ANDROID STATIC ANALYSIS REPORT

CO Exposure Notifications (minted1000003)

File Name:	CO Exposure Notifications_vminted1000003_apkpure.com.xapk
Package Name:	gov.co.cdphe.exposurenotifications
Average CVSS Score:	6.8
App Security Score:	60/100 (MEDIUM RISK)
Scan Date:	Nov. 19, 2021, 7:15 p.m.

FILE INFORMATION

File Name: CO Exposure Notifications_vminted1000003_apkpure.com.xapk
Size: 3.38MB
MD5: 05fe369de5ff42442f6e1036d48d114d
SHA1: f727762c5a53d2566ed84116df1a5b474ff954d8
SHA256: ba31125e4944b02b3eaec267e5bc890940f0d91c03e1a098fa0f83b57e436fd5

APP INFORMATION

App Name: CO Exposure Notifications
Package Name: gov.co.cdphe.exposurenotifications
Main Activity: com.google.android.apps.exposurenotification.home.ExposureNotificationActivity
Target SDK: 30
Min SDK: 21
Max SDK:
Android Version Name: minted1000003
Android Version Code: 10000032

APP COMPONENTS

Activities: 4
Services: 8
Receivers: 12
Providers: 2
Exported Activities: 0
Exported Services: 2
Exported Receivers: 4
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: 2020-10-09 22:45:24+00:00
Valid To: 2050-10-09 22:45:24+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x956b10e15fcfb8ce3a0a0cba80b9f6e91e3c2a05
Hash Algorithm: sha256
md5: 03c6179ea766de4dc59f48f9ad0f596a
sha1: a006a68af17cdbe0f90e7b36b923d5a0b49f04e3
sha256: be06dc51b4153612c83faf1371b6289c78e8ecaafda9a6ab42eeb4320a123f3a
sha512:
5cba3a3a6a174d4e5f72a90bbaacb63f3e50f5100cbd4f469a30b56e324955480c4bbed1e7c1ad594edcf40e5d3e9547bac457954377e9966042e9b40511282e

PublicKey Algorithm: rsa

Bit Size: 4096
Fingerprint: 64547dc23e60b2bcda3ad655a78979ee10c935072120b41ed3c352d2cf12558b

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 <7.0

APPLICATION PERMISSIONS

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.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.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check FINDINGS: Compiler — DETAILS: r8

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.google.android.apps.exposurenotification.home.ExposureNotificationActivity	Schemes: ens://, https://, Hosts: us-co.en.express,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup=true]	medium	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
2	Broadcast Receiver (com.google.android.apps.exposurenotification.nearby.ExposureNotificationBroadcastReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Broadcast Receiver (com.google.android.apps.exposurenotification.common.ExposureNotificationDismissedReceiver) 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.
4	Broadcast Receiver (com.google.android.apps.exposurenotification.nearby.SmsVerificationBroadcastReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	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.
6	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.

