Tesla Consulting

DON'T BE AN EASY TARGET

Security Audit CovidApp Executive Summary

18 Febbraio 2020, Stefano Fratepietro

Summary

- The goals of the security audit are:

- verify the security level of the mobile application;
- verify the absence of artifacts that can lead to the identification of a device;
- verify the security level of Amazon AWS cloud service;
- suggest an improvement plan in case of serious flaws.

- The build numbers of the reviewed apps are respectively: CoviDoc 1.1.11 and CovidApp 1.1.29

Document classification: Public

Tesla Consulting, Part of Be Group

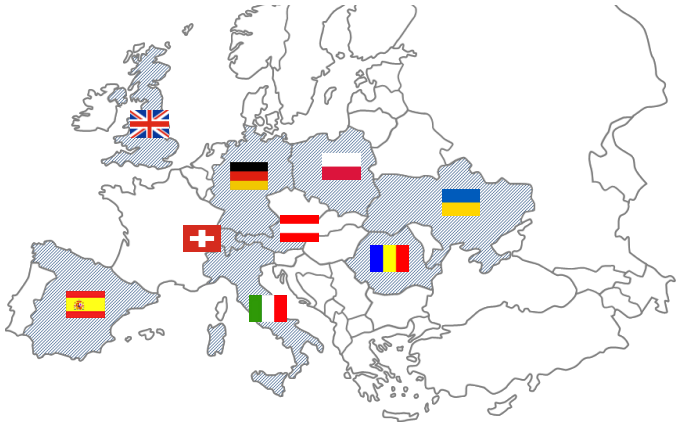
1. **The company was founded by Stefano Fratepietro in 2013**
2. In 2019 Tesla Consulting is purchased by the Be Think, Solve, Execute S.p.A. Group, an Italian multinational listed on the STAR segment
3. 6 years to establish from scratch a recognized **professional network in 8 European countries** beside Italy (42% of non domestic revenues in 2017). More than 1,600 professionals involved of which more than 1,100 are permanent.
4. 3-year Plan forecasts in 2022 an **EBITDA >45 €/mln with M&A**

Be Tesla Consulting

CYBER SECURITY TECHNOLOGY PARTNERS

QUALYS® FORCEPOINT Carbon Black.

proofpoint. SOPHOS splunk> VARONIS



Document classification: Public

Team

Stefano **Fratepietro**

CEO Tesla – CSO Be

Emanuele Bartoli

Cyber Security Specialist

Fabio **Cassanelli**

Head of CSCR

Document classification: Public

Methodology

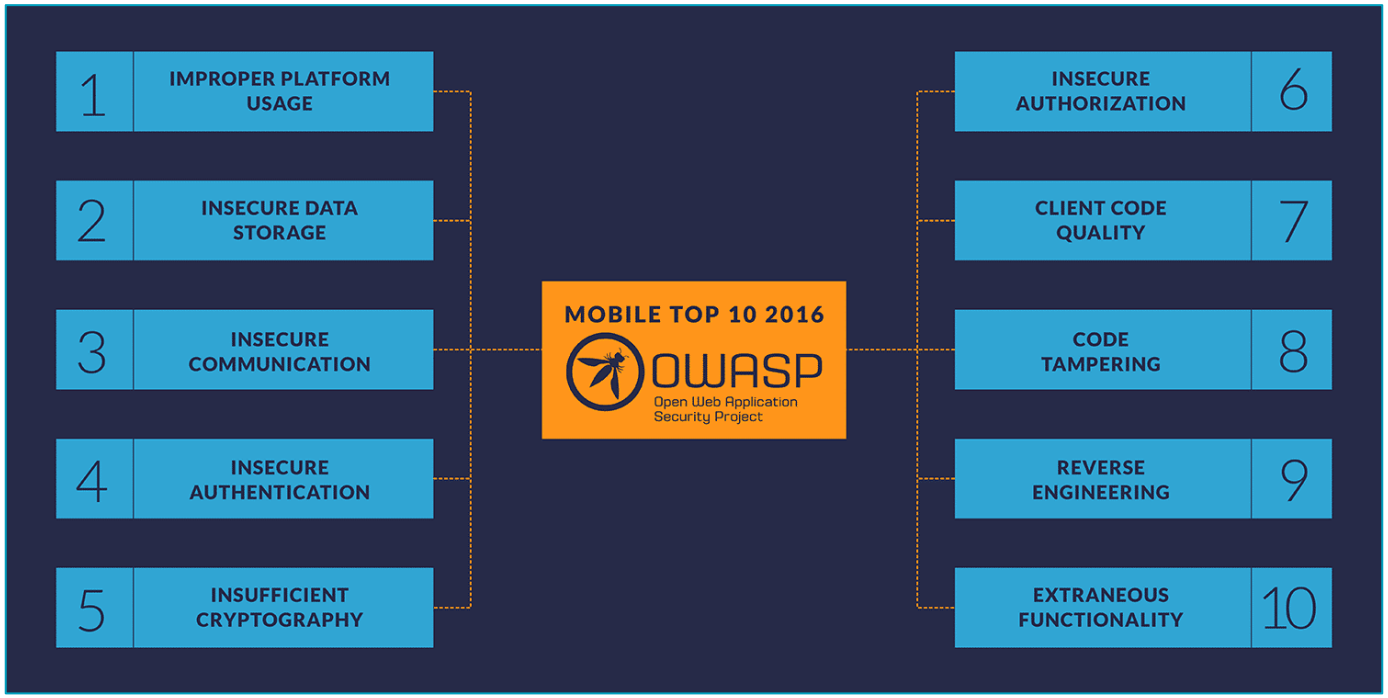
- The entire activity has been carried out by highly qualified Computer Scientists, with the following international certifications released by recognised IT security organisations:

- OSSTMM Professional Security Tester (**OPST**) released by ISECOM
- Offensive Security Certified Professional (**OSCP**) released by Offensive Security Ltd
- eLearnSecurity Mobile Application Penetration Tester (**eMAPT**) released by Caendra Inc.

Document classification: Public

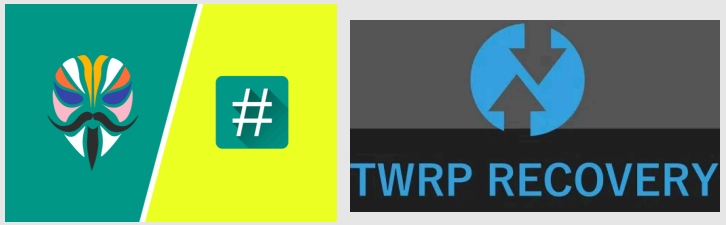
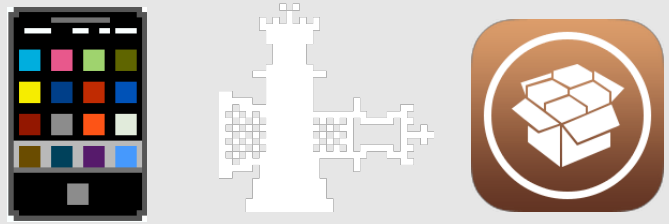
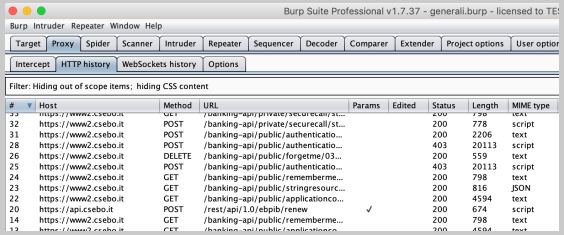
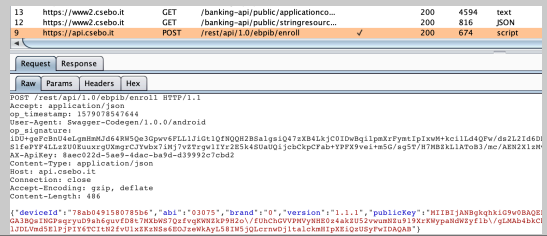
Methodology – Mobile Application

- We used the Open Web Application Security Project (OWASP) for the analysis of mobile applications, which provided practical indications on the checks to be carried out during a Mobile Application Penetration Test.



Document classification: Public

Toolkit

	Android	iOS
Vertical developer platform		
Tools for changing the integrity of the device or application		
Tool dedicate to inspect the network traffic		
Specific command line tools, open source and custom developed	adb, aapt, apktool, enjarify, qark, scandroid…	keychain_dumper, otool, class-dump, Clutch, ioscan…

