ANDROID STATIC ANALYSIS REPORT

Coronavirus UY (2.2.3)

File Name:	Coronavirus UY 2.2.3.apk
Package Name:	uy.gub.salud.plancovid19uy
Average CVSS Score:	6.4
App Security Score:	10/100 (CRITICAL RISK)
Trackers Detection:	3/285

FILE INFORMATION

File Name: Coronavirus UY 2.2.3.apk
Size: 22.22MB
MD5: 913417476abf54a7a673ee7786f775b3
SHA1: 2fb111dba2532d7d48a24480ff8183ed30d589bc
SHA256: f6b10931e1bb031a44531f320e398889573eaabf77b07ca26943ec540ff34b88

APP INFORMATION

App Name: Coronavirus UY
Package Name: uy.gub.salud.plancovid19uy
Main Activity: com.artech.activities.StartupActivity
Target SDK: 29
Min SDK: 19
Max SDK:
Android Version Name: 2.2.3
Android Version Code: 223

APP COMPONENTS

Activities: 16
Services: 16
Receivers: 10
Providers: 5
Exported Activities: 0
Exported Services: 1
Exported Receivers: 5
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=uy, ST=Montevideo, L=Montevideo, O=GUB UY, OU=MSP, CN=MSP GUB UY
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-03-17 13:03:10+00:00
Valid To: 2047-08-03 13:03:10+00:00
Issuer: C=uy, ST=Montevideo, L=Montevideo, O=GUB UY, OU=MSP, CN=MSP GUB UY
Serial Number: 0x18e60d1f
Hash Algorithm: sha256
md5: 6ffcf8ff7c26da4fd6332bb39a99fc5e
sha1: 44e5103e3faee7fc70a01542328229f19eb4667e
sha256: 65e21c8d72f9a39662a858cafd8a6b60879452443264097afaf2eca7c18c8063
sha512:
1631864365e10379099474a93169497ebe313907d093207d2150d60243d91857e4c10b96f997edcbc1cde96d445916385a7d4bcf5d8ab1e0673adf10dfa33466

PublicKey Algorithm: rsa
Bit Size: 2048

Fingerprint: 458de87d12253a6a9ac25309e6ab5967d28ff9bed212c0e007c392b6e1e22950

Certificate Status: Good
Description: Certificate looks good.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background. If you're requesting this permission, you must also request either
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.
uy.gub.salud.plancovid19uy.permission.C2D_MESSAGE	signature	Allows cloud to device messaging	Allows the application to receive push notifications.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground
android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.MODIFY_AUDIO_SETTINGS	dangerous	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read SD card contents	Allows an application to read from SD Card.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
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.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete SD card contents	Allows an application to write to the SD card.
android.permission.CHANGE_NETWORK_STATE	dangerous	change network connectivity	Allows an application to change the state of network connectivity.
com.google.android.providers.gsf.permission.READ_GSERVICES	dangerous	Unknown permission from android reference	Unknown permission from android reference
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	dangerous	Unknown permission from android reference	Unknown permission from android reference
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.

PERMISSION	STATUS	INFO	DESCRIPTION
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
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

PERMISSION	STATUS	INFO	DESCRIPTION
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

<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
Build.HARDWARE 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>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.HARDWARE check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION

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.
Broadcast Receiver (com.genexus.coreexternalobjects.geolocation.fused.LocationFusedProviderReceiver) is not Protected. [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.
Launch Mode of Activity (com.artech.android.gam.AuthManagementActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
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.
Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [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.
Broadcast Receiver (com.onesignal.BootUpReceiver) 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.

ISSUE	SEVERITY	DESCRIPTION
Broadcast Receiver (com.onesignal.UpgradeReceiver) 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.
Service (com.sinch.android.rtc.internal.client.fcm.InstanceIDTokenService) 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.
High Intent Priority (999) [android:priority]	medium	By setting an intent priority higher than another intent, the app effectively overrides other requests.