NO	ISSUE	SEVERITY	DESCRIPTION
7	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
1	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.	warning	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	f/b/a/b/i/s/i/z.java f/b/c/k/t/r0.java f/b/a/b/i/s/i/v.java f/b/a/b/i/s/i/t.java f/b/c/k/t/i.java e/t/f.java f/b/a/b/i/s/i/y.java f/b/c/k/t/a1.java f/b/c/k/t/b1.java f/b/c/k/t/q0.java f/b/a/b/i/s/i/w.java f/b/c/k/t/w0.java f/b/a/b/i/s/i/x.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	e/g/b/d.java f/a/b/v.java f/b/a/c/g/a.java e/i/a/o.java e/m/a/e0.java
3	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	h/a/j1/f0.java h/a/k1/g.java h/a/j1/h0.java h/a/j1/n2.java h/a/n1/a.java
4	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	h/a/k1/f.java
5	App creates temp file. Sensitive information should never be written into a temp file.	warning	CVSS V2: 5.5 (medium) CWE: CWE-276 Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	e/t/k.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 implement asymmetric key generation.
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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files 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.
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 in accordance with a specified cryptographic algorithm SHA-1/SHA-256/SHA-384/SHA-512 and message digest sizes 160/256/384/512 bits.
12	FCS_COP.1.1(3)	Selection-Based Security Functional Requirements	Cryptographic Operation - Signing	The application perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm ECDSA schemes using "NIST curves" P-256, P-384.
13	FCS_COP.1.1(4)	Selection-Based Security Functional Requirements	Cryptographic Operation - Keyed-Hash Message Authentication	The application perform keyed-hash message authentication with cryptographic algorithm ['HMAC-SHA-256'] .
14	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
15	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.
16	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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
support.google.com	good	**IP:** 142.251.40.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
apiserver.encv.org	good	**IP:** 34.107.223.222 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
www.jetbrains.com	good	**IP:** 18.200.1.21 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map
g.co	good	**IP:** 142.250.72.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.jetbrains.org	good	**IP:** 54.230.162.4 **Country:** United States of America **Region:** Florida **City:** Jacksonville **Latitude:** 30.332180 **Longitude:** -81.655647 **View:** Google Map
developer.android.com	good	**IP:** 142.251.35.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
plus.google.com	good	**IP:** 142.250.65.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
uwaterloo.ca	good	**IP:** 151.101.2.133 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
code.google.com	good	**IP:** 142.251.32.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.threeten.org	good	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.colorado.gov	good	**IP:** 99.83.143.241 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
mikepenz.com	good	**IP:** 172.67.141.197 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
enpa-ingestion-co.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
checkerframework.org	good	**IP:** 128.208.3.120 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.663902 **Longitude:** -122.291954 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
prod.exposurenotification.health	good	**IP:** 13.107.246.40 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
android.googlesource.com	good	**IP:** 173.194.204.82 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
kotlinlang.org	good	**IP:** 13.225.210.69 **Country:** United States of America **Region:** New Jersey **City:** Newark **Latitude:** 40.735661 **Longitude:** -74.172371 **View:** Google Map
commons.apache.org	good	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
git-wip-us.apache.org	good	**IP:** 52.202.80.70 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
cloud.google.com	good	**IP:** 142.251.40.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.cs.washington.edu	good	**IP:** 34.215.139.216 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	good	**IP:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.google.com	good	**IP:** 142.250.72.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	good	**IP:** 172.217.165.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
raw.githubusercontent.com	good	**IP:** 185.199.109.133 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
android.git.kernel.org	good	No Geolocation information available.
opensource.org	good	**IP:** 159.65.34.8 **Country:** United States of America **Region:** New Jersey **City:** Clifton **Latitude:** 40.858429 **Longitude:** -74.163757 **View:** Google Map
storage.googleapis.com	good	**IP:** 142.250.64.112 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
encdn.prod.exposurenotification.health	good	**IP:** 104.212.67.47 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
spdx.org	good	**IP:** 99.84.216.78 **Country:** United States of America **Region:** Virginia **City:** Dulles **Latitude:** 38.951668 **Longitude:** -77.448059 **View:** Google Map
schemas.android.com	good	No Geolocation information available.
addyourphone.com	good	**IP:** 141.193.213.10 **Country:** United States of America **Region:** Texas **City:** Austin **Latitude:** 30.271158 **Longitude:** -97.741699 **View:** Google Map
cs.android.com	good	**IP:** 142.250.65.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
covid19.colorado.gov	good	**IP:** 52.7.40.57 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.apache.org	good	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.gstatic.com	good	**IP:** 142.250.80.3 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
source.android.com	good	**IP:** 142.251.32.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
findbugs.sourceforge.net	good	**IP:** 204.68.111.100 **Country:** United States of America **Region:** California **City:** San Diego **Latitude:** 32.799797 **Longitude:** -117.137047 **View:** Google Map
tools.android.com	good	**IP:** 142.250.65.179 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