Document classification: Public

Tesla Consulting

DON'T BE AN EASY TARGET

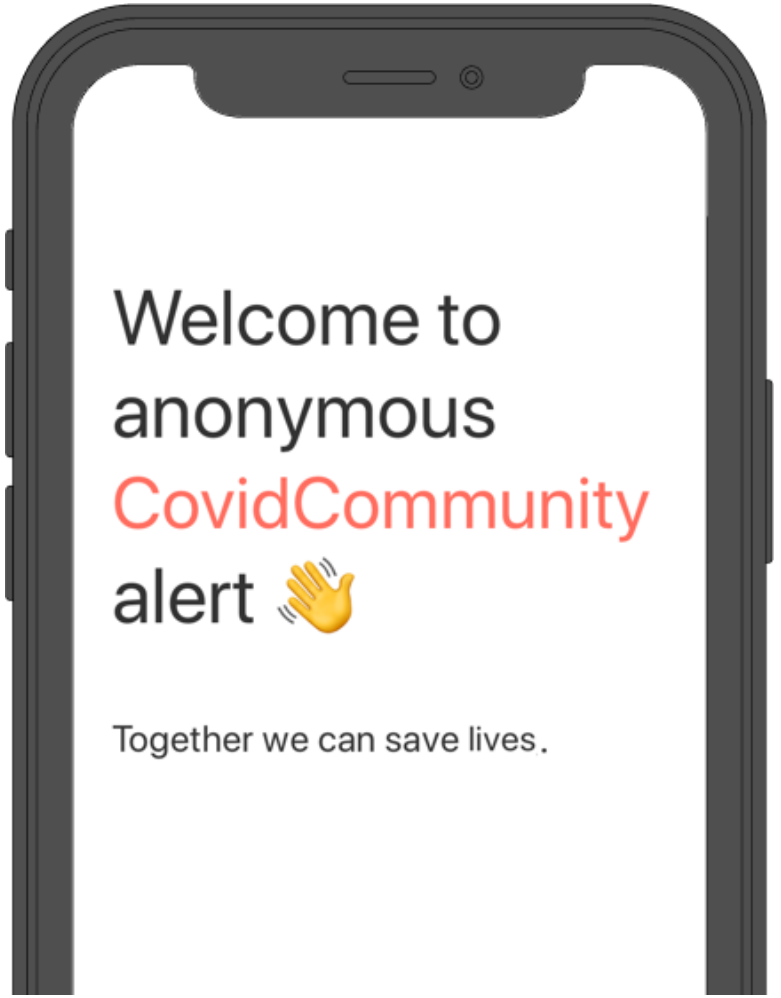
Mobile Application

User App device enroll

Document classification: Public

Introduction

- The service is based on the users (aka patients) that install a "user app" (org.coronavirus_outbreak_control.android) on their mobile devices. The device is then enrolled with a unique installation id to the backend, which also returns a server-assigned id to the device. By leveraging Bluetooth technology, the user app is able to track the proximity of one or more application users.
- Another key component of the service is the "doctor app" (org.coronavirus_outbreak_control_doctor.android), which can only be used by medical staff, which is able to change a patient status to positive, negative or recovered from COVID-19.
- By combining the status and the proximity monitoring capabilities of the app, it is possible to anonymously track which user (only identified by an installation and numeric id) met a COVID positive user and his/her level of risk.



Document classification: Public

User app first device enroll

- The output below shows the main steps of the data flow which intercurs between the mobile application and the backend endpoint during the setup process:

- The application initially issues a request containing the unique identifier of the current installation, other platform specific details, and the token released by the invisible Google Captcha challenge that the user must solve to enroll the device (this challenge is only shown to a small subset of users identified as potential bots).

```
POST /device/handshake HTTP/1.1
Content-Type: application/json; charset=utf-8
Content-Length: 484
Host: api.coronaviruscheck.org
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.1

{"os":{"name":"Android","version":"9"},"challenge":"03AHaCkAbHT48Cvbwrru7Rdsdu6d
hIDR0ULJ0snpkyZ7MgkT_ZEH-dGbNoKPvPfUGLz87uSef3W4Z-lIr-
AB1ymuwDz89Y89HEu6EYav96y9Q12-lIBQdDs_nKpK0Bm1fcVeFA_neM0v1_YIJtP-
RSDapJY4pLWHRUhO3okzoMnyFCiPJP3R2_iROLKd1D2C4F-jGbr-
TAoLnd1ZmqSKgPjzrjKQQUBxm33mer6XFUz34nP9QayUkYf7eNUnjcHCLZLk3_T4t-
2MXST08ZkYjMNv2-
9o2IyEg_KuyeRE7WQxp6zLGah3DtCP5BtKpwSJybXKtyeVV15Fv9","id":"4afde1d1-3ca1-4a6f-
b8a0-4b9f6849f7e7","device":{"model":"A0001","manufacturer":"OnePlus"}}
```

User app first device enroll

- The backend responds with a server-assigned user id and a JWT token, used for authentication purposes

```
HTTP/1.1 200 OK
Date: Tue, 07 Apr 2020 08:48:41 GMT
Content-Type: application/json
Connection: close
Server: openresty/1.15.8.3
Content-Length: 181

{"cache": true,"id": 1728, "token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1ODYyNDk5MjEsImlkIjoxNzI4LCJpYX
QiOjE1ODYyNDkzMjF9.c2x8oWi4LJmEm-dgOwRdpm_ije-xm4UP8BVpaQStUu8"}
```

As shown below, the JWT payload only contains the same server-assigned user id and additional data in epoch format to manage the token expiration.

JWT

```
Headers = {
  "alg" : "HS256",
  "typ" : "JWT"
}

Payload = {
  "exp" : 1586249921,
  "id" : 1728,
  "iat" : 1586249321
}

Signature = "c2x8oWi4LJmEm-dgOwRdpm_ije-xm4UP8BVpaQStUu8"
```

Document classification: Public

User app first device enroll

- The device then issues another PUT request to the endpoint with same JWT and user id.

```
PUT /device HTTP/1.1
Accept: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1ODYyNDk5MjEsImlkIjoxNzI4LCJpYXQ
iOjE1ODYyNDkzMjF9.c2x8oWi4LJmEm-dgOwRdpm_ije-xm4UP8BVpaQStUu8
Content-Type: application/json; charset=utf-8
Content-Length: 208
Host: api.coronaviruscheck.org
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.1

{"push_id":"cS7zcIjqTwGh8sePMOkRtW:APA91bF4cHG54gmxm9S7zW_tc8aqPjuwcPQGyg3ndD1Rf
SWlUu_l1g1WF315_wIpZ_ka44pHP5IZSoLeCA2TeSKKMWpS6PIDn2aZWzbaH_3Mc2rxHruTAvkFDd6-
ccKnG3dx7AA5TEZo","id":1728,"platform":"android"}
```