CODE ANALYSIS

ISSUE	SEVERITY	STANDARDS	FILES
			HTTPClient/b.java HTTPClient/n.java HTTPClient/j0.java HTTPClient/k.java HTTPClient/r0.java HTTPClient/i0.java HTTPClient/t0.java org/webrtc/CameraEnumerationAndroid.java org/webrtc/HardwareVideoEncoder.java org/webrtc/MediaConstraints.java org/simpleframework/xml/core/f1.java org/simpleframework/xml/core/t1.java i/a/a/a/w/b.java i/a/a/a/w/h.java i/a/a/a/w/i.java i/b/a/c/b.java i/b/a/d/f.java i/b/a/d/i/a.java i/b/a/d/h/b.java i/b/a/d/h/c.java i/b/a/d/h/d.java i/b/a/b/e.java g/v.java g/e0.java g/f0.java g/g.java g/r.java g/l.java g/a.java g/t.java g/g0/i/a.java g/g0/k/b.java g/g0/k/a.java f/b/a/c.java d/a/d0/f.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	d/a/c0/d.java d/a/n/a.java d/a/s/d.java d/a/o/i/t.java d/a/o/d/u.java d/a/o/d/b1/n.java d/a/m/v/b.java d/a/x/b.java d/a/p/w.java d/a/p/f.java d/d/a/a/b.java d/d/a/a/a.java d/d/a/a/i/b.java d/d/a/a/i/c.java d/d/a/a/i/g.java d/d/a/a/i/a.java d/d/a/a/i/u/j/b.java d/d/a/b/l/h.java d/d/a/b/l/i.java com/onesignal/u1.java com/genexus/coreexternalobjects/PhotoLibraryAPI.java com/genexus/coreusercontrols/matrixgrid/a.java com/genexus/controls/maps/googlev2/l.java com/genexus/b1/b.java com/genexus/db/a0/d.java com/genexus/db/a0/e.java com/genexus/db/a0/a.java com/genexus/a1/c/c.java com/genexus/a1/b/c.java com/artech/controls/g0.java com/artech/controls/d.java com/artech/controls/q1/c.java com/artech/controls/grids/d.java com/artech/controls/r1/b.java com/artech/controls/r1/c.java com/artech/android/layout/o.java com/artech/base/metadata/expressions/f0.java com/sinch/gson/JsonArray.java com/sinch/gson/JsonNull.java com/sinch/gson/JsonObject.java com/sinch/gson/JsonPrimitive.java com/sinch/gson/reflect/TypeToken.java com/sinch/gson/internal/LinkedTreeMap.java com/sinch/gson/internal/LazilyParsedNumber.java com/sinch/gson/internal/C$Gson$Types.java com/sinch/gson/internal/LinkedHashTreeMap.java com/sinch/android/rtc/internal/service/pubnub/Subscription.java com/sinch/android/rtc/internal/natives/PubSubChannel.java com/sinch/android/rtc/internal/natives/jni/NativePubSubscriber.java com/sinch/android/rtc/internal/client/calling/PeerConnection/PeerConnectionUtils.java com/sinch/android/rtc/internal/client/calling/PeerConnection/StatsCollector.java com/dvelop/videoconf/h.java b/r/j0.java b/r/s.java b/r/k0.java b/g/l/b0.java b/g/l/c0/a.java

ISSUE	SEVERITY	STANDARDS	FILES
			b/g/i/c0/c.java b/g/i/c0/d.java b/e/b.java b/e/f.java b/e/g.java b/b/a/b/b.java
			HTTPClient/a0.java HTTPClient/o0.java org/sqldroid/c.java org/webrtc/sinch/AudioDeviceUtil.java c/a/m/b.java d/a/o/c/a.java d/a/p/a0.java d/d/a/a/i/s/a.java d/d/a/b/m/a.java d/d/a/b/v/d.java d/d/a/b/l/h.java d/e/a/b.java d/e/a/a.java com/squareup/picasso/e0.java com/onesignal/g1.java com/onesignal/JobIntentService.java com/onesignal/g.java com/onesignal/shortcutbadger/b.java com/genexus/b.java com/genexus/c0.java com/genexus/e.java com/genexus/q0.java com/genexus/u0.java com/genexus/i0.java com/genexus/p0.java com/genexus/a.java com/genexus/g1/a/k.java com/genexus/g1/a/a.java com/genexus/util/Encryption.java com/genexus/util/r.java com/genexus/j1/m.java com/genexus/db/w.java com/genexus/db/v.java com/genexus/db/h.java com/genexus/db/f.java com/genexus/db/a0/h.java com/genexus/e1/b.java com/sinch/httpclient/HttpClient.java com/sinch/android/rtc/SinchHelpers.java com/sinch/android/rtc/internal/service/pubnub/PubNubPublisher.java com/sinch/android/rtc/internal/service/pubnub/PubNubListener.java com/sinch/android/rtc/internal/service/http/DefaultHttpService.java com/sinch/android/rtc/internal/service/http/HttpClientDefaults.java com/sinch/android/rtc/internal/natives/jni/NativeProxy.java com/sinch/android/rtc/internal/natives/jni/CallQualitySettings.java com/sinch/android/rtc/internal/natives/jni/Session.java com/sinch/android/rtc/internal/client/DefaultAudioController.java com/sinch/android/rtc/internal/client/DefaultSinchClient.java com/sinch/android/rtc/internal/client/SinchDBPathHelper.java

