< KTRL+INFORME >

<K+ LAB>

CoronApp_Colombia application technical analysis - Synthesis report

Bogotá, April 17, 2020

This report is based on research conducted primarily upon versions 1.2.29, 1.2.30, 1.2.31, and 1.2.32 of the CoronApp mobile phone application. During the investigation, new versions were released every 3 or 4 days. Release notes detailing changes made in each version are not available.

A previous version of this report was sent to those government entities involved in the development and implementation of this application, as well as COLCERT (Colombian Computer Emergency Response Team). Several changes were implemented by the corresponding entities, taking into account some of the report's findings. As of the date of this publication, the current version of the application is 1.2.36. Some comments in italics correspond to the changes that have been made since then.

Although they have been corrected, the details of the vulnerabilities that we have found are not published here.

The goal of this exercise is to contribute to an improvement in digital security and privacy.

0. Methodology

In addition to examining the available public information about CoronApp, which appears in the application itself and in the Google Play Store, the following non-intrusive methods were used:

- static analysis of permissions and trackers included in CoronApp's source code using *Exodus Privacy*[1] and *ClassyShark 3xodus*[2];
- static analysis of the app's accessible source code using *Apktool*[3] and analysis of the app's manifest (Android Manifest);
- analysis of the data flows generated and received by the application when installed on a phone running Android 7 using *Wireshark*[4]. Tests include sending data through the registration and health report forms;
- passive traffic analysis using virtual machines and Burp Suite[5]; Burp is a traffic analysis tool that uses an HTTP proxy to allow client-side data packets to be analyzed, including data that goes through an SSL (HTTPS).

Note 1: A deeper analysis has still not been possible to implement using the Burp tool since the last two analyzed versions of the app do not work on virtual machines (apparently they only work on computers with arm64 processors).

Note 2: Before carrying out the analyzes that involved filling out forms, a warning email was sent to several people related with CoronApp's management (working with the Instituto Nacional de Salud -INS-, the Agencia Nacional Digital -AND- and the Ministry of ICT -MINTIC-, see Annex [0]) looking to ensure that they would identify these forms and would not take that information into account in their respective analyzes and the alerts generated by their system.

1 *https://exodus-privacy.eu.org/en/*
2 *https://f-droid.org/en/packages/com.oF2pks.classyshark3xodus/*
3 *https://ibotpeaches.github.io/Apktool/*
4 *https://www.wireshark.org/* To make this capture, we generated a WIFI access point from the computer that was running the WireShark program. The cellphone using the CoronApp application accessed the Internet through this WIFI access point.
5 *https://portswigger.net/*

1. Data collected by the application

The application collects the following data (see screenshots in Annex [1]):

Type of data	Data
Personal data from the registration form	• Name and surname • ID type and number • Cellphone number • Gender • Date of birth • Country, State, City of residence • Email • Password
Sensitive personal data from reporting and registration forms	• Ethnic origin • Health report: I feel fine / I feel sick • Symptoms • Contact with people with symptoms • Medical care received • Previous travel to other countries
Data that may be collected by the application in a “not visible” way	• Phone contacts • Device location (systematically sent by the app[6]) • Nearby WIFI networks • Information available via Bluetooth, particularly about other nearby Bluetooth devices

The last part is related to the broad amount of authorizations requested by the application.