Document classification: Public

User app second device enroll

- Below is shown the same exact flow for the enrollment of the second testing device, which will be interacting with first one described earlier.

```
POST /device/handshake HTTP/1.1
Content-Type: application/json; charset=utf-8
Content-Length: 488
Host: api.coronaviruscheck.org
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.1

{"device":{"manufacturer":"OnePlus","model":"A0001"},"id":"6fcaaacf-4965-4b66-
adf9-2a2493dc2bda","challenge":"03AHaCkAYyCiFjG-7APsj1JDjQ4qpsrgwQNXZnvzJ-
3QmAYXVv1z1XFqWia5eJKd0JgDlFqM29pQUyw0Dz7pD9ffeSjmI0wnRTSZlDsURz4Fotoj_IW66g8FPP
bb_Kd5AR4l6d6dkjyonUpG9MzqUXbIHhEVeh85OU65KV0rCFBl4h8EZBivk01OVK213-
Jpj11ntn6A4CDVdmMgbQSSvwBpAXfjGVzsAa5woJgwvdEMwye-Ddri-
fyxbTTP8eNE9owFqSimX43DqA5f-vIuNoomEAoMuq1bFtkktVcMlQPZYOGbs3W-
Y_ZIpOFmH6h4OY7ZXbXwMqXOB4","os":{"name":"Android","version":"6.0.1"}}
```

```
HTTP/1.1 200 OK
Date: Tue, 07 Apr 2020 08:51:52 GMT
Content-Type: application/json
Connection: close
Server: openresty/1.15.8.3
Content-Length: 181

{"cache": true,"id": 1730, "token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1ODYyNTAxMTIsImlkIjoxNzMwLCJpYX
QiOjE1ODYyNDk1MTJ9.Z-nXEa_SxMpGkfsIGhrvnFvAsnggupwD8jymYBYtFBM"}
```

User app second device enroll

JWT

```
Headers = {
  "alg" : "HS256",
  "typ" : "JWT"
}

Payload = {
  "exp" : 1586250112,
  "id" : 1730,
  "iat" : 1586249512
}

Signature = "Z-nXEa_SxMpGkfsIGhrvnFvAsnggupwD8jymYBYtFBM"
```

```
PUT /device HTTP/1.1
Accept: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1ODYyNTAxMTIsImlkIjoxNzMwLCJpYXQ
iOjE1ODYyNDk1MTJ9.Z-nXEa_SxMpGkfsIGhrvnFvAsnggupwD8jymYBYtFBM
Content-Type: application/json; charset=utf-8
Content-Length: 208
Host: api.coronaviruscheck.org
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.1

{"platform":"android","id":1730,"push_id":"esgs1dJLRQmq0QOKl545oz:APA91bFVhSdfHp
Nw5PShs3ta95CltQLKeGgqnl4ItG2rPoDNCpL7NJ_FXNQBpZwAvZONoyyuafmGMaJ6vIaKxCA6277Kou
u7d2uykfIO4KcmdAHZUVGjN4TektGBkAnM1_GBFCPErCLB"}
```

Document classification: Public

Tesla Consulting

DON'T BE AN EASY TARGET

Mobile Application

User App interaction

Document classification: Public

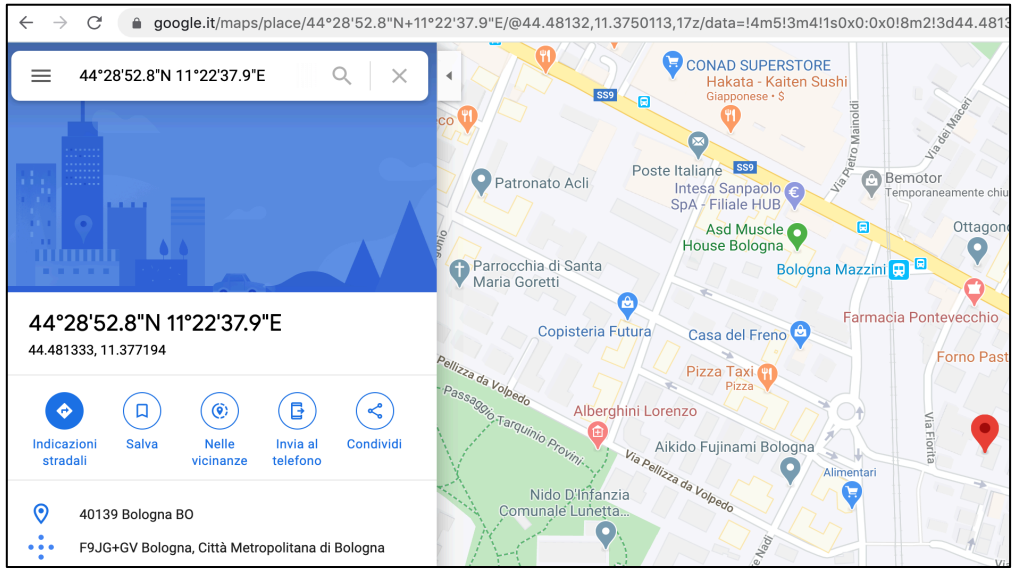
User apps interaction

- The below request shows the main task carried on by the application: at regular ten minutes intervals, the device issues a request to the backend containing the user ids of other devices that use the Covid Outbreak Control application and that have been seen within a proximity range.