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	com/sinch/android/rtc/internal/client/DefaultManagedPush.java com/sinch/android/rtc/internal/client/video/ProxyVideoSink.java com/sinch/android/rtc/internal/client/calling/JsepMessage.java com/sinch/android/rtc/internal/client/calling/PeerConnection/PeerConnectionUtils.java com/sinch/android/rtc/internal/client/calling/PeerConnection/PeerConnectionInstance.java com/sinch/android/rtc/internal/client/calling/PeerConnection/DefaultPeerConnectionClient.java com/sinch/android/rtc/internal/client/calling/PeerConnection/PeerConnectionObserver.java com/sinch/android/rtc/internal/client/calling/PeerConnection/StatsCollector.java com/sinch/android/rtc/internal/client/calling/PeerConnection/SDPObserver.java com/sinch/android/rtc/internal/client/calling/PeerConnection/ConnectionObserver.java com/sinch/android/rtc/internal/client/calling/PeerConnection/SdpUtils.java com/sinch/android/rtc/internal/client/calling/PeerConnection/DefaultPeerConnectionFactoryWrapper.java com/sinch/android/rtc/internal/client/fcm/FcmTask.java com/sinch/android/rtc/internal/client/fcm/PersistedToken.java com/sinch/android/rtc/internal/client/fcm/InstanceIDTokenService.java com/sinch/android/rtc/internal/client/fcm/TokenRefreshTask.java com/sinch/android/rtc/internal/client/libloader/NativeLibLoader.java com/sinch/android/rtc/internal/client/libloader/ReLinkerLibraryLoader.java com/sinch/android/rtc/audio/WebRtcProximitySensor.java com/sinch/android/rtc/audio/AudioManagerInternal.java com/sinch/android/rtc/audio/BluetoothManager.java com/dvelop/videoconf/h.java b/r/z.java b/r/g0.java b/r/e0.java b/r/d0.java b/r/f0.java b/r/y.java b/i/b/a.java b/n/a/a.java b/g/j/a.java b/g/e/b.java b/g/e/h.java b/g/e/d.java b/g/e/e.java b/g/e/i.java b/g/e/f.java b/g/k/b.java b/g/l/b.java b/g/l/w.java b/g/l/e.java b/g/l/g.java b/g/l/u.java

ISSUE	SEVERITY	STANDARDS	FILES
			b/g/l/t.java b/g/t0/d.java b/t/a/b.java b/s/a/a/i.java b/a/o/g.java b/a/k/a/a.java b/o/b.java b/o/a.java b/m/a/b.java b/j/a/a.java b/q/a/c.java b/l/a/a.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	HTTPClient/e0.java HTTPClient/d0.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	org/sqldroid/m.java d/a/x/f.java d/d/a/a/i/u/j/z.java d/d/a/a/i/u/j/e0.java d/d/a/a/i/u/j/d0.java com/onesignal/m1.java com/genexus/coreexternalobjects/r1/g/b.java com/genexus/coreexternalobjects/r1/g/d.java com/artech/android/notification/a.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	i/a/a/a/w/b.java d/a/m/f.java com/genexus/h.java com/genexus/u0.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	d/a/m/t/a.java d/a/m/v/b.java d/a/p/q0.java com/sinch/android/rtc/internal/client/calling/PeerConnection/PeerConnectionUtils.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	d/a/p/w.java d/a/p/q0.java com/genexus/coreexternalobjects/ActionsAPI.java b/o/b.java
Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-295 - Improper Certificate Validation **OWASP Top 10:** M3: Insecure Communication **OWASP MASVS:** MSTG-NETWORK-3	d/a/p/t0.java
Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	**CVSS V2:** 8.8 (high) **CWE:** CWE-749 - Exposed Dangerous Method or Function **OWASP Top 10:** M1: Improper Platform Usage **OWASP MASVS:** MSTG-PLATFORM-7	com/onesignal/r2.java