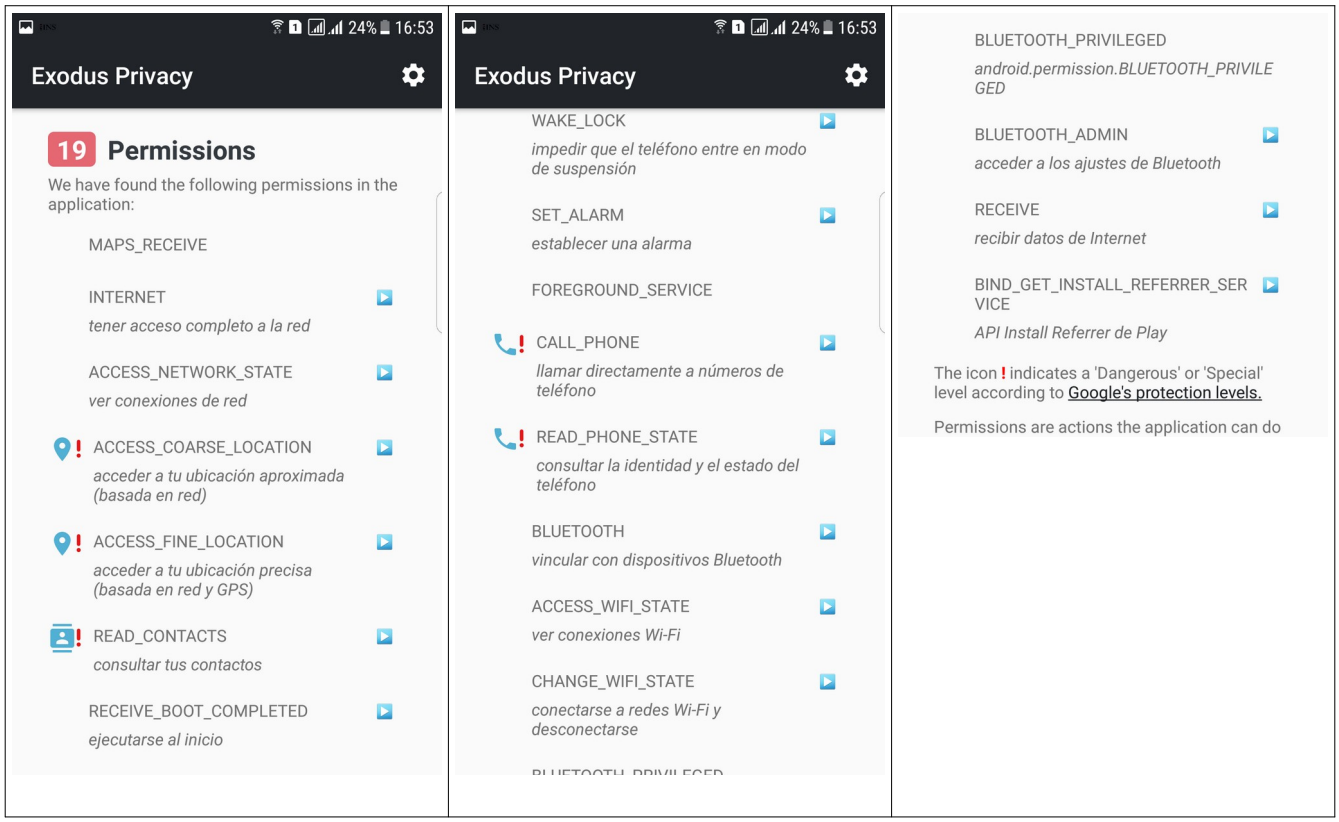
In the latest versions, the data collected by the registration form was reduced to name and surname, ID type and number, phone, and cellphone number.

6 The GPS coordinates appear in the captures made with WireShark.

2. Application permissions and passive data collection

2.1 Application permissions

This application requests a huge amount of permissions[7]. The following is the list that appears when Exodus Privacy is used. These coincide with the application manifest, see annex [2]):



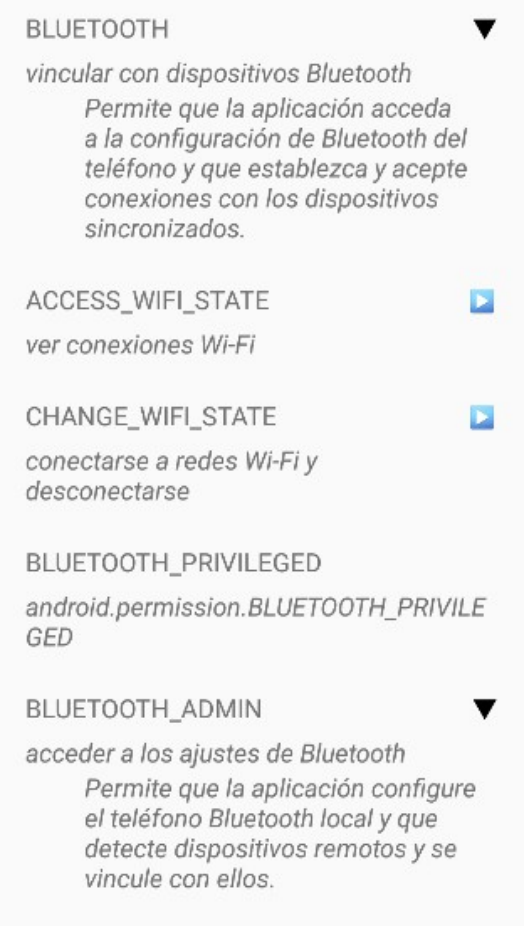
There are several permissions that can be intrusive in terms of privacy:

- Device location access: the analysis of WireShark logs shows that the application regularly sends the GPS coordinates of the device;
- access to contacts;
- access to the information of available WIFI networks detected by the device;
- access to Bluetooth devices that the phone can detect.

7 Most are not explicitly requested to the user during installation or use.

Also, after installing the application, it runs automatically at startup ("RECEIVE_BOOT_COMPLETED" permission).
It is important to note that version 1.2.29 of the application requested 14 permissions. These permissions have been expanded to 19 from version 1.2.30 and are maintained in the following analyzed versions. Three Bluetooth-related permissions are new and we couldn't find an explanation or information about it in the application's documentation.

As shown in the screenshot below, the BLUETOOTH_ADMIN permission can be quite intrusive as it can detect nearby devices (those with Bluetooth function activated).



In the latest version of the app, 16 permissions are requested. Access to phone contacts has been removed. Permissions related to device location, Bluetooth, and nearby WIFI networks remain.

2.2 A curious fact: the inclusion of the HypeLabs library in the latest versions of the application

The inclusion of the software development kit (SDK) called “Hypelabs”[8] is shown in the Android manifest of the application. HypeLabs is a company that develops this type of SDK to give applications the ability to create local “mesh” networks using the communication features available on the phone such as Bluetooth and WiFi. This may be related to the new app permissions we just mentioned.