- If that is the case, the two applications share their own user ids (which are transmitted to each other via Bluetooth LE technology).
  Other information sent to the backend are: the timestamp of the interaction, the RSSI of the Bluetooth signals and the GPS coordinates approximated to the 5th decimal digit. The latter is sent to the backend only if the user opted-in to share it.

```
POST /interaction/report HTTP/1.1
Accept: application/json
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1ODYyNTAxMTIsImlkIjoxNzMwLCJpYXQiOjE1ODYyNDk1MTJ9.Z-nXEa_SxMpGkfsIGhrvnFvAsnggupwD8jymYBYtFBM
Content-Type: application/json; charset=utf-8
Content-Length: 111
Host: api.coronaviruscheck.org
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.1

{"i":1730,"p":"a","v":2,"z":[{"o":1728,"w":1586249521,"t":114,"r":65,"s":"1.4","x":"44.48132","y":"11.37720"}]}
```



User apps interaction

- The server responds stating the next time interval (in seconds) for the next report to be issued:

```
HTTP/1.1 200 OK
Date: Tue, 07 Apr 2020 08:53:56 GMT
Content-Type: application/json
Content-Length: 33
Connection: close
Server: openresty/1.15.8.3

{"next_try":600,"location":false}
```

Document classification: Public

Tesla Consulting

DON'T BE AN EASY TARGET

Mobile Application

The doctor App

Document classification: Public

The Doctor App

- The service include also a "Doctor App", which comprises a different enrollment process:

1. The Doctor's mobile phone number is registered as "authorised" in the backend by the operators or through a previous invitation by an authorised individual.
2. During the first install, the doctor is required to input his own mobile phone number, which is used to receive a second factor of authentication (six digits pin) via SMS text message.

- The output below summarises the process; the doctor initially inputs his mobile phone number:

```
POST /v1/activation/request HTTP/1.1
Content-Type: application/json; charset=utf-8
Content-Length: 32
Host: doctors.coronaviruscheck.org
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.1

{"phone_number":"+39335[REDACTED]50"}
```

```
HTTP/1.1 202 Accepted
Date: Tue, 07 Apr 2020 14:00:48 GMT
Content-Length: 0
Connection: close
```

Document classification: Public

The Doctor App

- The doctor receives the six digits pin (334645) via SMS text message and inputs that in the second authentication step:

```
GET /v1/activation/confirm/334645 HTTP/1.1
Host: doctors.coronaviruscheck.org
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.1
```

- The output below shows the security token released after the code verification has been successful:

```
HTTP/1.1 200 OK
Date: Tue, 07 Apr 2020 14:01:10 GMT
Content-Type: application/json
Content-Length: 84
Connection: close

{"id":41,"token":"47094dee0120fc8f0c3dd4adefbff4eeff7b50aa7c088352ea152520d49f86da"}
```

Document classification: Public

The Doctor App

- The Doctor app then issues a "refresh token" request with its token, to obtain a JWT used for session management purposes:

```
POST /v1/authenticate HTTP/1.1
Authorization: Bearer
47094dee0120fc8f0c3dd4adefbff4eeff7b50aa7c088352ea152520d49f86da
Content-Type: application/json; charset=utf-8
Content-Length: 2
Host: doctors.coronaviruscheck.org
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.1

{}
```

```
HTTP/1.1 200 OK
Date: Tue, 07 Apr 2020 14:01:11 GMT
Content-Type: application/json
Content-Length: 128
Connection: close

{"token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1ODYyNjg2NzEsImlkIjo0M
X0.jhSgy_jWp9S6xpRq8MUIkYUgDH8Xsz0nIQGYTLwcT-I"}
```

Document classification: Public

The Doctor App

- As shown in the screenshot below, the content of the JWT token only includes the doctor's numeric id. It is also important to notice that the format is different by the one of the patient's, to avoid authorisation issues between doctor's and patient's tokens.

JWT

```
Headers = {
  "alg" : "HS256",
  "typ" : "JWT"
}

Payload = {
  "exp" : 1586268671,
  "id" : 41
}

Signature = "jhSgy_jWp9S6xpRq8MUIkYUgDH8Xsz0nIQGYTLwcT-I"
```

Document classification: Public

The Doctor App

- The following is the Doctor's app main screen, once the enrollment process is completed:

Document classification: Public

Tesla Consulting

DON'T BE AN EASY TARGET

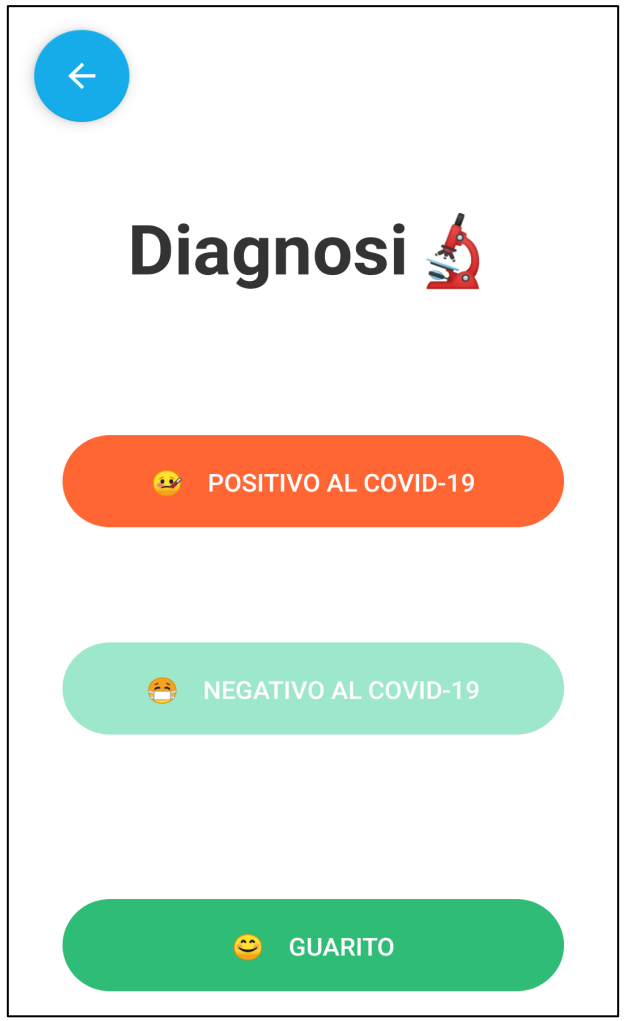
Mobile Application

Doctor App changing a patient's status

Document classification: Public

Doctor App changing a patient's status

- The main purpose of the doctor app is to change the health status of the users, in case a COVID-19 test has been carried out.



Document classification: Public

Doctor App changing a patient's status

- Below there is an example of a request issued by the doctor application when changing the status of a user.
- The POST request sends as URL parameters the patient's user id (1730) and the corresponding status, where:

- • 0 means negative to COVID-19
- • 1 means positive to COVID-19
- • 2 is a temporary status before confirming the patient is positive to COVID-19
- • 3 means recovered from COVID-19

```
POST /v1/mark/1730/2 HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1ODYyNjk2NTMsImlkIjo0MX0.s-
6dskPmSZNx3LM7wGLHjAqSkUGUM2eY3mDdJRIDRek
Content-Type: application/json; charset=utf-8
Content-Length: 2
Host: doctors.coronaviruscheck.org
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.1

{}
```

Document classification: Public

Doctor App changing a patient's status

- The server responds with a "transaction" id (1292), the status change for the patient, and the information of the doctor who made the change.

```
HTTP/1.1 200 OK
Date: Tue, 07 Apr 2020 14:25:26 GMT
Content-Type: application/json
Content-Length: 105
Connection: close

{"id":1292,"patient_id":1730,"old_status":0,"actual_status":2,"updated_by":41,"u
pdated_at":1586269526000}
```

Document classification: Public

Doctor App changing a patient's status

- A patient can only be moved to state 1 (positive) after having been confirming as state 2 (suspected).

```
POST /v1/mark/1730/1 HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1ODYyNjk2NTMsImlkIjo0MX0.s-
6dskPmSZNx3LM7wGLHjAqSkUGUM2eY3mDdJRIDRek
Content-Type: application/json; charset=utf-8
Content-Length: 2
Host: doctors.coronaviruscheck.org
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.1

{}
```

```
HTTP/1.1 200 OK
Date: Tue, 07 Apr 2020 14:25:45 GMT
Content-Type: application/json
Content-Length: 105
Connection: close

{"id":1293,"patient_id":1730,"old_status":2,"actual_status":1,"updated_by":41,"u
pdated_at":1586269544000}
```

Document classification: Public

Tesla Consulting

DON'T BE AN EASY TARGET

Mobile Application

Security issue #1

Document classification: Public

#1 User IDs pollution by ineffective captcha validation

- It was identified that the captcha code, obtained after resolving the Google captcha challenge, is not properly validated by the Covid API backend. As a consequence, it was possible to re-use the same captcha challenge with different device ids.

```
POST /device/handshake HTTP/1.1
Content-Type: application/json; charset=utf-8
Content-Length: 508
Host: api.coronaviruscheck.org
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.1

{"device":{"manufacturer":"unknown","model":"Android SDK built for
x86"},"id":"ac045bcb-449a-486e-bf32-
155eb34496dc","challenge":"03AHaCkAbJ5TD1lJfrZ_p66ebPL9AdfpoTFA9dOzvha9WU3IuJRB3
D9m2k8ma7OneFrKLUK1XvINGJ8eZ6XMfkQYgYj6hzxAnIQPgg_ttyR1BIHXo6kSGNAesAPk55vvNLuhE
cuUv_z9Kr2eE0Dz-MWxb_cSVql63g6JwV6WRdsMSO4bELrKDGWOcOHHLu_BcTti0CGVUZv0-
YNQjP7DuYhTpAATs9TsAaECctvF93kHGHtql1xXDU3_C4zUOXBscZDzk7wl8rFzr8VgODzlSXMGnti_B
C62msC0L0TYYZz5XYPH4m7CZWiEWsVXTJtk_iMt8BS027s5DB","os":{"name":"Android","versi
on":"5.0.2"}}
```

```
HTTP/1.1 200 OK
Date: Wed, 01 Apr 2020 16:32:49 GMT
Content-Type: application/json
Connection: close
Server: openresty/1.15.8.3
Content-Length: 181

{"cache": true,"id": 1636, "token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1ODU3NTkzNjksImlkIjoxNjM2LCJpYX
QiOjE1ODU3NTg3Njl9.w5f2NF1wz1zavQeXkmNyXoYg2i8as3XxsivHXzSi2l0"}
```