ISSUE	SEVERITY	STANDARDS	FILES
Remote WebView debugging is enabled.	high	**CVSS V2:** 5.4 (medium) **CWE:** CWE-919 - Weaknesses in Mobile Applications **OWASP Top 10:** M1: Improper Platform Usage **OWASP MASVS:** MSTG-RESILIENCE-2	com/onesignal/r2.java
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	com/genexus/coreexternalobjects/ClipboardAPI.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	com/sinch/android/rtc/internal/service/crypto/DefaultCryptoService.java com/sinch/android/rtc/internal/client/Sha1Utils.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/sinch/android/rtc/internal/client/fcm/PersistedToken.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
java.sun.com	good	**IP:** 156.151.59.19 **Country:** United States of America **Region:** California **City:** Belmont **Latitude:** 37.53244 **Longitude:** -122.248833 **View:** Google Map
apache.org	good	**IP:** 95.216.24.32 **Country:** Finland **Region:** Uusimaa **City:** Helsinki **Latitude:** 60.169521 **Longitude:** 24.93545 **View:** Google Map
xml.org	good	**IP:** 104.239.240.11 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
onesignal.com	good	**IP:** 104.18.225.52 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.7757 **Longitude:** -122.395203 **View:** Google Map
www.w3.org	good	**IP:** 128.30.52.100 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.365078 **Longitude:** -71.104523 **View:** Google Map
xmlpull.org	good	**IP:** 74.50.62.60 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.814899 **Longitude:** -96.879204 **View:** Google Map
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
coronavirus-app-bf0e2.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
github.com	good	**IP:** 13.236.229.21 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map
servicios.coronavirus.gub.uy	good	**IP:** 190.64.214.37 **Country:** Uruguay **Region:** Montevideo **City:** Montevideo **Latitude:** -34.833462 **Longitude:** -56.167351 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.genexus.com	good	**IP:** 54.85.65.168 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.04372 **Longitude:** -77.487488 **View:** Google Map
www.youtube.com	good	**IP:** 172.217.167.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

URLS

URL	FILE
http://xmlpull.org/v1/doc/features.html#process-docdecl http://xmlpull.org/v1/doc/features.html#process-namespaces http://xmlpull.org/v1/doc/features.html#report-namespace-prefixes http://xmlpull.org/v1/doc/features.html#validation	org/xmlpull/v1/XmlPullParser.java
http://www.w3.org/2001/XMLSchema-instance	org/xmlpull/v1/util/XmlPullUtil.java
http://www.w3.org/2001/XMLSchema-instance	org/xmlpull/v1/wrapper/XmlSerializerWrapper.java
http://www.w3.org/2001/XMLSchema-instance	org/xmlpull/v1/wrapper/XmlPullParserWrapper.java
http://xmlpull.org/v1/doc/features.html#xmldecl-standalone http://www.w3.org/2001/XMLSchema-instance	org/xmlpull/v1/wrapper/classic/StaticXmlSerializerWrapper.java
http://www.w3.org/2001/XMLSchema-instance	org/xmlpull/v1/wrapper/classic/StaticXmlPullParserWrapper.java
http://apache.org/xml/features/validation/dynamic http://apache.org/xml/features/validation/schema http://xml.org/sax/properties/declaration-handler http://xml.org/sax/properties/lexical-handler http://xml.org/sax/features/namespaces http://xml.org/sax/features/namespace-prefixes http://xml.org/sax/features/validation	org/xmlpull/v1/sax2/Driver.java
http://xmlpull.org/v1/doc/properties.html#xmldecl-standalone http://xmlpull.org/v1/doc/properties.html#xmldecl-version	org/xmlpull/v1/builder/impl/XmlPullBuilderImpl.java
http://www.w3.org/xmlns/2000/ http://www.w3.org/XML/1998/namespace	org/xml/sax/m/d.java

