

ANDROID STATIC ANALYSIS REPORT



MD COVID Alert (minted1100011)

File Name: MD COVID Alert_vminted1100011_apkpure.com.xapk

Package Name: gov.md.covid19.exposurenotifications

Average CVSS Score: 0

App Security Score: 100/100 (LOW RISK)

Scan Date: Feb. 20, 2022, 5:54 p.m.



File Name: MD COVID Alert_vminted1100011_apkpure.com.xapk

Size: 3.73MB

MD5: ecdae9c59767307b623cc388e72bf101

SHA1: 18a96674d20c39de27ff4caffafc6e17d76ffa91

SHA256: 0729b753dd99220a5028df9c6edfdc3329dd02ae2d085914dbf9a58743b9ae7a

i APP INFORMATION

App Name: MD COVID Alert

Package Name: gov.md.covid19.exposurenotifications

Main Activity: com.google.android.apps.exposurenotification.home.ExposureNotificationActivity

Target SDK: 31 Min SDK: 21 Max SDK:

Android Version Name: minted1100011
Android Version Code: 11000112

EE APP COMPONENTS

Activities: 4 Services: 8 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: 2020-10-28 23:37:41+00:00 Valid To: 2050-10-28 23:37:41+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0x6605dd6c514b98f7e6de7313f5ed83e5127aeaaa

Hash Algorithm: sha256

md5: 62b187cb0c274c5b7df0bc7b1bbb6999

sha1: 6430ff9cd6342273d6d5df8fe81c993c24a3d215

sha256: 88c7ed9eb63dbac119125d843ffe8287e16744910dfef592f311e0a66abc8ae2

sha512: 96e89c63dd9891525a54600feacbe55993a1ee6b257aa2eca1bb72d017de8c397b15e8f5a24805a5348ba8251e5d6097b073e6df28d1453633e251774cf3a154

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: a64ebb036f8cb76ba797a45a16b8fe27fd1948d6ff58ed8c017e8a6aa909bc7f

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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
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	
	FINDINGS	DETAILS
classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check
	Compiler	r8



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

△ NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

Q 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.

NO	ISSUE	SEVERITY	DESCRIPTION
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.
3	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
4	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.
5	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
6	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

FILES	SEVERITY	ISSUE	NO	
		SEVERITY	ISSUE SEVERITY	NO ISSUE SEVERITY

■ NIAP ANALYSIS v1.3

NO IDENTIFIER REQUIREMENT FEATURE DESCRIPTION

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
cs.android.com	good	IP: 142.250.217.78 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.jetbrains.org	good	IP: 65.8.68.36 Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map
android.git.kernel.org	good	No Geolocation information available.
prod.exposurenotification.health	good	IP: 13.107.246.70 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
spdx.org	good	IP: 13.227.65.104 Country: United States of America Region: California City: San Francisco Latitude: 37.774929 Longitude: -122.419418 View: Google Map

DOMAIN	STATUS	GEOLOCATION
code.google.com	good	IP: 142.251.33.78 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
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
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
health.maryland.gov	good	IP: 167.102.44.35 Country: United States of America Region: Maryland City: Annapolis Latitude: 39.004379 Longitude: -76.507141 View: Google Map

DOMAIN	STATUS	GEOLOCATION
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
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.jetbrains.com	good	IP: 52.37.61.85 Country: United States of America Region: Oregon City: Portland Latitude: 45.523449 Longitude: -122.676208 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

Т

DOMAIN	STATUS	GEOLOCATION
kotlinlang.org	good	IP: 65.8.68.4 Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map
schemas.android.com	good	No Geolocation information available.
g.co	good	IP: 172.217.14.238 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 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
support.google.com	good	IP: 142.250.217.78 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
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
uwaterloo.ca	good	IP: 151.101.130.133 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
cloud.google.com	good	IP: 142.251.33.110 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
github.com	good	IP: 140.82.112.4 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.google.com	good	IP: 172.217.14.228 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
plus.google.com	good	IP: 142.250.217.110 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 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
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

DOMAIN	STATUS	GEOLOCATION
www.gstatic.com	good	IP: 142.250.217.99 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
encdn.prod.exposurenotification.health	good	IP: 104.212.67.109 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
covidlink.maryland.gov	good	IP: 3.135.81.88 Country: United States of America Region: Ohio City: Columbus Latitude: 39.961182 Longitude: -82.998787 View: Google Map

DOMAIN	STATUS	GEOLOCATION
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
coronavirus.maryland.gov	good	IP: 52.86.108.135 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
tools.android.com	good	IP: 142.251.33.115 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
developer.android.com	good	IP: 142.250.217.78 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

Т

DOMAIN	STATUS	GEOLOCATION
play.google.com	good	IP: 172.217.14.238 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
source.android.com	good	IP: 142.250.217.78 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map



