_script_37_1496216_r.java com/tns/gen/android/animation/Animator_AnimatorListener.java com/tns/gen/android/animation/ValueAnimator_AnimatorUpdateListener.java com/tns/gen/android/view/ViewTreeObserver_OnGlobalLayoutListener.java com/tns/gen/android/view/View_OnClickListener.java com/tns/gen/android/view/Choreographer_FrameCallback.java com/tns/gen/android/view/GestureDetector_SimpleOnGestureListener_script_37_1333360_r.java com/tns/gen/android/view/View_OnLayoutChangeListener.java com/tns/gen/android/view/ViewTreeObserver_OnScrollChangedListener.java com/tns/gen/android/view/ScaleGestureDetector_SimpleOnScaleGestureListener_script_37_1334788_r.java com/tns/gen/android/view/GestureDetector_SimpleOnGestureListener_script_37_1335657_r.java com/tns/gen/com/jesusm/kfingerprintmanager/KFingerprintManager_AuthenticationCallback.java com/tns/bindings/desc/reflection/ClassInfo.java
MD5 is a weak hash known to have hash collisions.	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-4	org/nativescript/widgets/image/Cache.java

ISSUE	SEVERITY	STANDARDS	FILES
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	org/nativescript/widgets/image/Cache.java
SHA-1 is a weak hash known to have hash collisions.	high	**CVSS V2:** 5.9 (medium) **CWE:** CWE-327 - Use of a Broken or Risky Cryptographic Algorithm **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-4	org/ow2/asmdex/ApplicationWriter.java fi/iki/elonen/NanoWSD.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	fi/iki/elonen/NanoWSD.java com/tns/AppConfig.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	fi/iki/elonen/NanoHTTPD.java
App creates temp file. Sensitive information should never be written into a temp file.	high	**CVSS V2:** 5.5 (medium) **CWE:** CWE-276 - Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2	fi/iki/elonen/NanoHTTPD.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/tns/binding/tests/Dummy.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
bolivia-segura.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
file:///	org/nativescript/widgets/image/Fetcher.java
file:///	org/nativescript/widgets/image/Worker.java
https://bolivia-segura.firebaseio.com	Android String Resource

FIREBASE DATABASES

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

TRACKERS

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

PLAYSTORE INFORMATION

Title: Bolivia Segura

Score: 2.73 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** 4.2 and up **Category:** Health & Fitness **Play Store URL:** com.agetic.coronavirusapp

Developer Details: Agetic Bolivia, Agetic+Bolivia, None, https://boliviasegura.gob.bo, contacto@agetic.gob.bo,

Release Date: Mar 12, 2020 **Privacy Policy:** Privacy link

Description:

Toda la información oficial acerca del Coronavirus(COVID-19) en Bolivia: - Prevenciones y cuidados - Síntomas - Preguntas frecuentes - Números de Emergencia - Datos Oficiales - Comunicados Oficiales - Últimas Noticias #QuédateEnCasa

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.