URL	FILE
http://www.w3.org/XML/1998/namespace http://xml.org/sax/features/namespaces http://xml.org/sax/features/namespace-prefixes http://xml.org/sax/features/xmlns-uris	org/xml/sax/m/f.java
http://xml.org/sax/features/validation http://xml.org/sax/features/external-general-entities http://xml.org/sax/features/external-parameter-entities http://apache.org/xml/features/allow-java-encodings http://apache.org/xml/features/warn-on-duplicate-entitydef http://apache.org/xml/features/standard-uri-conformant http://apache.org/xml/properties/internal/symbol-table http://apache.org/xml/properties/internal/error-reporter http://apache.org/xml/properties/internal/entity-resolver http://apache.org/xml/properties/internal/validation-manager http://apache.org/xml/properties/input-buffer-size http://apache.org/xml/properties/security-manager http://www.w3.org/TR/1998/REC-xml-19980210 file:/// http://apache.org/xml/features/internal/parser-settings http://apache.org/xml/features/ http://apache.org/xml/properties/	i/a/a/a/n.java
http://www.w3.org/TR/1998/REC-xml-19980210 http://apache.org/xml/properties/internal/symbol-table http://apache.org/xml/properties/internal/error-reporter http://apache.org/xml/properties/internal/entity-manager	i/a/a/a/v.java
http://xml.org/sax/features/validation http://apache.org/xml/features/scanner/notify-char-refs http://apache.org/xml/properties/internal/symbol-table http://apache.org/xml/properties/internal/error-reporter http://apache.org/xml/properties/internal/entity-manager http://www.w3.org/TR/1998/REC-xml-19980210	i/a/a/a/h.java
http://www.w3.org/TR/1998/REC-xml-19980210	i/a/a/a/p.java
http://www.w3.org/TR/1998/REC-xml-19980210	i/a/a/a/e.java
http://xml.org/sax/features/namespaces http://xml.org/sax/features/validation http://apache.org/xml/features/scanner/notify-builtin-refs http://apache.org/xml/features/scanner/notify-char-refs http://apache.org/xml/properties/internal/symbol-table http://apache.org/xml/properties/internal/error-reporter http://apache.org/xml/properties/internal/entity-manager http://apache.org/xml/properties/internal/entity-resolver http://www.w3.org/TR/1998/REC-xml-19980210 http://apache.org/xml/features/ http://apache.org/xml/properties/	i/a/a/a/i.java
http://apache.org/xml/features/nonvalidating/load-external-dtd http://apache.org/xml/features/disallow-doctype-decl http://apache.org/xml/properties/internal/dtd-scanner http://apache.org/xml/properties/internal/validation-manager http://apache.org/xml/properties/internal/namespace-context http://www.w3.org/TR/1998/REC-xml-19980210 http://apache.org/xml/features/ http://apache.org/xml/properties/	i/a/a/a/j.java