URLS

URL	FILE
http://schemas.android.com/apk/res/android	e/i/b/b/h.java
https://plus.google.com/	f/b/a/c/b/m/g0.java
https://github.com/grpc/grpc-java/issues/5015	h/a/j1/m1.java
https://support.google.com/android?p=enx_app_usage https://support.google.com/android/answer/9888358 http://g.co/ens https://support.google.com/android?p=enx_reporting http://www.colorado.gov/pacific/cdphe/exposure-notifications-privacy-policy https://addyourphone.com https://covid19.colorado.gov/exposure-notifications-20200922-70b1448 https://www.gstatic.com/prio-manifests/gov.co.cdphe.exposurenotifications.config.json https://covid19.colorado.gov/exposure-notifications/privacy-policy https://storage.googleapis.com/covidtech_public_assets_1/CO_EN-186-186.png https://encdn.prod.exposurenotification.health/ https://encdn.prod.exposurenotification.health/v1/index.txt https://prod.exposurenotification.health/v1/publish https://apiserver.encv.org/api/certificate https://apiserver.encv.org/api/verify https://apiserver.encv.org/api/user-report https://covid19.colorado.gov/exposure-notifications https://covid19.colorado.gov/are-you-sick/testing-for-covid-19 https://enpa-ingestion-co.firebaseio.com https://support.google.com/googleplay/answer/9037938 https://support.google.com/android?p=enx_overview https://www.google.com/covid19/exposurenotifications/ http://mikepenz.com/ https://github.com/mikepenz/AboutLibraries https://developer.android.com/jetpack/androidx/releases/activity#1.2.0 https://cs.android.com/androidx/platform/frameworks/support https://developer.android.com/jetpack/androidx http://source.android.com https://developer.android.com/jetpack/androidx/releases/appcompat#1.3.0-alpha02 https://developer.android.com/topic/libraries/architecture/index.html http://developer.android.com/tools/extras/support-library.html	

URL	FILE
http://tools.android.com https://android.googlesource.com/platform/tools/sherpa https://developer.android.com/jetpack/androidx/releases/core#1.5.0-alpha02 https://developer.android.com/jetpack/androidx/releases/fragment#1.3.0 https://developer.android.com/jetpack/androidx/releases/lifecycle#2.3.0 data:2.1.0 https://developer.android.com/jetpack/androidx/releases/savedstate#1.1.0 https://developer.android.com/jetpack/androidx/releases/work#2.5.0-beta01 http://source.android.com/ https://android.git.kernel.org/ https://github.com/material-components/material-components-android http://www.google.com https://github.com/google/auto/tree/master/value http://github.com/google/auto http://findbugs.sourceforge.net/ https://code.google.com/p/jsr-305/ https://www.google.com https://github.com/google/dagger https://github.com/google/dagger/ https://github.com/google/j2objc/ https://cloud.google.com http://www.google.com/ https://github.com/googlei18n/libphonenumber/ https://github.com/JakeWharton/ThreeTenABP/ https://github.com/mikepenz/FastAdapter http://commons.apache.org/proper/commons-io/ https://git-wip-us.apache.org/repos/asf?p=commons-io.git https://github.com/abseil/abseil-cpp https://github.com/google/boringssl https://www.google.com/covid19/exposurenotifications https://github.com/google/exposure-notifications-android https://github.com/google/libprio-cc https://github.com/protocolbuffers/protobuf https://github.com/grpc/grpc-java https://github.com/perfmark/perfmark http://code.google.com/p/atinject/ http://code.google.com/p/atinject/source/checkout https://www.cs.washington.edu/, http://uwaterloo.ca/, https://www.cs.washington.edu/research/plse/ https://checkerframework.org https://github.com/typetools/checker-framework.git http://www.jetbrains.com http://www.jetbrains.org https://github.com/JetBrains/intellij-community https://www.jetbrains.com https://kotlinlang.org/ https://github.com/JetBrains/kotlin https://www.threeten.org https://www.threeten.org/threetenbp https://github.com/ThreeTen/threetenbp http://www.apache.org/licenses/LICENSE-2.0 http://www.apache.org/licenses/LICENSE-2.0.html https://spdx.org/licenses/BSD-3-Clause.html https://raw.githubusercontent.com/google/boringssl/master/LICENSE http://source.android.com/, http://source.android.com/compatibility) https://developer.android.com/studio/terms.html http://opensource.org/licenses/MIT https://support.google.com/android?p=en_analytics https://play.google.com/store/apps/details?id=%1$s https://support.google.com/android?p=enxsms	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://enpa-ingestion-co.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	f/b/a/c/b/y.java
posure_notifications@state.co	Android String Resource