CoronaApp introduces this SDK in version 1.2.30. The few changes introduced in version 1.2.31 are related to this same library. This change raises questions since in the published documentation of this application a feature that requires this functionality is never mentioned. However, this library can allow someone to deduce the relative location of a person compared with another, in combination with the use of personal data collected by the application. The ethical and legal conclusions of this type of surveillance should be reviewed if this hypothesis were to be confirmed.

It is important to note that it has not been concluded that this is the use that will be given to the capabilities of this library. In fact, the application was not making use of this library until the latest version.

Further analysis is necessary to produce a conclusive answer to this issue.

Regarding the mentioned permissions as well as the inclusion of this library, the National Digital Agency answered the following:

"*The application's request for geolocation, WiFi and Bluetooth networks permissions, as well as the processing of said data, is necessary to identify the location of users and any close contact they may have with people around them since this will allow locating citizens with potential symptoms, possible sources, and chains of COVID-19 contagion, allowing the National Institute of Health to collect the necessary and timely information to act diligently in the face of the great risks of spread identified in the population.”*

8 https://hypelabs.io/

3. Application's data transfer security

3.1 An unsafe data transfer up to version 1.2.31

Until version 1.2.31, after analyzing the data-flow generated by the application from the phone (Wireshark) or from an emulation environment (Burp) showed that personal registration data was transferred without security nor encryption, using the HTTP[9] protocol. Data were transferred to a dedicated subdomain of the Government's National Digital Agency ("apicovid.and.gov.co"), hosted on an server of Amazon Web Service located in the State of Washington[10] (see Annex [3]). This web server is a Nginx server version 1.17.9 (latest version).

The analysis also shows that the GPS coordinates of the device are regularly sent to this same server using the same protocol.

Regarding the transfer of health data (reports), data packets were not possible to identify with certainty because the information is encoded since these fields were checkboxes. However, since when transferring this data the application communicated only using the HTTP protocol (towards a server with the same IP address), it can be deduced - almost certainly - that this data transfer was not secure either.

As of version 1.2.32 (from March 31) the use of the HTTP protocol was replaced by the secure HTTPS protocol (HTTP encapsulated in the SSL / TLS encrypted protocol). A new subdomain was created ("apicovid2.and.gov.co") and linked with a new web server[11], with which the application currently communicates.

This is a major improvement in terms of the application's security as data is now transferred using an encrypted channel.

However, this vulnerability persists on the devices of people who have not updated the application since the old server is still active and data continues to be transferred to it in an unsafe manner. In addition, complementary analyzes conducted by the NGO Access Now showed that the new server continued to respond to HTTP requests with the same HTTP protocol.

This issue was corrected and in the latest versions the possibility for the application to communicate with the server using the HTTP protocol has definitively been removed.

---

9 HyperText Transfer Protocol. The transfer is done using an unconventional port (5000) but this does not change the lack of protocol security.

10 The web server has the IP address: 52.87.234.39.

11 The new server has the IP address: 34.199.57.23. It is also hosted by Amazon.

3.2 A Serious Vulnerability issue in the Application's Authentication method

[Although the vulnerability issue mentioned in this section has been apparently fixed, we have removed some details in order not to facilitate attacks. The goal of this exercise is to contribute to an improvement in digital security and privacy.]

This vulnerability involves an authentication flaw that could allow an attacker to access personal data of users registered in the application's backend server (with which the application communicates).

The backend server used by Coronapp_colombia does not exert sufficient access control to resources that should be restricted for each user, allowing an attacker to have the ability to access user resources without the need for any authentication. This vulnerability could lead to a possible listing of huge amounts of sensitive data from users registered in the application.

In a package review done in the application flow, it was found that some packages that should include an authentication token do not include it, and yet the API sends responses that correspond to actions that should normally carry authentication.

This issue is found in the server that had been used until version 1.2.31 of the application (server using HTTP without SSL / TLS, domain "apicovid.and.gov.co" and IP address: 52.87.234.39 ”) and that had apparently been replaced in version 1.2.32 as mentioned (server using HTTP with SSL / TLS, domain "apicovid2.and.gov.co" and IP address: 34.199.57.23). However, the original server hasn't been put out of operation so this vulnerability issue persists.

[…]

With this in mind, other application “endpoints” (URLs) are likely to have the same problem. […]

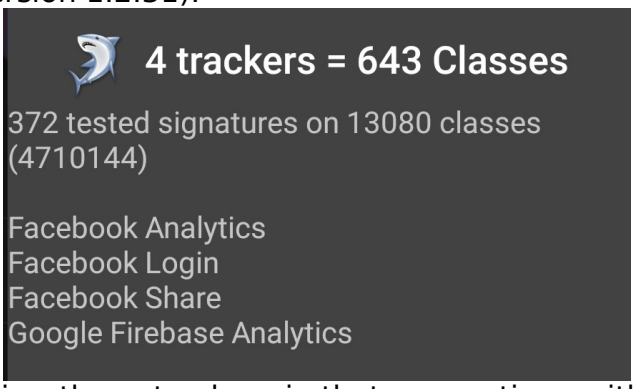
which would facilitate automating an attack to extract information.