URL	FILE
http://www.w3.org/TR/1999/REC-xml-names-19990114 http://www.w3.org/TR/1998/REC-xml-19980210	i/a/a/a/s.java
http://www.w3.org/TR/1998/REC-xml-19980210	i/a/a/a/f.java
http://www.w3.org/TR/1999/REC-xml-names-19990114 http://www.w3.org/TR/1998/REC-xml-19980210	i/a/a/a/g.java
http://apache.org/xml/features/continue-after-fatal-error http://apache.org/xml/properties/internal/error-handler http://apache.org/xml/features/ http://apache.org/xml/properties/	i/a/a/a/r.java
http://www.w3.org/TR/1998/REC-xml-19980210 http://apache.org/xml/features/internal/parser-settings http://apache.org/xml/properties/internal/symbol-table http://apache.org/xml/properties/internal/error-reporter http://apache.org/xml/properties/internal/entity-manager http://xml.org/sax/features/validation http://xml.org/sax/features/namespaces http://apache.org/xml/features/scanner/notify-char-refs http://apache.org/xml/properties/	i/a/a/a/u.java
http://www.w3.org/2001/XMLSchema http://www.w3.org/TR/REC-xml http://www.w3.org/XML/XMLSchema/v1.0	i/a/a/a/a.java
http://xml.org/sax/features/namespaces http://apache.org/xml/properties/internal/symbol-table http://apache.org/xml/properties/internal/error-reporter http://www.w3.org/TR/1999/REC-xml-names-19990114 http://apache.org/xml/properties/	i/a/a/a/t.java
http://www.w3.org/TR/1999/REC-xml-names-19990114	i/a/a/a/w/p.java
http://apache.org/xml/properties/internal/validator/dtd	i/a/a/a/w/e.java
http://www.w3.org/TR/REC-xml	i/a/a/a/w/i.java
http://xml.org/sax/features/validation http://apache.org/xml/features/validation/warn-on-duplicate-attdef http://apache.org/xml/features/validation/warn-on-undeclared-elemdef http://apache.org/xml/features/scanner/notify-char-refs http://apache.org/xml/features/standard-uri-conformant http://apache.org/xml/features/validation/balance-syntax-trees http://apache.org/xml/properties/internal/symbol-table http://apache.org/xml/properties/internal/error-reporter http://apache.org/xml/properties/internal/error-handler http://apache.org/xml/properties/internal/entity-resolver http://apache.org/xml/properties/internal/grammar-pool http://apache.org/xml/properties/internal/validator/dtd http://apache.org/xml/properties/locale http://www.w3.org/TR/1998/REC-xml-19980210 http://www.w3.org/TR/1999/REC-xml-names-19990114	i/a/a/a/w/j.java
http://www.w3.org/TR/1999/REC-xml-names-19990114	i/a/a/a/w/f.java

URL	FILE
http://xml.org/sax/features/validation http://apache.org/xml/features/validation/warn-on-duplicate-attdef http://apache.org/xml/features/validation/warn-on-undeclared-elemdef http://apache.org/xml/features/scanner/notify-char-refs http://apache.org/xml/properties/internal/symbol-table http://apache.org/xml/properties/internal/error-reporter http://apache.org/xml/properties/internal/grammar-pool http://apache.org/xml/properties/internal/validator/dtd http://www.w3.org/TR/1998/REC-xml-19980210 http://apache.org/xml/features/internal/parser-settings http://apache.org/xml/features/validation/schema http://www.w3.org/TR/REC-xml	i/a/a/a/w/k.java
http://xml.org/sax/features/namespaces http://xml.org/sax/features/validation http://apache.org/xml/features/validation/dynamic http://apache.org/xml/features/validation/balance-syntax-trees http://apache.org/xml/properties/internal/symbol-table http://apache.org/xml/properties/internal/error-reporter http://apache.org/xml/properties/internal/grammar-pool http://apache.org/xml/properties/internal/datatype-validator-factory http://apache.org/xml/properties/internal/validation-manager http://www.w3.org/TR/1998/REC-xml-19980210 http://www.w3.org/TR/REC-xml http://apache.org/xml/features/internal/parser-settings http://apache.org/xml/features/validation/schema http://apache.org/xml/features/validation/warn-on-duplicate-attdef http://java.sun.com/xml/jaxp/properties/schemaLanguage	i/a/a/a/w/l.java
http://apache.org/xml/features/internal/parser-settings http://xml.org/sax/features/validation http://xml.org/sax/features/namespaces http://xml.org/sax/features/external-general-entities http://xml.org/sax/features/external-parameter-entities http://xml.org/sax/properties/xml-string http://apache.org/xml/properties/internal/symbol-table http://apache.org/xml/properties/internal/error-handler http://apache.org/xml/properties/internal/entity-resolver http://apache.org/xml/features/ http://xml.org/sax/properties/	i/a/a/c/c.java