URL	FILE
http://schemas.android.com/apk/res/android	e/b/a/m.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	

nttps://covidlink.maryland.gov/content/mdcovidalert/privacy-policy/	FILE	
https://covidlink.maryland.gov/content/mdcovidalert/alerted/	1125	
https://www.gstatic.com/prio-manifests/gov.md.covid19.exposurenotifications.config.json		
nttps://health.maryland.gov/mdcovidalert/Pages/Home.aspx		
https://coronavirus.maryland.gov/pages/contact-tracing		
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		
nttps://apiserver.encv.org/api/verify		
https://health.maryland.gov/mdcovidalert/		
https://support.google.com/googleplay/answer/9037938		
nttps://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#1.2.4		
https://cs.android.com/androidx/platform/frameworks/support		
https://developer.android.com/jetpack/androidx/releases/annotation#1.1.0		
https://developer.android.com/jetpack/androidx/releases/annotation#1.3.0-alpha01		
https://developer.android.com/jetpack/androidx/releases/appcompat#1.4.0-alpha03		
https://developer.android.com/topic/libraries/architecture/index.html		
http://source.android.com		
http://developer.android.com/tools/extras/support-library.html		
http://tools.android.com		
https://github.com/androidx/constraintlayout		
attps://developer.android.com/jetpack/androidx		
https://developer.android.com/jetpack/androidx/releases/core#1.7.0-alpha01		
https://developer.android.com/jetpack/androidx/releases/emoji2#1.0.0-alpha03		
https://developer.android.com/jetpack/androidx/releases/fragment#1.3.6		
https://developer.android.com/jetpack/androidx/releases/hilt#1.0.0		
https://developer.android.com/jetpack/androidx/releases/hilt#1.0.0-alpha03		
ttps://developer.android.com/jetpack/androidx/releases/lifecycle#2.4.0-alpha02		
https://developer.android.com/jetpack/androidx/releases/lifecycle#2.3.1		
data:2.1.0		
https://developer.android.com/jetpack/androidx/releases/resourceinspection#1.0.0-alpha03		
nttps://developer.android.com/jetpack/androidx/releases/savedstate#1.1.0		
nttps://developer.android.com/jetpack/androidx/releases/startup#1.0.0		
nttps://developer.android.com/jetpack/androidx/releases/work#2.7.0-rc01		

http://source.android.com/	
btRt://android.git.kernel.org/	FILE
https://github.com/material-components/material-components-android	
http://www.google.com	Android String Resource
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/google/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	
btfks://www.threeten.org/threetenbp	FILE
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

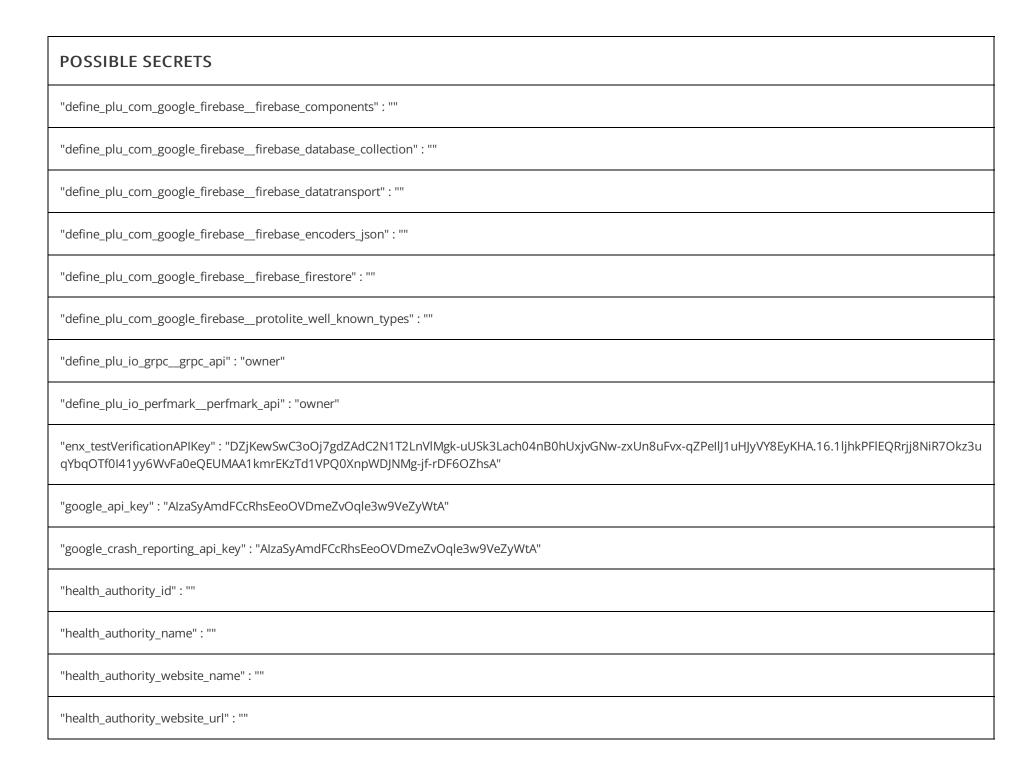
https://support.google.com/android?p=enxsms