We think that this vulnerability issue can be reproduced by making a request to the API hosted at: […]

In order to evaluate our findings, we asked the support line for security incidents from NGO Access Now to review our diagnosis of this vulnerability issue and they agree with our analysis.

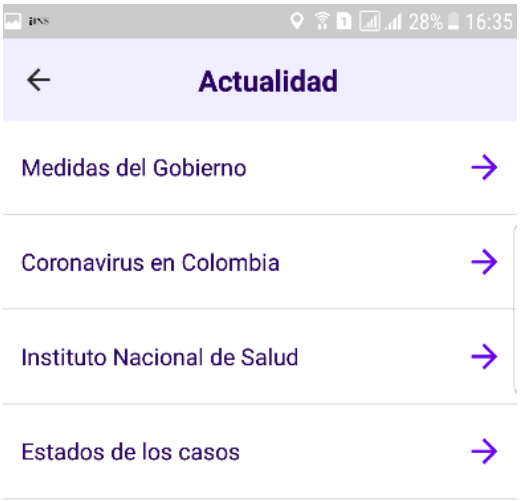
4. Trackers in the application

The analysis of trackers found directly in the application code shows us the following (the same ones appear in version 1.2.31):



The consequence of using these trackers is that connections with Google and Facebook servers can be observed in the flow captures (Wireshark). This generates a direct user trace by these third parties through the use of an application that processes sensitive data.

It should also be noted that because the purpose of this application is to provide information, it is connected to the websites of the Presidency, the National Institute of Health, and the Ministry of Health. Connections to various third-party servers are shown, including advertising platforms:



However, the presence of the latter is not directly due to the application but to the external Internet sites from which they extract the information.

In the latest version of the app, there are two trackers (Google CrashLytics and Google Firebase Analytics). Facebook's trackers have been removed.

ANNEXES - References

[0] Preliminary email sent to INS, AND and MINTIC

Subject: Analysis of the CoronApp application
Date: Sat, 28 Mar 2020 15:35:43 -0500
From: XXXXXX - Karisma <XXXXXXX@karisma.org.co>
Organization: Fundación Karisma
To: XXX@ins.gov.co, XXX@mintic.gov.co, XXX@and.gov.co, XXX@mintic.gov.co
CC: XXX XXX <XXXX@karisma.org.co>, XXX XXX<XXXXX@karisma.org.co>

Good afternoon,

Karisma Foundation is a civil society organization, founded in 2003 and located in Bogotá, that seeks to respond to the opportunities and threats that arise in the context of "technology for development" for the exercise of human rights. Karisma carries out activism with multiple perspectives - legal and technological - in coalitions with local, regional and international partners.

For several years we have been evaluating security and privacy aspects of some web pages and applications associated with procedures and services of public interest. These analyzes have been reported to the Ministry of Technology (MINTIC), which on several occasions has provided us with means of communication with those teams or individuals responsible for the operation of the analyzed platforms. We hope to receive this kind of support in this occasion.

Right now **we are conducting a non-intrusive analysis of the CoronApp application**, promoted by the National Institute of Health, in terms of privacy and digital security. Part of our evaluation includes the analysis of the data traffic generated by the forms that collect personal information, and for this reason, we want to inform you that you will find records in the name of Karisma, associated with the email XXX@karisma.org.co. This data is not real and should not be taken into account for health reports or alert generation.

Once we have the full report of our findings on the CoronApp application, we will send it to you in the first place.