URL	FILE
http://apache.org/xml/features/continue-after-fatal-error http://apache.org/xml/features/nonvalidating/load-external-dtd http://apache.org/xml/properties/internal/error-reporter http://apache.org/xml/properties/internal/entity-manager http://apache.org/xml/properties/internal/document-scanner http://apache.org/xml/properties/internal/dtd-scanner http://apache.org/xml/properties/internal/dtd-processor http://apache.org/xml/properties/internal/validator/dtd http://apache.org/xml/properties/internal/namespace-binder http://apache.org/xml/properties/internal/grammar-pool http://apache.org/xml/properties/internal/datatype-validator-factory http://apache.org/xml/properties/internal/validation-manager http://java.sun.com/xml/jaxp/properties/schemaSource http://java.sun.com/xml/jaxp/properties/schemaLanguage http://apache.org/xml/properties/locale http://www.w3.org/TR/1998/REC-xml-19980210 http://www.w3.org/TR/1999/REC-xml-names-19990114 http://apache.org/xml/features/ http://apache.org/xml/properties/ http://xml.org/sax/features/namespaces	i/a/a/c/d.java
http://apache.org/xml/features/validation/schema/normalized-value http://apache.org/xml/features/validation/schema/element-default http://apache.org/xml/features/validation/schema/augment-psvi http://apache.org/xml/features/generate-synthetic-annotations http://apache.org/xml/features/validate-annotations http://apache.org/xml/features/honour-all-schemaLocations http://apache.org/xml/features/namespace-growth http://apache.org/xml/features/internal/tolerate-duplicates http://apache.org/xml/features/validation/schema http://apache.org/xml/features/validation/schema-full-checking http://apache.org/xml/features/validation/schema/ignore-xsi-type-until-elemdecl http://apache.org/xml/features/validation/id-idref-checking http://apache.org/xml/features/validation/identity-constraint-checking http://apache.org/xml/features/validation/unparsed-entity-checking http://apache.org/xml/properties/schema/external-schemaLocation http://apache.org/xml/properties/schema/external-noNamespaceSchemaLocation http://apache.org/xml/properties/validation/schema/root-type-definition http://apache.org/xml/properties/validation/schema/root-element-declaration http://apache.org/xml/properties/internal/validation/schema/dv-factory http://apache.org/xml/features/ http://apache.org/xml/properties/ http://java.sun.com/xml/jaxp/properties/ http://apache.org/xml/properties/internal/validator/schema http://www.w3.org/TR/xml-schema-1	i/a/a/c/p.java
http://apache.org/xml/properties/internal/entity-resolver http://apache.org/xml/properties/internal/error-handler	i/a/a/c/s.java
http://apache.org/xml/features/scanner/notify-builtin-refs http://apache.org/xml/properties/internal/symbol-table http://apache.org/xml/properties/internal/grammar-pool	i/a/a/c/f.java

URL	FILE
http://apache.org/xml/features/continue-after-fatal-error http://apache.org/xml/features/nonvalidating/load-external-dtd http://xml.org/sax/features/validation http://xml.org/sax/features/namespaces http://apache.org/xml/features/validation/schema/normalized-value http://apache.org/xml/features/validation/schema/element-default http://apache.org/xml/features/validation/schema/augment-psvi http://apache.org/xml/features/generate-synthetic-annotations http://apache.org/xml/features/validate-annotations http://apache.org/xml/features/honour-all-schemaLocations http://apache.org/xml/features/namespace-growth http://apache.org/xml/features/internal/tolerate-duplicates http://apache.org/xml/features/validation/schema/ignore-xsi-type-until-elemdecl http://apache.org/xml/features/validation/id-idref-checking http://apache.org/xml/features/validation/identity-constraint-checking http://apache.org/xml/features/validation/unparsed-entity-checking http://apache.org/xml/features/internal/validation/schema/use-grammar-pool-only http://apache.org/xml/features/validation/schema http://apache.org/xml/features/validation/schema-full-checking http://xml.org/sax/features/external-general-entities http://xml.org/sax/features/external-parameter-entities http://apache.org/xml/features/internal/parser-settings http://apache.org/xml/properties/internal/symbol-table http://apache.org/xml/properties/internal/error-handler http://apache.org/xml/properties/internal/entity-resolver http://apache.org/xml/properties/internal/error-reporter http://apache.org/xml/properties/internal/entity-manager http://apache.org/xml/properties/internal/document-scanner http://apache.org/xml/properties/internal/dtd-scanner http://apache.org/xml/properties/internal/dtd-processor http://apache.org/xml/properties/internal/validator/dtd http://apache.org/xml/properties/internal/datatype-validator-factory http://apache.org/xml/properties/internal/validation-manager http://apache.org/xml/properties/internal/validator/schema http://xml.org/sax/properties/xml-string http://apache.org/xml/properties/internal/grammar-pool http://java.sun.com/xml/jaxp/properties/schemaSource http://java.sun.com/xml/jaxp/properties/schemaLanguage http://apache.org/xml/properties/schema/external-schemaLocation http://apache.org/xml/properties/schema/external-noNamespaceSchemaLocation http://apache.org/xml/properties/locale http://apache.org/xml/properties/validation/schema/root-type-definition http://apache.org/xml/properties/validation/schema/root-element-declaration http://apache.org/xml/properties/internal/validation/schema/dv-factory http://www.w3.org/TR/1998/REC-xml-19980210 http://www.w3.org/TR/1999/REC-xml-names-19990114 http://apache.org/xml/features/ http://www.w3.org/TR/xml-schema-1 http://apache.org/xml/properties/ http://java.sun.com/xml/jaxp/properties/ http://xml.org/sax/properties/	i/a/a/c/r.java