HARDCODED SECRETS

POSSIBLE SECRETS
"define_plu_com_google_android_datatransport__transport_api" : ""
"define_plu_com_google_firebase__firebase_auth_interop" : ""
"define_plu_com_google_firebase__firebase_common" : ""
"define_plu_com_google_firebase__firebase_components" : ""
"define_plu_com_google_firebase__firebase_database_collection" : ""
"define_plu_com_google_firebase__firebase_datatransport" : ""
"define_plu_com_google_firebase__firebase_encoders_json" : ""
"define_plu_com_google_firebase__firebase_firestore" : ""
"define_plu_com_google_firebase__protolite_well_known_types" : ""
"define_plu_io_grpc__grpc_api" : "owner"
"define_plu_io_perfmark__perfmark_api" : "owner"
"enx_testVerificationAPIKey" : "s8zeTxjfOn0ftfPsjkxGZWpbRsBXh8shyKvvmOufML_uvE1sfHJau7eLjjz-7G6F3aTyAY8yXLRZXq-GIzymbw.11.tRcOdxhdAsKy9rT2manDl4tIoubCzuqVa6rLM70koSchZi5OqfhGVOKvqLZN9o9xzWXRFa42Phd8V5HIlAAitw"
"firebase_database_url" : "https://enpa-ingestion-co.firebaseio.com"
"google_api_key" : "AIzaSyCxF41wwOrmfpzEx-3mcELgSuc91bDbaLE"

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyCxF41wwOrmfpzEx-3mcELgSuc91bDbaLE"
"health_authority_id" : ""
"health_authority_name" : ""
"health_authority_website_name" : ""
"health_authority_website_url" : ""
"library_AboutLibraries_author" : "Mike Penz"
"library_AboutLibraries_authorWebsite" : "http://mikepenz.com/"
"library_androidx_annotation__annotation_author" : "AOSP"
"library_androidx_annotation__annotation_experimental_author" : "AOSP"
"library_androidx_appcompat__appcompat_author" : "AOSP"
"library_androidx_appcompat__appcompat_resources_author" : "AOSP"
"library_androidx_arch_core__core_common_author" : "AOSP"
"library_androidx_arch_core__core_runtime_author" : "AOSP"
"library_androidx_cardview__cardview_author" : "AOSP"
"library_androidx_collection__collection_author" : "AOSP"
"library_androidx_constraintlayout__constraintlayout_author" : "AOSP"
"library_androidx_constraintlayout__constraintlayout_solver_author" : "AOSP"
"library_androidx_coordinatorlayout__coordinatorlayout_author" : "AOSP"
"library_androidx_core__core_author" : "AOSP"
"library_androidx_core__core_ktx_author" : "AOSP"
"library_androidx_cursoradapter__cursoradapter_author" : "AOSP"
"library_androidx_customview__customview_author" : "AOSP"
"library_androidx_documentfile__documentfile_author" : "AOSP"
"library_androidx_drawerlayout__drawerlayout_author" : "AOSP"
"library_androidx_dynamicanimation__dynamicanimation_author" : "AOSP"
"library_androidx_fragment__fragment_author" : "AOSP"

