MOBSF

ANDROID STATIC ANALYSIS REPORT

Care19 Alert (1.2)

File Name:	Care19 Alert_v1.2_apkpure.com.xapk
Package Name:	com.proudcrowd.exposure
Average CVSS Score:	6.8
App Security Score:	60/100 (MEDIUM RISK)
Trackers Detection:	3/407
Scan Date:	Jan. 25, 2022, 1:24 a.m.

FILE INFORMATION

File Name: Care19 Alert_v1.2_apkpure.com.xapk
Size: 6.75MB
MD5: 021488f89a4813fc47f19cd4ba25e891

SHA1: 5775fd7bee47d8f3af24e53aacb2b89ed4086537
SHA256: c1b4b955f0787f271d47e388814fb4af7e974fa385fa75d0cf4b3de28bcfbe22

APP INFORMATION

App Name: Care19 Alert
Package Name: com.proudcrowd.exposure
Main Activity: com.proudcrowd.exposure.activity.TriageActivity
Target SDK: 29
Min SDK: 23
Max SDK:
Android Version Name: 1.2
Android Version Code: 10

APP COMPONENTS

Activities: 15
Services: 11
Receivers: 12
Providers: 2
Exported Activities: 0
Exported Services: 2
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-07-07 18:33:39+00:00
Valid To: 2050-07-07 18:33:39+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xaa3ea6d8d502a098a8b3d1a4348d4712450fcfdb
Hash Algorithm: sha256
md5: 1b9f51de5c1c84a87cc00b7d5f68a5fe
sha1: a2ab23a6580874fc3ac60aabd5c8544dcf7d2579
sha256: 44c833a1d60d1a5c8f4e3542ac1c05cfc7a487a6bcad0f972c329252ea3609a9
sha512: 69f2267a0caa6e2f2a3dadeedb1b707b14990ef889bcfae507469bd54c3d377de7002f001834972e8e934b31f56baae7c3e84f0f59c5e84e38ef0c5f3e7264c6
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 5d3c1590544caaa4852e728b53f24a90350322179c04142bb4f0f865a7807c37

STATUS	DESCRIPTION
secure	Application is signed with a code signing certificate
warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	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.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	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.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.TAGS check SIM operator check</td></tr><tr><td>Compiler</td><td>r8</td></tr></table>

FILE	DETAILS
classes2.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Anti-VM Code</td><td>Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.TAGS check network operator name check possible VM check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	Broadcast Receiver (com.proudcrowd.exposure.core.ExposureBroadcastReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.nearby.exposurenotification.EXPOSURE_CALLBACK [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.
2	Service (com.google.android.gms.nearby.exposurenotification.WakeUpService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.nearby.exposurenotification.EXPOSURE_CALLBACK [android:exported=true]	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. 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.
3	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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	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. 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.
5	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bugfender/sdk/a/a/f/a.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				Calculator.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bugfender/sdk/a/d/a.java com/bugfender/sdk/a/a/i/a.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/engine/GlideException.java com/proudcrowd/exposure/core/ScanManager.java com/proudcrowd/exposure/datasource/ExposureDownloadDataSource.java com/proudcrowd/exposure/core/FakeScanManager.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bugfender/sdk/a/b/a.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bugfender/sdk/a/a/l/a/p/c.java com/bumptech/glide/request/target/ViewTarget.java com/bugfender/sdk/a/b/d/a.java com/bumptech/glide/load/engine/DecodeJob.java com/bugfender/sdk/a/a/l/a/i.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/engine/Engine.java com/proudcrowd/exposure/datasource/BaseFuturesDataSource.java com/proudcrowd/exposure/datasource/ExposureUploadDataSource.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/proudcrowd/exposure/misc/SingleLiveEvent.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/proudcrowd/exposure/viewmodel/ExposureViewModel.java com/bumptech/glide/load/model/FileLoader.java com/bugfender/sdk/a/a/l/a/f.java com/bugfender/sdk/a/a/l/a/k.java com/proudcrowd/exposure/fragment/BaseCellAdapter.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/load/engine/SourceGenerator.java com/proudcrowd/exposure/fragment/ProtectFragment.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/Glide.java com/bumptech/glide/util/pool/FactoryPools.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/ImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bugfender/sdk/a/b/d/c.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/load/resource/bitmap/DefaultIm

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ageHeaderParser.java com/proudcrowd/exposure/core/ExposureManager.java com/bumptech/glide/manager/RequestManagerFragment.java com/bugfender/sdk/a/b/c/a.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/proudcrowd/exposure/core/NetworkCheck.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/module/ManifestParser.java com/bugfender/sdk/Bugfender.java com/bugfender/sdk/a/a/l/a/a.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/proudcrowd/exposure/activity/StudyConsentActivity.java com/bugfender/sdk/a/a/b.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/gifdecoder/GifHeaderParser.java
2	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	com/proudcrowd/exposure/datasource/ExposureDownloadDataSource.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	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/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/proudcrowd/exposure/storage/ExposureNotificationSharedPreferences.java com/bumptech/glide/load/Option.java
4	SHA-1 is a weak hash known to have hash collisions.	warning	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/bugfender/sdk/a/a/e/d.java
5	The App uses an insecure Random Number Generator.	warning	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/bugfender/sdk/a/a/m/a.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	CVSS V2: 0 (info) OWASP MASVS: MSTG-NETWORK-4	com/proudcrowd/exposure/datasource/BaseDataSource.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['bluetooth', 'network connectivity'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
12	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
13	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
14	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
15	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.
16	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
dashboard.bugfender.com	good	**IP:** 31.170.103.66 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
care19-exposure.firebaseio.com	good	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
storage.googleapis.com	good	**IP:** 142.250.217.112 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.bugfender.com	good	**IP:** 31.170.103.66 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
exposureapi.care19.app	good	**IP:** 104.43.254.102 **Country:** United States of America **Region:** Iowa **City:** Des Moines **Latitude:** 41.600540 **Longitude:** -93.609108 **View:** Google Map

URLS

URL	FILE
http://localhost/	retrofit2/Response.java
data:image	com/bumptech/glide/load/model/DataUrlLoader.java
file:///android_asset/	com/bumptech/glide/load/model/AssetUriLoader.java
https://api.bugfender.com/ https://dashboard.bugfender.com	com/bugfender/android/BuildConfig.java

URL	FILE
https://storage.googleapis.com/exposure-notification-export-lmuvk	com/proudcrowd/exposure/datasource/ExposureManagerDataSource.java
https://exposureapi.care19.app/	com/proudcrowd/exposure/datasource/BaseDataSource.java
https://care19-exposure.firebaseio.com	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://care19-exposure.firebaseio.com	info App talks to a Firebase Database.

TRACKERS

TRACKER	CATEGORIES	URL
Bugfender	Crash reporting, Analytics	https://reports.exodus-privacy.eu.org/trackers/233
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://care19-exposure.firebaseio.com"
"google_api_key" : "AIzaSyDGvKTGzPN1tXbbFHGrQhZC5zbc0nhIaO4"
"google_crash_reporting_api_key" : "AIzaSyDGvKTGzPN1tXbbFHGrQhZC5zbc0nhIaO4"

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 v3.4.5 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.