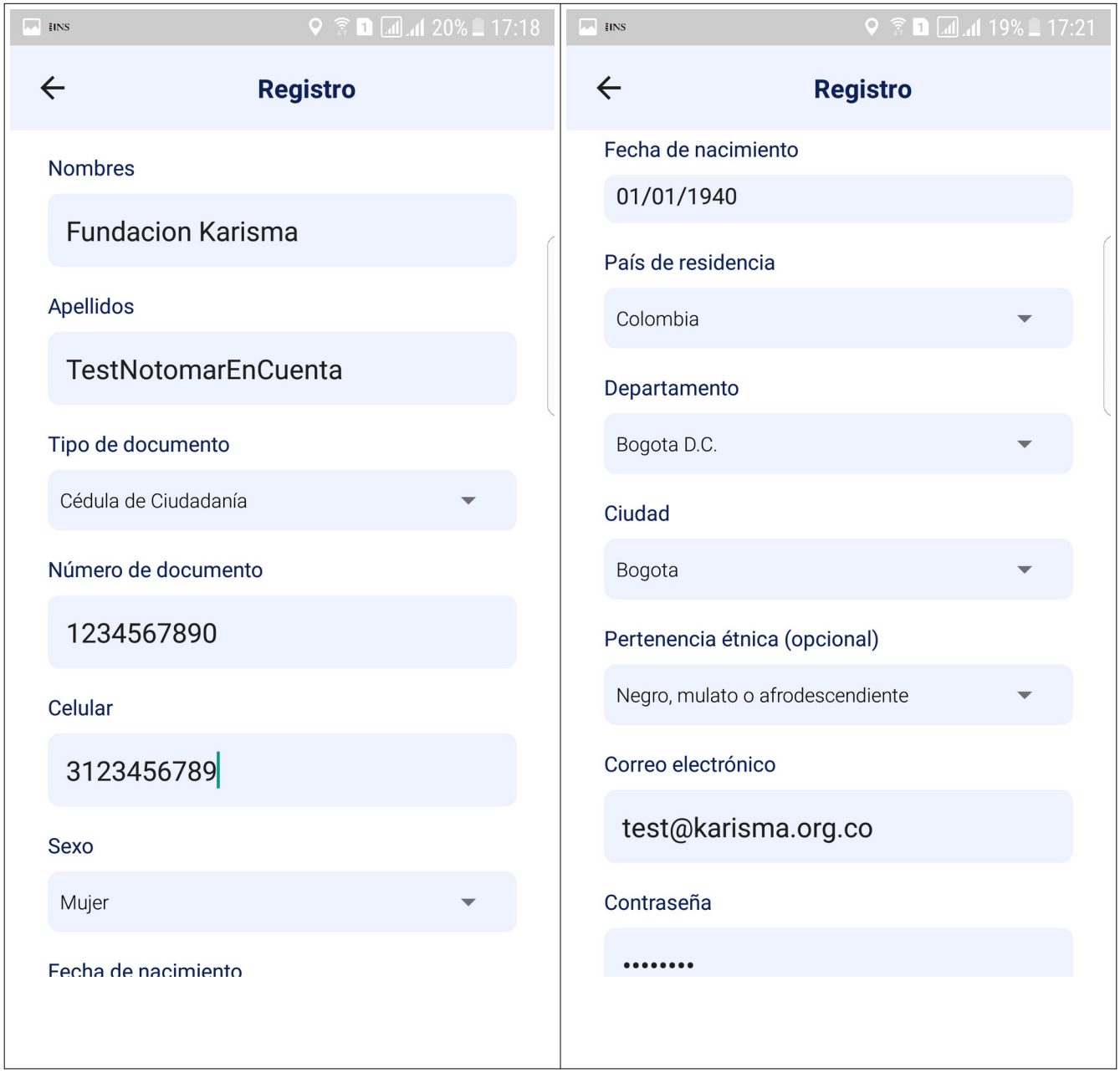
If you have any questions or concerns about the subject, you can contact us by answering this email. We look forward to answering any questions.