POSSIBLE SECRETS
"library_androidx_hilt__hilt_common_author" : "AOSP"
"library_androidx_hilt__hilt_lifecycle_viewmodel_author" : "AOSP"
"library_androidx_hilt__hilt_work_author" : "AOSP"
"library_androidx_interpolator__interpolator_author" : "AOSP"
"library_androidx_legacy__legacy_support_core_utils_author" : "AOSP"
"library_androidx_lifecycle__lifecycle_common_author" : "AOSP"
"library_androidx_lifecycle__lifecycle_livedata_author" : "AOSP"
"library_androidx_lifecycle__lifecycle_livedata_core_author" : "AOSP"
"library_androidx_lifecycle__lifecycle_process_author" : "AOSP"
"library_androidx_lifecycle__lifecycle_runtime_author" : "AOSP"
"library_androidx_lifecycle__lifecycle_service_author" : "AOSP"
"library_androidx_lifecycle__lifecycle_viewmodel_author" : "AOSP"
"library_androidx_lifecycle__lifecycle_viewmodel_savedstate_author" : "AOSP"
"library_androidx_loader__loader_author" : "AOSP"
"library_androidx_localbroadcastmanager__localbroadcastmanager_author" : "AOSP"
"library_androidx_navigation__navigation_common_author" : "AOSP"
"library_androidx_navigation__navigation_fragment_author" : "AOSP"
"library_androidx_navigation__navigation_runtime_author" : "AOSP"
"library_androidx_print__print_author" : "AOSP"
"library_androidx_recyclerview__recyclerview_author" : "AOSP"
"library_androidx_room__room_common_author" : "AOSP"
"library_androidx_room__room_guava_author" : "AOSP"
"library_androidx_room__room_runtime_author" : "AOSP"
"library_androidx_savedstate__savedstate_author" : "AOSP"
"library_androidx_slice__slice_builders_author" : "AOSP"
"library_androidx_slice__slice_core_author" : "AOSP"

POSSIBLE SECRETS
"library_androidx_sqlite__sqlite_author" : "AOSP"
"library_androidx_sqlite__sqlite_framework_author" : "AOSP"
"library_androidx_transition__transition_author" : "AOSP"
"library_androidx_vectordrawable__vectordrawable_animated_author" : "AOSP"
"library_androidx_vectordrawable__vectordrawable_author" : "AOSP"
"library_androidx_viewpager2__viewpager2_author" : "AOSP"
"library_androidx_viewpager__viewpager_author" : "AOSP"
"library_androidx_work__work_runtime_author" : "AOSP"
"library_com_google_android__annotations_author" : "The Android Open Source Projects"
"library_com_google_android_datatransport__transport_api_libraryArtifactId" : "com.google.android.datatransport:transport-api:2.2.1"
"library_com_google_android_datatransport__transport_api_libraryDescription" : ""
"library_com_google_android_datatransport__transport_api_libraryName" : "transport-api"
"library_com_google_android_datatransport__transport_api_libraryVersion" : "2.2.1"
"library_com_google_android_datatransport__transport_api_licenseId" : "Apache_2_0"
"library_com_google_android_datatransport__transport_api_licenseIds" : "Apache_2_0"
"library_com_google_android_material__material_author" : "AOSP"
"library_com_google_auto_value__auto_value_annotations_author" : "Google LLC"
"library_com_google_auto_value__auto_value_annotations_authorWebsite" : "http://www.google.com"
"library_com_google_dagger__dagger_author" : "Google, Inc."
"library_com_google_dagger__dagger_authorWebsite" : "https://www.google.com"
"library_com_google_dagger__dagger_lint_aar_author" : "Google, Inc."
"library_com_google_dagger__dagger_lint_aar_authorWebsite" : "https://www.google.com"
"library_com_google_dagger__hilt_android_author" : "Google, Inc."
"library_com_google_dagger__hilt_android_authorWebsite" : "https://www.google.com"
"library_com_google_dagger__hilt_core_author" : "Google, Inc."
"library_com_google_dagger__hilt_core_authorWebsite" : "https://www.google.com"