URL	FILE
http://xml.org/sax/features/namespaces http://xml.org/sax/features/string-interning http://xml.org/sax/properties/lexical-handler http://xml.org/sax/properties/declaration-handler http://xml.org/sax/properties/dom-node http://xml.org/sax/features/allow-dtd-events-after-endDTD http://apache.org/xml/properties/internal/entity-resolver http://xml.org/sax/features/ http://apache.org/xml/properties/internal/error-handler http://xml.org/sax/properties/	i/a/a/c/a.java
https://servicios.coronavirus.gub.uy/appservicesv2/	uy/gub/salud/plancovid19uy/MainApplication.java
file://)	d/a/d0/f.java
data:JSON	com/onesignal/z1.java
https://onesignal.com/android_frame.html	com/onesignal/l1.java
https://onesignal.com/api/v1/	com/onesignal/r1.java
data://	com/genexus/util/h.java
http://xml.org/sax/features/external-general-entities http://xml.org/sax/features/external-parameter-entities http://apache.org/xml/features/disallow-doctype-decl http://apache.org/xml/features/nonvalidating/load-external-dtd	com/genexus/j1/m.java
data://	com/genexus/b1/r/a.java
www.youtube.com file:///android_asset/fonts/	com/artech/controls/o0.java
https://maps.google.com/maps/api/staticmap?markers=%s&zoom=%s&size=%sx%s&sensor=false&maptype=%s&key=%s%s	com/artech/controls/q1/e/a.java
https://www.genexus.com/	com/artech/android/gam/a.java
www.youtube.com	com/artech/activities/WebViewActivity.java
http://www.w3.org/2001/XMLSchema-instance	com/artech/base/synchronization/bc/SdtGxPendingEvent.java
http://www.w3.org/2001/XMLSchema-instance	com/artech/base/synchronization/dps/SdtGxSynchroEventSDT_GxSynchroEventSDTItem.java
https://coronavirus-app-bf0e2.firebaseio.com https://github.com/vinc3m1 https://github.com/vinc3m1/RoundedImageView https://github.com/vinc3m1/RoundedImageView.git	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://coronavirus-app-bf0e2.firebaseio.com	info App talks to a Firebase Database.

✉ EMAILS

EMAIL	FILE
example@example.com	d/a/p/e0.java

TRACKERS

TRACKER	URL
DOV-E	https://reports.exodus-privacy.eu.org/trackers/179
Google Firebase Analytics	https://reports.exodus-privacy.eu.org/trackers/49
OneSignal	https://reports.exodus-privacy.eu.org/trackers/193

▶ PLAYSTORE INFORMATION

Title: Coronavirus UY

Score: 4.19774 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** 4.4 and up **Category:** Health & Fitness **Play Store URL:** uy.gub.salud.plancovid19uy

Developer Details: AGESIC, AGESIC, None, http://coronavirus.uy, atencionalusuario@msp.gub.uy,

Release Date: Mar 20, 2020 **Privacy Policy:** Privacy link

Description:

Esta aplicación le permitirá ingresar sus datos personales y de salud a fin de determinar si es necesario realizarle un análisis por el Coronavirus COVID-19. Luego de registrado podrá hacer seguimiento de su caso y los siguientes pasos que deberá realizar. Aplicación para uso dentro del territorio de la República Oriental del Uruguay.

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

APP SECURITY SCORE	RISK
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.