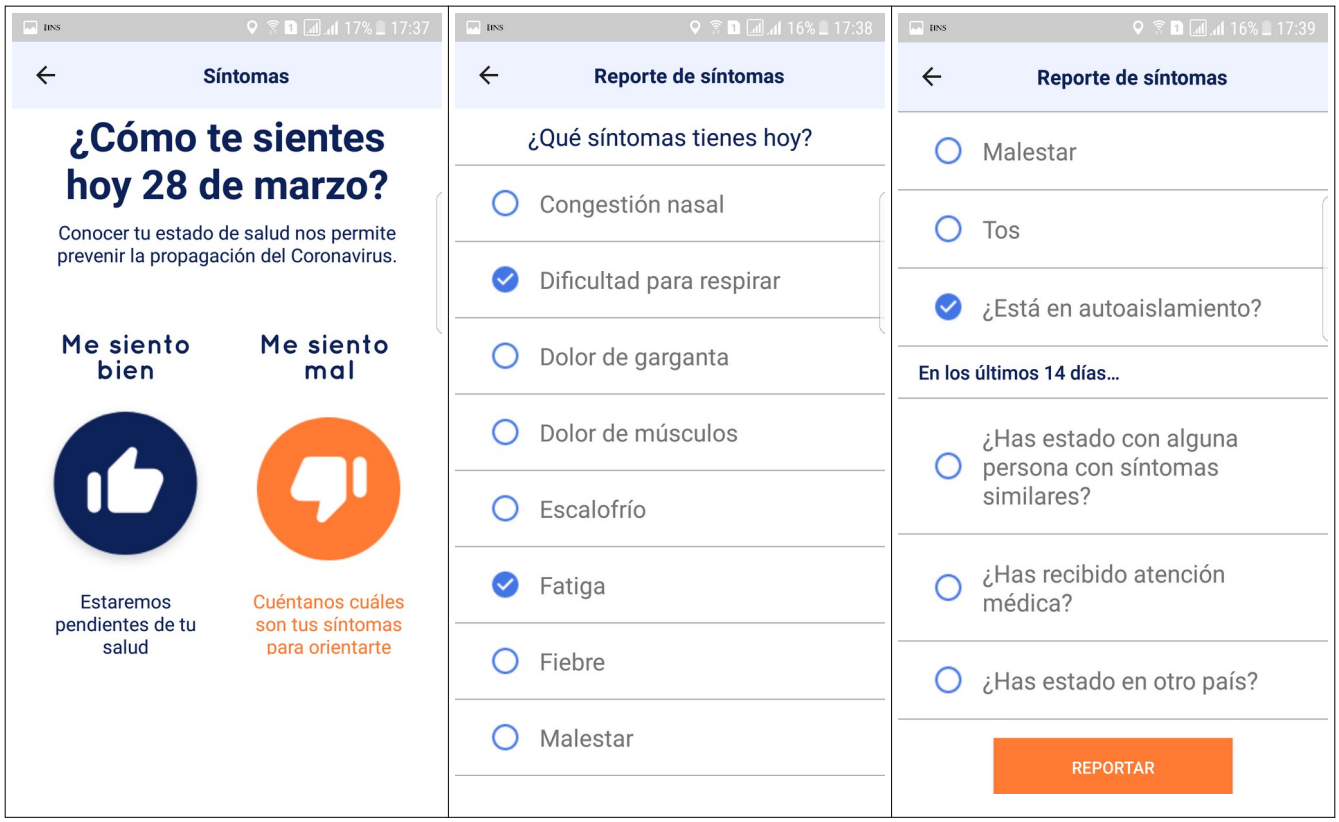
Sincerely,

Karisma Foundation

[1] CoronApp application data collection forms

(completed for analysis)




Síntomas
¿Cómo te sientes hoy 28 de marzo?
Conocer tu estado de salud nos permite prevenir la propagación del Coronavirus.
Me siento bien
Me siento mal
Estaremos pendientes de tu salud
Cuéntanos cuáles son tus síntomas para orientarte
Reporte de síntomas
¿Qué síntomas tienes hoy?
Congestión nasal
Dificultad para respirar
Dolor de garganta
Dolor de músculos
Escalofrío
Fatiga
Fiebre
Malestar
Reporte de síntomas
Malestar
Tos
¿Está en autoaislamiento?
En los últimos 14 días...
¿Has estado con alguna persona con síntomas similares?
¿Has recibido atención médica?
¿Has estado en otro país?
REPORTAR

[2] Application permissions. App manifest (Android Manifest)

(Android Manifest, .xml file made by developers to describe the application technically)

AndroidManifest.xml (~/karisma/coronapp/co.gov.ins.guardianes_33_apps.evozi.com)

File Edit View Search Tools Documents Help

```xml
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" android:compileSdkVersion="29"
android:compileSdkVersionCodename="10" package="co.gov.ins.guardianes" platformBuildVersionCode="29" platformBuildVersionName="10">
    <uses-permission android:name="co.gov.ins.guardianes.permission.MAPS_RECEIVE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="com.android.alarm.permission.SET_ALARM"/>
    <uses-permission android:name="android.permission.FOREGROUND_SERVICE"/>
    <uses-permission android:name="android.permission.CALL_PHONE"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.BLUETOOTH"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
    <uses-feature android:name="android.hardware.bluetooth_le" android:required="true"/>
    <uses-permission android:name="android.permission.BLUETOOTH_PRIVILEGED"/>
    <uses-permission android:name="android.permission.BLUETOOTH"/>
    <uses-permission android:name="android.permission.BLUETOOTH_ADMIN"/>
    <uses-feature android:name="android.hardware.camera" android:required="true"/>
    <uses-feature android:glEsVersion="0x00020000" android:required="true"/>
    <uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
    <uses-permission android:name="com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE"/>
    <application android:allowBackup="true" android:appComponentFactory="androidx.core.app.CoreComponentFactory" android:extractNativeLibs="false" android:icon="@mipmap/
ic_gds" android:isSplitRequired="true" android:label="@string/app_name_short" android:largeHeap="true" android:name="co.gov.ins.guardianes.manager.Application"
android:roundIcon="@mipmap/ic_gds" android:theme="@style/Theme.Home" android:usesCleartextTraffic="true" android:networkSecurityConfig="@xml/network_security_config">
        <activity android:exported="false" android:name="co.gov.ins.guardianes.view.menu.CoronappAbout"
android:parentActivityName="co.gov.ins.guardianes.view.HomeActivity" android:screenOrientation="portrait" android:theme="@style/Theme.NoActionBar"/>
        <activity android:name="co.gov.ins.guardianes.view.news.TypeOfDiseaseActivity" android:parentActivityName="co.gov.ins.guardianes.view.news.NewsActivity"
android:screenOrientation="portrait" android:theme="@style/Theme.NoActionBar" android:usesCleartextTraffic="true"/>
        <activity android:name="co.gov.ins.guardianes.view.welcome.WelcomeIntro" android:screenOrientation="portrait"/>
        <uses-library android:name="org.apache.http.legacy" android:required="false"/>
        <activity android:name="co.gov.ins.guardianes.view.SplashActivity" android:noHistory="true" android:screenOrientation="fullSensor" android:theme="@style/
Theme.NoActionBar">
```

[3] Sending Registration data using the HTTP protocol (version 1.2.30)

