ANDROID STATIC ANALYSIS REPORT

COVID19 CAT (Failed)

File Name:	COVID19 CAT 1.0.2.apk
Package Name:	Failed
Average CVSS Score:	6.1
App Security Score:	30/100 (HIGH RISK)
Trackers Detection:	3/285

FILE INFORMATION

File Name: COVID19 CAT 1.0.2.apk
Size: 3.23MB
MD5: da64943017606d5e9de4b421ba7b66dc
SHA1: fcbf08d9c4f72aca322ef17450e35193900c3b45
SHA256: 3d0f7b85eb2faade388960aa2e4d8243547755cc603bc5aaafbeb27844cb3914

APP INFORMATION

App Name: COVID19 CAT
Package Name: Failed
Main Activity:
Target SDK:
Min SDK:
Max SDK:
Android Version Name: Failed
Android Version Code: Failed

APP COMPONENTS

Activities: 0
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=ES, ST=Catalunya, L=Barcelona, O=Generalitat de Catalunya, OU=Direcci¢ General d'Atenci¢ Ciutadana i Difusi¢, CN=Ricard Mateu
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-07-17 09:54:14+00:00
Valid To: 2067-04-20 09:54:14+00:00
Issuer: C=ES, ST=Catalunya, L=Barcelona, O=Generalitat de Catalunya, OU=Direcci¢ General d'Atenci¢ Ciutadana i Difusi¢, CN=Ricard Mateu
Serial Number: 0x50053646
Hash Algorithm: sha1
md5: 4c85af6630cf5ed6a3b926d0ac3d2872
sha1: 2b9ac28b45b89adf1d7ed40635dba24666879f30
sha256: 2ab5c95ae49e6edcb1fb7dac8cb563887f76d2f26376ab9b512d6bde78f43de0
sha512:

8dbf7331cb3476bf9fe0e950b9712b71a78e0aae0d088ceb8331b98c65c6bcfd0e48dadf16670a9f54d9ca458b4a59df9d99247551ec7543a2a8603fdf34c7fa

PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: e51aa1e0bdd84e9e1c15db4230c39f3f78255042bb7e45eddc21dbe2da81a934

Certificate Status: Warning
Description: The app is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.The manifest indicates SHA256withRSA is in use. Please verify this manually.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.MODEL check Build.MANUFACTURER check network operator name check FINDINGS: Compiler — DETAILS: dx

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION

CODE ANALYSIS

ISSUE	SEVERITY	STANDARDS	FILES
			cat/gencat/mobi/StopCovid19Cat/main/f.java a/n/ba.java a/n/da.java a/n/V.java a/n/ca.java a/n/ea.java a/n/U.java a/a/a/a/a.java a/a/c/g.java a/f/g/b.java a/f/a/a.java a/f/a/a/b.java a/f/a/a/h.java a/f/f/a.java a/f/h/C0056b.java a/f/h/v.java a/f/h/e.java a/f/h/g.java a/f/h/t.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	a/f/b/b.java a/f/b/e.java a/f/b/f.java a/f/b/k.java a/o/a/a/k.java a/h/a/c.java a/j/a/a.java a/k/a/b.java a/l/a/b.java c/c/a/a/a/a/b.java c/c/a/a/a/a/c.java c/c/a/a/a/a/a.java c/c/a/a/c/d/m.java c/c/a/b/a/h.java c/c/a/b/b/a.java com/mubiquo/library/mmm/B.java com/mubiquo/library/mmm/C0600i.java com/mubiquo/library/mmm/w.java com/mubiquo/library/mmm/z.java com/mubiquo/library/mmm/AlarmReceiver.java com/mubiquo/library/mmm/O.java com/mubiquo/library/mmm/v.java com/mubiquo/library/mmm/C.java com/mubiquo/library/mmm/C0592a.java com/mubiquo/library/mmm/C0597f.java com/mubiquo/library/mmm/H.java com/mubiquo/library/mmm/D.java com/mubiquo/library/mmm/q.java com/mubiquo/library/mmm/C0607p.java com/mubiquo/library/mmm/BackgroundFetchIntentService.java com/mubiquo/library/mmm/I.java com/mubiquo/library/mmm/J.java com/mubiquo/library/mmm/s.java com/mubiquo/library/mmm/C0593b.java com/mubiquo/library/mmm/F.java com/mubiquo/library/mmm/G.java com/mubiquo/library/mmm/BootCompleteBroadcastReceiver.java com/mubiquo/library/mmm/C0604m.java com/mubiquo/library/mmm/C0601j.java com/mubiquo/library/mmm/K.java com/mubiquo/library/mmm/C0598g.java