#1 User IDs pollution by ineffective captcha validation

- The below request issues the same exact captcha solution with a slightly modified device id

```
POST /device/handshake HTTP/1.1
Content-Type: application/json; charset=utf-8
Content-Length: 514
Host: api.coronaviruscheck.org
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.1

{"device":{"manufacturer":"unknown","model":"Android SDK built for
x86"},"id":"ac045bcb-449a-486e-bf32-
155eb34496dclalala","challenge":"03AHaCkAbJ5TD1lJfrZ_p66ebPL9AdfpoTFA9dOzvha9WU3
IuJRB3D9m2k8ma7OneFrKLUK1XvINGJ8eZ6XMfkQYgYj6hzxAnIQPgg_ttyR1BIHXo6kSGNAesAPk55v
vNLuhEcuUv_z9Kr2eE0Dz-MWxb_cSVql63g6JwV6WRdsMSO4bELrKDGWOcOHHLu_BcTti0CGVUZv0-
YNQjP7DuYhTpAATs9TsAaECctvF93kHGHtql1xXDU3_C4zUOXBscZDzk7wl8rFzr8VgODzlSXMGnti_B
C62msC0L0TYYZz5XYPH4m7CZWiEWsVXTJtk_iMt8BS027s5DB","os":{"name":"Android","versi
on":"5.0.2"}}
```

- The server accepted the request and allocated a new server assigned user id. As visible also from the above request, the captcha was first used on the 1st of April and was still accepted on the 7th, as shown from the below response.

```
HTTP/1.1 200 OK
Date: Tue, 07 Apr 2020 10:24:52 GMT
Content-Type: application/json
Connection: close
Server: openresty/1.15.8.3
Content-Length: 181

{"cache":false,"id": 1732, "token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1ODYyNTU2OTIsImlkIjoxNzMyLCJpYX
QiOjE1ODYyNTUwOTJ9.XVpi9xwYlGP5ZQJztsJufQiOHTEki1JcbVaZCnx1Hp8"}
```

Document classification: Public

#1 User IDs pollution by ineffective captcha validation

- Here there is another request issued with the same logic - the device id is different but captcha is the same.

```
POST /device/handshake HTTP/1.1
Content-Type: application/json; charset=utf-8
Content-Length: 516
Host: api.coronaviruscheck.org
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.1

{"device":{"manufacturer":"unknown","model":"Android SDK built for
x86"},"id":"ac045bcb-449a-486e-bf32-
155eb34496dclalalala","challenge":"03AHaCkAbJ5TD1lJfrZ_p66ebPL9AdfpoTFA9dOzvha9W
U3IuJRB3D9m2k8ma7OneFrKLUK1XvINGJ8eZ6XMfkQYgYj6hzxAnIQPgg_ttyRlBIHXo6kSGNAesAPk5
5vvNLuhEcuUv_z9Kr2eE0Dz-MWxb_cSVql63g6JwV6WRdsMSO4bELrKDGWOcOHHLu_BcTti0CGVUZv0-
YNQjP7DuYhTpAATs9TsAaECctvF93kHGHtq1lxXDU3_C4zUOXBscZDzk7wl8rFzr8VgODzlSXMGnti_B
C62msC0L0TYYZz5XYPH4m7CZWiEWsVXTJtk_iMt8BS027s5DB","os":{"name":"Android","versi
on":"5.0.2"}}
```

- The server still issued a new user id.

```
HTTP/1.1 200 OK
Date: Tue, 07 Apr 2020 10:25:11 GMT
Content-Type: application/json
Connection: close
Server: openresty/1.15.8.3
Content-Length: 181

{"cache":false,"id": 1733, "token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1ODYyNTU3MTEsImlkIjoxNzMzLCJpYX
QiOjE1ODYyNTUxMTF9.IBst6bebRbrs60ylR2AF46WMKjZ56tVR2fBvglcPVHg"}
```

- This may lead to a backend database pollution, since a malicious attacker may automate the process to make the server allocate a multitude of user ids. Further more, as also shared with the developers, this has a particular impact given the small payload size which can be transmitted by the app via Bluetooth LE, therefore leading to a Denial of Service condition where there are no more valid user ids available to allocate.