Wireshark · Packet 535 · Captura WireShark 2 (Registro).pca

```
› Frame 535: 925 bytes on wire (7400 bits), 925 bytes captured (7400 bits) on interface 0
› Ethernet II, Src: MurataMa_18:e0:1f (b8:d7:af:18:e0:1f), Dst: klab-Inspiron-7559.local (84:ef:18:ce:6a:21)
› Internet Protocol Version 4, Src: 10.42.0.202 (10.42.0.202), Dst: apicovid.and.gov.co (52.87.234.39)
› Transmission Control Protocol, Src Port: 57220, Dst Port: 5000, Seq: 1, Ack: 1, Len: 859
˅ IPA protocol ip.access, type: unknown 0x53
    DataLen: 20559
    Protocol: Unknown (0x53)

0000  84 ef 18 ce 6a 21 b8 d7  af 18 e0 1f 08 00 45 00   ····j!·· ····· ··E·
0010  03 8f 5f 52 40 00 40 06  ae a4 0a 2a 00 ca 34 57   ··_R@·@· ···*··4W
0020  ea 27 df 84 13 88 c6 a8  74 62 c1 10 4a 54 80 18   ·'····· ·· tb··JT··
0030  02 ad 37 4e 00 00 01 01  08 0a 00 13 2b 3e 06 1e   ··7N···· ····+>··
0040  81 c5 50 4f 53 54 20 2f  75 73 65 72 2f 63 72 65   ··POST / user/cre
0050  61 74 65 20 48 54 54 50  2f 31 2e 31 0d 0a 61 70   ate HTTP /1.1··ap
0060  70 5f 74 6f 6b 65 6e 3a  20 64 34 31 64 38 63 64   p_token:  d41d8cd
0070  39 38 66 30 30 62 32 30  34 65 39 38 30 30 39 39   98f00b20 4e980099
0080  38 65 63 66 38 34 32 37  65 0d 0a 43 6f 6e 74 65   8ecf8427 e··Conte
0090  6e 74 2d 54 79 70 65 3a  20 61 70 70 6c 69 63 61   nt-Type:  applica
00a0  74 69 6f 6e 2f 6a 73 6f  6e 0d 0a 43 6f 6e 74 65   tion/jso n··Conte
00b0  6e 74 2d 4c 65 6e 67 74  68 3a 20 36 32 36 0d 0a   nt-Lengt h: 626··
00c0  48 6f 73 74 3a 20 61 70  69 63 6f 76 69 64 2e 61   Host: ap icovid.a
00d0  6e 64 2e 67 6f 76 2e 63  6f 3a 35 30 30 30 0d 0a   nd.gov.c o:5000··
00e0  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 4b 65 65 70   Connecti on: Keep
00f0  2d 41 6c 69 76 65 0d 0a  41 63 63 65 70 74 2d 45   -Alive·· Accept-E
0100  6e 63 6f 64 69 6e 67 3a  20 67 7a 69 70 0d 0a 55   ncoding:  gzip··U
0110  73 65 72 2d 41 67 65 6e  74 3a 20 6f 6b 68 74 74   ser-Agen t: okhtt
0120  70 2f 34 2e 32 2e 32 0d  0a 0d 0a 7b 22 66 69 72   p/4.2.2· ···{"fir
0130  73 74 6e 61 6d 65 22 3a  22 46 75 6e 64 61 63 69   stname": "Fundaci
0140  6f 6e 20 4b 61 72 69 73  6d 61 22 2c 22 6c 61 73   on Karis ma","las
0150  74 6e 61 6d 65 22 3a 22  54 65 73 74 4e 6f 74 6f   tname":" TestNoto
0160  6d 61 72 45 6e 43 75 65  6e 74 61 22 2c 22 64 6f   marEnCue nta","do
0170  63 75 6d 65 6e 74 5f 74  79 70 65 22 3a 22 43 43   cument_t ype":"CC
0180  22 2c 22 64 6f 63 75 6d  65 6e 74 5f 6e 75 6d 62   ","docum ent_numb
0190  65 72 22 3a 22 31 32 33  34 35 36 37 38 39 30 22   er":"123 4567890"
01a0  2c 22 70 68 6f 6e 65 22  3a 22 33 31 32 33 34 35   ,"phone" :"312345
01b0  36 37 38 39 22 2c 22 65  6d 61 69 6c 22 3a 22 74   6789","e mail":"t
01c0  65 73 74 40 6b 61 72 69  73 6d 61 2e 6f 72 67 2e   est@kari sma.org.
01d0  63 6f 22 2c 22 70 61 73  73 77 6f 72 64 22 3a 22   co","pas sword":"
01e0  41 7a 65 72 74 79 37 38  22 2c 22 63 6c 69 65 6e   Azerty78 ","clien
01f0  74 22 3a 22 61 70 69 22  2c 22 67 65 6e 64 65 72   t":"api" ,"gender
0200  22 3a 22 46 65 6d 65 6e  69 6e 6f 22 2c 22 61 70   ":"Femen ino","ap
0210  70 5f 74 6f 6b 65 6e 22  3a 22 64 34 31 64 38 63   p_token" :"d41d8c
```

Here you can see an HTTP packet transferring the form data. The unusual use of port 5000 causes Wireshark to not recognize the HTTP protocol, but its content shows that it is (POST / user / create HTTP /1.1) and shows the data filled in the registration form:
firstname: Fundacion Karisma, lastname: TestNoTenerEncuenta, document number 1234567890, phone: 3123456789, email: test@karisma.org.co, gender: femenino e incluso el password: Azerty78. In the part that follows, all the other data entered in the form is shown.