ISSUE	SEVERITY	STANDARDS	FILES
			com/mubiquo/library/mmm/u.java com/mubiquo/library/mmm/y.java com/mubiquo/library/mmm/C0594c.java com/mubiquo/library/mmm/C0602k.java com/mubiquo/library/mmm/L.java com/mubiquo/library/mmm/C0603l.java com/mubiquo/library/mmm/M.java com/mubiquo/library/mmm/C0595d.java com/mubiquo/library/mmm/x.java com/mubiquo/library/mmm/A.java com/mubiquo/library/mmm/LocationProviderIntentService.java com/mubiquo/library/mmm/t.java com/mubiquo/library/lottusse/n.java com/mubiquo/library/lottusse/q.java com/mubiquo/library/lottusse/i.java com/mubiquo/library/lottusse/r.java com/microsoft/appcenter/utils/a.java b/a/a/a/d/h.java b/a/a/a/d/g.java
			a/n/ia.java a/n/ja.java a/n/M.java a/f/a/a/b.java a/f/h/C.java a/f/h/a/b.java a/f/h/a/c.java a/d/h.java a/d/d.java a/d/i.java a/b/a/b/b.java c/c/a/b/a/h.java c/c/a/b/a/i.java d/C0621n.java d/w.java d/C0608a.java d/u.java d/C0615h.java d/y.java d/L.java d/M.java d/a/e/e.java d/a/e/a.java com/microsoft/appcenter/crashes/a/a/b.java com/microsoft/appcenter/crashes/a/a/c.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	com/microsoft/appcenter/crashes/a/a/d.java com/microsoft/appcenter/crashes/a/a/e.java com/microsoft/appcenter/crashes/a/a/f.java com/microsoft/appcenter/crashes/a/a/g.java com/microsoft/appcenter/crashes/a/a/a.java com/microsoft/appcenter/http/k.java com/microsoft/appcenter/http/HttpException.java com/microsoft/appcenter/b/a/b.java com/microsoft/appcenter/b/a/c.java com/microsoft/appcenter/b/a/h.java com/microsoft/appcenter/b/a/e.java com/microsoft/appcenter/b/a/i.java com/microsoft/appcenter/b/a/f.java com/microsoft/appcenter/b/a/a.java com/microsoft/appcenter/b/a/c/b.java com/microsoft/appcenter/b/a/c/c.java com/microsoft/appcenter/b/a/c/d.java com/microsoft/appcenter/b/a/c/e.java com/microsoft/appcenter/b/a/c/f.java com/microsoft/appcenter/b/a/c/a.java com/microsoft/appcenter/b/a/b/n.java com/microsoft/appcenter/b/a/b/c.java com/microsoft/appcenter/b/a/b/h.java com/microsoft/appcenter/b/a/b/d.java com/microsoft/appcenter/b/a/b/e.java com/microsoft/appcenter/b/a/b/i.java com/microsoft/appcenter/b/a/b/j.java com/microsoft/appcenter/b/a/b/f.java com/microsoft/appcenter/b/a/b/g.java com/microsoft/appcenter/b/a/b/l.java com/microsoft/appcenter/b/a/b/m.java com/microsoft/appcenter/b/a/b/a.java