POSSIBLE SECRETS
"library_com_google_firebase__firebase_auth_interop_libraryArtifactId" : "com.google.firebase:firebase-auth-interop:18.0.0"
"library_com_google_firebase__firebase_auth_interop_libraryDescription" : ""
"library_com_google_firebase__firebase_auth_interop_libraryName" : "firebase-auth-interop"
"library_com_google_firebase__firebase_auth_interop_libraryVersion" : "18.0.0"
"library_com_google_firebase__firebase_auth_interop_licenseId" : "ASDKL"
"library_com_google_firebase__firebase_auth_interop_licenseIds" : "ASDKL"
"library_com_google_firebase__firebase_common_libraryArtifactId" : "com.google.firebase:firebase-common:19.3.1"
"library_com_google_firebase__firebase_common_libraryDescription" : ""
"library_com_google_firebase__firebase_common_libraryName" : "firebase-common"
"library_com_google_firebase__firebase_common_libraryVersion" : "19.3.1"
"library_com_google_firebase__firebase_common_licenseId" : "Apache_2_0"
"library_com_google_firebase__firebase_common_licenseIds" : "Apache_2_0"
"library_com_google_firebase__firebase_components_libraryArtifactId" : "com.google.firebase:firebase-components:16.0.0"
"library_com_google_firebase__firebase_components_libraryDescription" : ""
"library_com_google_firebase__firebase_components_libraryName" : "firebase-components"
"library_com_google_firebase__firebase_components_libraryVersion" : "16.0.0"
"library_com_google_firebase__firebase_components_licenseId" : "Apache_2_0"
"library_com_google_firebase__firebase_components_licenseIds" : "Apache_2_0"
"library_com_google_firebase__firebase_database_collection_libraryArtifactId" : "com.google.firebase:firebase-database-collection:17.0.1"
"library_com_google_firebase__firebase_database_collection_libraryDescription" : ""
"library_com_google_firebase__firebase_database_collection_libraryName" : "firebase-database-collection"
"library_com_google_firebase__firebase_database_collection_libraryVersion" : "17.0.1"
"library_com_google_firebase__firebase_database_collection_licenseId" : "Apache_2_0"
"library_com_google_firebase__firebase_database_collection_licenseIds" : "Apache_2_0"
"library_com_google_firebase__firebase_datatransport_libraryArtifactId" : "com.google.firebase:firebase-datatransport:17.0.8"
"library_com_google_firebase__firebase_datatransport_libraryDescription" : ""

POSSIBLE SECRETS
"library_com_google_firebase__firebase_datatransport_libraryName" : "firebase-datatransport"
"library_com_google_firebase__firebase_datatransport_libraryVersion" : "17.0.8"
"library_com_google_firebase__firebase_datatransport_licenseId" : "Apache_2_0"
"library_com_google_firebase__firebase_datatransport_licenseIds" : "Apache_2_0"
"library_com_google_firebase__firebase_encoders_json_libraryArtifactId" : "com.google.firebase:firebase-encoders-json:16.1.0"
"library_com_google_firebase__firebase_encoders_json_libraryDescription" : ""
"library_com_google_firebase__firebase_encoders_json_libraryName" : "firebase-encoders-json"
"library_com_google_firebase__firebase_encoders_json_libraryVersion" : "16.1.0"
"library_com_google_firebase__firebase_encoders_json_licenseId" : "Apache_2_0"
"library_com_google_firebase__firebase_encoders_json_licenseIds" : "Apache_2_0"
"library_com_google_firebase__firebase_firestore_libraryArtifactId" : "com.google.firebase:firebase-firestore:21.6.0"
"library_com_google_firebase__firebase_firestore_libraryDescription" : ""
"library_com_google_firebase__firebase_firestore_libraryName" : "firebase-firestore"
"library_com_google_firebase__firebase_firestore_libraryVersion" : "21.6.0"
"library_com_google_firebase__firebase_firestore_licenseId" : "Apache_2_0"
"library_com_google_firebase__firebase_firestore_licenseIds" : "Apache_2_0"
"library_com_google_firebase__protolite_well_known_types_libraryArtifactId" : "com.google.firebase:protolite-well-known-types:17.1.0"
"library_com_google_firebase__protolite_well_known_types_libraryDescription" : ""
"library_com_google_firebase__protolite_well_known_types_libraryName" : "protolite-well-known-types"
"library_com_google_firebase__protolite_well_known_types_libraryVersion" : "17.1.0"
"library_com_google_firebase__protolite_well_known_types_licenseId" : "Apache_2_0"
"library_com_google_firebase__protolite_well_known_types_licenseIds" : "Apache_2_0"
"library_com_google_guava__failureaccess_author" : "Kevin Bourrillion"
"library_com_google_guava__failureaccess_authorWebsite" : "http://www.google.com"
"library_com_google_guava__guava_author" : "Kevin Bourrillion"
"library_com_google_guava__guava_authorWebsite" : "http://www.google.com"