Data is transferred to the domain "apicovid.and.gov.co" on a server with IP address 52.87.234.39.

[4] This Annex has been removed.

In order not to facilitate attacks, even though we know that the reported vulnerability issue is currently corrected, we will not disclose the details of this annex. The goal of this exercise is to contribute to an improvement in digital security and privacy.

[5] Wireshark captures Extract, app version 1.2.31, executed on an Android 7 phone

In order not to facilitate attacks, even though we know that the reported vulnerability is currently corrected, a section of this annex (the request) has been removed. However, we leave a portion of the server response that shows the personal datas that it was possible to access.

HTTP/1.1 200 OK
Server: nginx/1.17.9
Date: Mon, 30 Mar 2020 00:04:43 GMT
Content-Type: application/json; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
25a
{"error":false,"message":[...]","member":{"id":[...]","picture":0,"dob":"1942-01-01T00:00:00","city":"Bogota","state":"Bogota D.C.","gender":"Hombre","firstname":"Fundacion Karismados","user":"[...]","platform":"android","client":"api","country":"Colombia","race":"Indigena","relationship":"Conyugue","lastname":"PruebaNotomarEncuentaEstosDato","app_token":"d41d8cd98f00b204e9800998ecf8427e","createdAt":"2020-03-30T00:04:43.2472659+00:00","updatedAt":"2020-03-30T00:04:43.2472702+00:00","document_number":"1234567899","document_type":"TI"}}

[6] Burp flow extract (app version 1.2.29)

Only part of the original Annex (server response) is shown.

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: nginx/1.17.9
Date: Tue, 31 Mar 2020 20:47:39 GMT
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 2361

{"error":"false","data":[{"surveys":[{"id":"5e83a9f9ebc6fc0001072d67","platform":"android","no_symptom":"Y","lon":-122.084,"lat":37.4219983,"app_token":
"d41d8cd98f00b204e9800998ecf8427e","user":"5e83a9e0ebc6fc0001072d65","week_of":"2020-03-31T20:37:13.866Z","coordinates":[-122.084,37.4219983],"createdAt":
"2020-03-31T20:37:13.866Z","updatedAt":"2020-03-31T20:37:13.866Z","client":"api","hadTravelledAbroad":false,"startDate":"0001-01-01T00:00:00Z","hadContagiousContact":false,
"hadHealthCare":false},{"id":"5e83a9f9ebc6fc0001072d66","platform":"android","no_symptom":"Y","lon":-122.084,"lat":37.4219983,"app_token":"d41d8cd98f00b204e9800998ecf8427e",
"user":"5e83a9e0ebc6fc0001072d65","week_of":"2020-03-31T20:37:13.858Z","coordinates":[-122.084,37.4219983],"createdAt":"2020-03-31T20:37:13.858Z","updatedAt":
"2020-03-31T20:37:13.858Z","client":"api","hadTravelledAbroad":false,"startDate":"0001-01-01T00:00:00Z","hadContagiousContact":false,"hadHealthCare":false}],"user":{"id":
"5e83a9e0ebc6fc0001072d65","picture":0,"dob":"1900-01-01T00:00:00Z","city":"Bogota","email":"test2@karisma.org.co","state":"Bogota D.C.","gender":"Masculino","firstname":
"usuario prueba","platform":"android","country":"Colombia","race":"Escoge una opción","gcm_token":
"czwM3ujW-3E:APA91bHpXXOtwPhvtxOCnyc_28Ii74SSbfDwfTBU2fEy_JBA0YjHzosPOYmWifDN5P-fsaDAGzGSgM-lii69uVH4hyeWbA5XqsB8kwqqH4wlOegTQEchIH4lFY8yDyKP8cRpUVy9cwkT","lastname":"test",
"week_of":"2020-04-01T20:36:48.512Z","active":"Y","isAdmin":false,"app":"d41d8cd98f00b204e9800998","age":120,"ageGroup":"80","token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbmlxdWVfbmFtZSI6IjVlODNhOWUwZWJjNmZjMDAwMTA3MmQ2NSIsIm5iZiI6MTU4NTY4NzAwOCwiZXhwIjoxNTg4Mjc5MDA4LCJpYXQiOjElODU2ODcwMDh9.UPE_NdBRtNqY
zAyLhxIPmN8RKoFAb3pmx-tFbwAMTJc","device_id":"4dc1b4eb13a5f495","document_number":"12345678","document_type":"CC","createdAt":"2020-03-31T20:36:48.512Z","updatedAt":
"2020-03-31T20:36:48.512Z"},"id":"5e83ac67ebc6fc0001072d80","picture":0,"dob":"1900-01-01T00:00:00Z","city":"Bogota","state":"Bogota D.C.","gender":"Hombre","firstname":
"usuario2 prueba","platform":"android","country":"Colombia","race":"Rom-Gitano","relationship":"Bisnieto","lastname":"test","appToken":"d41d8cd98f00b204e9800998ecf8427e",
"createdAt":"2020-03-31T20:47:35.982Z","updatedAt":"2020-03-31T20:47:35.982Z","documentNumber":"12345678","documentType":"CC"}]}
```