ISSUE	SEVERITY	STANDARDS	FILES
			com/microsoft/appcenter/analytics/b/a.java com/microsoft/appcenter/analytics/b/a/a.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/mubiquo/library/mmm/K.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	com/mubiquo/library/mmm/K.java com/mubiquo/library/mmm/L.java com/microsoft/appcenter/utils/d/d.java com/microsoft/appcenter/persistence/a.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/microsoft/appcenter/a/i.java
The App uses an insecure Random Number Generator.	high	CVSS V2: 7.5 (high) CWE: CWE-330 - Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/microsoft/appcenter/http/j.java

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
s3.amazonaws.com	good	IP: 52.216.136.214 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.04372 Longitude: -77.487488 View: Google Map
pagead2.googlesyndication.com	good	IP: 172.217.167.98 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
mmm.mubiquo.com	good	**IP:** 52.0.78.156 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.04372 **Longitude:** -77.487488 **View:** Google Map
stag.mubiquo.com	good	No Geolocation information available.
data.mubiquo.com	good	No Geolocation information available.
schemas.android.com	good	No Geolocation information available.
mobile.events.data.microsoft.com	good	**IP:** 52.114.133.60 **Country:** United States of America **Region:** Virginia **City:** Washington **Latitude:** 38.713451 **Longitude:** -78.159439 **View:** Google Map
api.backendcovid19.net	good	**IP:** 52.85.43.26 **Country:** Australia **Region:** Victoria **City:** Melbourne **Latitude:** -37.813999 **Longitude:** 144.963318 **View:** Google Map
location.backendcovid19.net	good	**IP:** 52.31.195.109 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.34399 **Longitude:** -6.26719 **View:** Google Map
stop-covid19-cat.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
in.appcenter.ms	good	**IP:** 20.185.75.141 **Country:** United States of America **Region:** Virginia **City:** Washington **Latitude:** 38.713451 **Longitude:** -78.159439 **View:** Google Map

URLS

URL	FILE
http://schemas.android.com/apk/res/android	a/f/a/a/i.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	c/c/a/a/a/a/b.java
https://stag.mubiquo.com/v1/endpoints/inboxandgeofences https://mmm.mubiquo.com/v1/endpoints/inboxandgeofences https://stag.mubiquo.com/v1/endpoints/checkin https://data.mubiquo.com/v1/endpoints/checkin https://mmm.mubiquo.com/v1/endpoints/checkin	com/mubiquo/library/mmm/K.java
https://s3.amazonaws.com/lottussetestdev.mubiquo.net https://s3.amazonaws.com/lottussetestuat.mubiquo.net https://s3.amazonaws.com/lottussetestlive.mubiquo.net https://s3.amazonaws.com/lottusse-dev.mubiquo.net https://s3.amazonaws.com/lottusse-uat.mubiquo.net https://s3.amazonaws.com/lottusse-live.mubiquo.net	com/mubiquo/library/lottusse/i.java
https://mobile.events.data.microsoft.com/OneCollector/1.0	com/microsoft/appcenter/b/c.java
https://in.appcenter.ms	com/microsoft/appcenter/b/a.java
https://api.backendcovid19.net/api/v1	b/a/a/a/d/b.java
https://location.backendcovid19.net/api/v1	b/a/a/a/d/h.java
https://api.backendcovid19.net/api/v1	b/a/a/a/d/d.java
https://api.backendcovid19.net/api/v1	b/a/a/a/d/f.java
https://stop-covid19-cat.firebaseio.com	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://stop-covid19-cat.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

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

TRACKER	URL
Microsoft Appcenter Analytics	https://reports.exodus-privacy.eu.org/trackers/243
Microsoft Appcenter Crashes	https://reports.exodus-privacy.eu.org/trackers/238

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

Report Generated by - MobSF v3.0.8 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.