POSSIBLE SECRETS
"library_com_google_guava__listenablefuture_author" : "Kevin Bourrillion"
"library_com_google_guava__listenablefuture_authorWebsite" : "http://www.google.com"
"library_com_google_protobuf__protobuf_javalite_author" : "Hao Nguyen"
"library_com_google_protobuf__protobuf_javalite_authorWebsite" : "https://cloud.google.com"
"library_com_googlecode_libphonenumber__libphonenumber_author" : "Shaopeng Jia, Lara Rennie"
"library_com_googlecode_libphonenumber__libphonenumber_authorWebsite" : "http://www.google.com/"
"library_com_jakewharton_threetenabp__threetenabp_author" : "Jake Wharton"
"library_com_mikepenz__aboutlibraries_core_author" : "Mike Penz"
"library_com_mikepenz__fastadapter_author" : "Mike Penz"
"library_com_squareup_okio__okio_author" : "Square, Inc"
"library_commons_io__commons_io_author" : "Scott Sanders, dlon Gillard, Nicola Ken Barozzi, Henri Yandell, Stephen Colebourne, Jeremias Maerki, Matt hew Hawthorne, Martin Cooper, Rob Oxspring, Jochen Wiedmann, Niall Pemberton, Jukka Zitting, Gary Gregory, Kristian Rosenvold"
"library_fastadapter_author" : "Mike Penz"
"library_fastadapter_authorWebsite" : "http://mikepenz.com/"
"library_io_grpc__grpc_android_author" : "gRPC Contributors"
"library_io_grpc__grpc_android_authorWebsite" : "https://www.google.com"
"library_io_grpc__grpc_api_author" : "gRPC Contributors"
"library_io_grpc__grpc_api_authorWebsite" : "https://www.google.com"
"library_io_grpc__grpc_api_isOpenSource" : "true"
"library_io_grpc__grpc_api_libraryArtifactId" : "io.grpc:grpc-api:1.28.0"
"library_io_grpc__grpc_api_libraryDescription" : "gRPC: API"
"library_io_grpc__grpc_api_libraryName" : "io.grpc:grpc-api"
"library_io_grpc__grpc_api_libraryVersion" : "1.28.0"
"library_io_grpc__grpc_api_libraryWebsite" : "https://github.com/grpc/grpc-java"
"library_io_grpc__grpc_api_licenseId" : "Apache_2_0"
"library_io_grpc__grpc_api_licenseIds" : "Apache_2_0"
"library_io_grpc__grpc_api_owner" : "gRPC Contributors"

POSSIBLE SECRETS
"library_io_grpc__grpc_api_repositoryLink" : "https://github.com/grpc/grpc-java"
"library_io_grpc__grpc_core_author" : "gRPC Contributors"
"library_io_grpc__grpc_core_authorWebsite" : "https://www.google.com"
"library_io_grpc__grpc_okhttp_author" : "gRPC Contributors"
"library_io_grpc__grpc_okhttp_authorWebsite" : "https://www.google.com"
"library_io_grpc__grpc_protobuf_lite_author" : "gRPC Contributors"
"library_io_grpc__grpc_protobuf_lite_authorWebsite" : "https://www.google.com"
"library_io_grpc__grpc_stub_author" : "gRPC Contributors"
"library_io_grpc__grpc_stub_authorWebsite" : "https://www.google.com"
"library_io_perfmark__perfmark_api_author" : "Carl Mastrangelo"
"library_io_perfmark__perfmark_api_isOpenSource" : "true"
"library_io_perfmark__perfmark_api_libraryArtifactId" : "io.perfmark:perfmark-api:0.19.0"
"library_io_perfmark__perfmark_api_libraryDescription" : "PerfMark API"
"library_io_perfmark__perfmark_api_libraryName" : "perfmark:perfmark-api"
"library_io_perfmark__perfmark_api_libraryVersion" : "0.19.0"
"library_io_perfmark__perfmark_api_libraryWebsite" : "https://github.com/perfmark/perfmark"
"library_io_perfmark__perfmark_api_licenseId" : "Apache_2_0"
"library_io_perfmark__perfmark_api_licenseIds" : "Apache_2_0"
"library_io_perfmark__perfmark_api_owner" : "Carl Mastrangelo"
"library_io_perfmark__perfmark_api_repositoryLink" : "https://github.com/perfmark/perfmark"
"library_org_checkerframework__checker_compat_qual_author" : "Michael Ernst, Werner M. Dietl, Suzanne Millstein"
"library_org_checkerframework__checker_compat_qual_authorWebsite" : "https://www.cs.washington.edu/, http://uwaterloo.ca/, https://www.cs.washington.edu/research/plse/"
"library_org_codehaus_mojo__animal_sniffer_annotations_author" : "Kohsuke Kaw, Stephen Connolly"
"library_org_jetbrains__annotations_author" : "JetBrains Team"
"library_org_jetbrains__annotations_authorWebsite" : "http://www.jetbrains.com"
"library_org_jetbrains_kotlin__kotlin_android_extensions_runtime_author" : "Kotlin Team"