Document classification: Public

Tesla Consulting

DON'T BE AN EASY TARGET

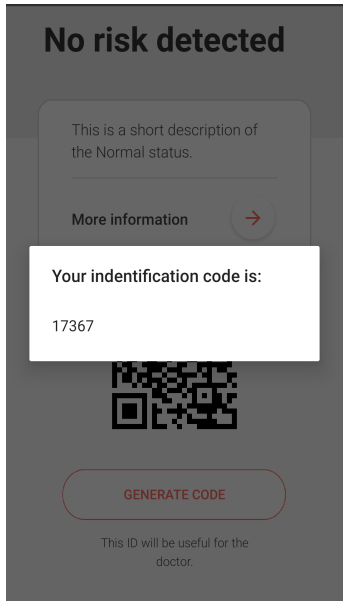
Mobile Application

Security issue #2

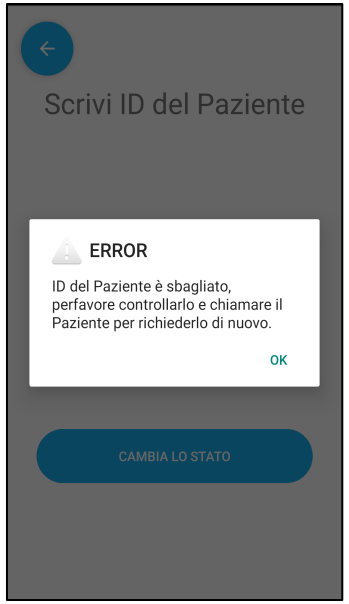
Document classification: Public

#2 Lack of patient's checksum control in network communication

- When a doctor is about to change a patient status, he must input an identification code (which can be provided by the patient itself), corresponding to the server-assigned user id concatenated to a "checksum" control value, as highlighted in the screenshot.



- In case the doctor inputs only the user id without the checksum value, an error is returned preventing the status change. This aims to prevent a doctor from changing a user status by mistake.



Document classification: Public

#2 User IDs pollution by ineffective captcha validation

- However, the actual request issued for the status change does not contain anywhere the checksum value, meaning that the control check is only performed within the app but it's not replicated on a network level.

- As visible from below, the following request is successfully processed with no need of the checksum value.

```
POST /v1/mark/1736/1 HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1ODYyNzIyNTQsImlkIjo0MX0.d3VoVOf
Y-zoz4Rw4I7JFef8tTYB0ynoek8ik1EeYJvU
Content-Type: application/json; charset=utf-8
Content-Length: 2
Host: doctors.coronaviruscheck.org
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.1

{}
```

```
HTTP/1.1 200 OK
Date: Tue, 07 Apr 2020 15:01:27 GMT
Content-Type: application/json
Content-Length: 105
Connection: close

{"id":1304,"patient_id":1736,"old_status":2,"actual_status":1,"updated_by":41,"u
pdated_at":1586271687000}
```

Document classification: Public

Tesla Consulting

DON'T BE AN EASY TARGET

Mobile Application

Security issue #3

Document classification: Public

#3 Mass status change

- By design, a doctor is allowed to change the status of every patient. This is intended as a design behaviour, since different doctors may be involved in a patient history.
- However, as seen in Finding #2, the request issued by a doctor is simple and predictable in structure, as the only "dynamic" field is the patient numeric user ID, which is just a progressive number (and no controls are performed on the checksum value, which would guarantee the "physical" relationship between doctor and patient).
- Combined with the lack of control on the patient's ID checksum value, this could allow a doctor to issue a multitude of requests by only progressively changing the user id, which would be processed also in case of patients which never had a relationship with the "malicious" doctor, therefore mining the whole application purpose.
- The following request/response pair shows how it was possible to specify a patient id which was never involved in the previous use cases, as the only parameter needed is the predictable progressive numeric id.

```
POST /v1/mark/1725/0 HTTP/1.1
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE1ODYyNzEwMzMsImlkIjo0MX0.dHA9ok2
jVK751r3k8DXRPLgpFs7QNXd9eAqn3XAXqCQ
Content-Type: application/json; charset=utf-8
Content-Length: 2
Host: doctors.coronaviruscheck.org
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.1

{}
```

```
HTTP/1.1 200 OK
Date: Tue, 07 Apr 2020 14:42:59 GMT
Content-Type: application/json
Content-Length: 105
Connection: close

{"id":1299,"patient_id":1725,"old_status":3,"actual_status":0,"updated_by":41,"u
pdated_at":1586270579000}
```

Tesla Consulting
DON'T BE AN EASY TARGET

Amazon AWS

Security issue #1
Missing MFA Auth

Document classification: Public

#1 Missing MFA Auth

- To login into the tenant as an administrator, only a username and password are required without the use of two-factor authentication.
- Many data breaches are the result of passwords that fail to provide enough protection. Today, a single authentication at login isn't enough to keep your data safe, and multi-factor authentication (MFA) is a must. By requiring users to login using their account password and then go through a second step, you can reduce your risk exposure. Some common examples of MFA include:
- • OTP (one-time passwords): Sending OTPs via phone or email to the user to verify their identity before completing their login.
- • USB hardware tokens: Attaching a USB that generates an OTP to authenticate the user before allowing access.
- AWS users looking for a way to employ MFA without adding another line item to their security budget can make use of free tools like Google Authenticator.

Document classification: Public

Conclusion

- All the patient identities are masked and it is not possible to identify the real person:
  - There are no information on local storage that an attacker can use to identify a patient
  - There is no relevant information sent that an attacker can use to identify a patient
  - There are no relevant issues with the Amazon AWS cloud services

- According to the Covid Community Alert Dev team, the security issues were resolved with the release CoviDoc 1.1.12 and CovidApp 1.1.30

- These controls are valid for the current implementation of the platform and will be redone if an implementation has been carried out from scratch on another infrastructure. We are available to assist the team for a secure implementation on other infrastructures.

Document classification: Public

Tesla Consulting

DON'T BE AN EASY TARGET

Tesla Consulting Srl, Part of Be Group
Via Enrico Mattei 88, 40138 Bologna – ITALY

Tel: +39 0510548633
http://www.teslaconsulting.it