POSSIBLE SECRETS
"library_org_jetbrains_kotlin__kotlin_android_extensions_runtime_authorWebsite" : "https://www.jetbrains.com"
"library_org_jetbrains_kotlin__kotlin_stdlib_author" : "Kotlin Team"
"library_org_jetbrains_kotlin__kotlin_stdlib_authorWebsite" : "https://www.jetbrains.com"
"library_org_jetbrains_kotlin__kotlin_stdlib_common_author" : "Kotlin Team"
"library_org_jetbrains_kotlin__kotlin_stdlib_common_authorWebsite" : "https://www.jetbrains.com"
"library_org_jetbrains_kotlin__kotlin_stdlib_jdk7_author" : "Kotlin Team"
"library_org_jetbrains_kotlin__kotlin_stdlib_jdk7_authorWebsite" : "https://www.jetbrains.com"
"library_org_jetbrains_kotlin__kotlin_stdlib_jdk8_author" : "Kotlin Team"
"library_org_jetbrains_kotlin__kotlin_stdlib_jdk8_authorWebsite" : "https://www.jetbrains.com"
"library_org_threeten__threetenbp_author" : "Stephen Colebourne"
"library_org_threeten__threetenbp_authorWebsite" : "https://www.threeten.org"
"private_analytics_footer" : "These analytics, such as the number of notifications in your region, help health authorities understand how COVID-19 spread s. They can’t be read by Google and are aggregated for your health authority so they can’t be linked to your phone. %1$s"
"private_analytics_footer_learn_more" : "Learn more"
"private_analytics_footer_onboarding" : "These analytics can’t be read by Google and are aggregated for your health authority so they can’t be linked to yo ur phone. %1$s"
"private_analytics_link" : "https://support.google.com/android?p=en_analytics"
"private_analytics_subtitle" : "Share Exposure Notifications analytics with your health authority"
"private_analytics_title" : "Help your health authority understand the spread of COVID-19"
"settings_private_analytics_subtitle" : "Exposure Notifications analytics sharing"

PLAYSTORE INFORMATION

Title: CO Exposure Notifications

Score: 3.76 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** 5.0 and up **Category:** Medical **Play Store URL:** gov.co.cdphe.exposurenotifications

Developer Details: Colorado Department of Public Health & Environment, Colorado+Department+of+Public+Health+%26+Environment, None, https://covid19.colorado.gov/Exposure-notifications, CO_Exposure_Notifications@state.co.us,

Release Date: Oct 16, 2020 **Privacy Policy:** Privacy link

Description:

CO Exposure Notifications is the official Exposure Notifications app of Colorado and the Colorado Department of Public Health and Environment. Exposure Notifications is a voluntary new service developed in partnership with Google and Apple to help slow the spread of COVID-19. No GPS, location information or personal identifiers will ever be collected, stored or shared by this service. CO Exposure Notifications can quickly notify you if you've likely been exposed to COVID-19. Knowing about a potential exposure allows you to reduce the risk to your family, friends, neighbors and community. By enabling Exposure

Notifications, whenever you are within 6 feet of someone for at least 10 minutes, both phones will exchange secure, anonymous tokens using Bluetooth. If another user you've been near tests positive for COVID-19, they can upload their result to the app which will send a push notification to you and anyone else their phone has exchanged tokens with recently, notifying you to a possible exposure. If you test positive, you can easily and anonymously notify others to help stop the spread of COVID-19. To learn more, please visit https://covid19.colorado.gov/Exposure-notifications

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.