EMAIL	FILE
u0013android@android.com0 u0013android@android.com	f/b/a/c/b/y.java

HARDCODED SECRETS

POSSIBLE SECRETS
"define_plu_com_google_android_datatransport_transport_api" : ""
"define_plu_com_google_firebasefirebase_auth_interop" : ""
"define_plu_com_google_firebasefirebase_common" : ""



POSSIBLE SECRETS
"library_AboutLibraries_author" : "Mike Penz"
"library_AboutLibraries_authorWebsite" : "http://mikepenz.com/"
"library_androidx_annotationannotation_author" : "AOSP"
"library_androidx_annotationannotation_experimental_author" : "AOSP"
"library_androidx_appcompat_appcompat_author" : "AOSP"
"library_androidx_appcompatappcompat_resources_author" : "AOSP"
"library_androidx_arch_corecore_common_author" : "AOSP"
"library_androidx_arch_corecore_runtime_author" : "AOSP"
"library_androidx_cardviewcardview_author" : "AOSP"
"library_androidx_collectioncollection_author" : "AOSP"
"library_androidx_constraintlayout_constraintlayout_author" : "AOSP"
"library_androidx_constraintlayout_constraintlayout_core_author" : "AOSP"
"library_androidx_coordinatorlayout_coordinatorlayout_author" : "AOSP"
"library_androidx_corecore_author" : "AOSP"
"library_androidx_corecore_ktx_author" : "AOSP"

POSSIBLE SECRETS
"library_androidx_cursoradapter_cursoradapter_author" : "AOSP"
"library_androidx_customviewcustomview_author" : "AOSP"
"library_androidx_documentfiledocumentfile_author" : "AOSP"
"library_androidx_drawerlayoutdrawerlayout_author" : "AOSP"
"library_androidx_dynamicanimationdynamicanimation_author" : "AOSP"
"library_androidx_emoji2emoji2_author" : "AOSP"
"library_androidx_emoji2emoji2_views_helper_author" : "AOSP"
"library_androidx_fragment_fragment_author" : "AOSP"
"library_androidx_hilthilt_common_author" : "AOSP"
"library_androidx_hilthilt_lifecycle_viewmodel_author" : "AOSP"
"library_androidx_hilthilt_work_author" : "AOSP"
"library_androidx_interpolator_interpolator_author" : "AOSP"
"library_androidx_legacylegacy_support_core_utils_author" : "AOSP"
"library_androidx_lifecyclelifecycle_common_author" : "AOSP"
"library_androidx_lifecyclelifecycle_livedata_author" : "AOSP"

POSSIBLE SECRETS
"library_androidx_lifecyclelifecycle_livedata_core_author" : "AOSP"
"library_androidx_lifecyclelifecycle_process_author" : "AOSP"
"library_androidx_lifecyclelifecycle_runtime_author" : "AOSP"
"library_androidx_lifecyclelifecycle_service_author" : "AOSP"
"library_androidx_lifecyclelifecycle_viewmodel_author" : "AOSP"
"library_androidx_lifecyclelifecycle_viewmodel_savedstate_author" : "AOSP"
"library_androidx_loader_loader_author" : "AOSP"
"library_androidx_localbroadcastmanagerlocalbroadcastmanager_author" : "AOSP"
"library_androidx_navigation_navigation_common_author" : "AOSP"
"library_androidx_navigationnavigation_fragment_author" : "AOSP"
"library_androidx_navigation_navigation_runtime_author" : "AOSP"
"library_androidx_printprint_author" : "AOSP"
"library_androidx_recyclerviewrecyclerview_author" : "AOSP"
"library_androidx_resourceinspection_resourceinspection_annotation_author" : "AOSP"
"library_androidx_roomroom_common_author" : "AOSP"

POSSIBLE SECRETS	
"library_androidx_roomroom_guava_author" : "AOSP"	
"library_androidx_roomroom_runtime_author" : "AOSP"	
"library_androidx_savedstatesavedstate_author" : "AOSP"	
"library_androidx_sliceslice_builders_author" : "AOSP"	
"library_androidx_sliceslice_core_author" : "AOSP"	
"library_androidx_sqlitesqlite_author" : "AOSP"	
"library_androidx_sqlitesqlite_framework_author" : "AOSP"	
"library_androidx_startupstartup_runtime_author" : "AOSP"	
"library_androidx_transition_transition_author" : "AOSP"	
"library_androidx_vectordrawablevectordrawable_animated_author" : "AOSP"	
"library_androidx_vectordrawablevectordrawable_author" : "AOSP"	
"library_androidx_viewpager2viewpager2_author" : "AOSP"	
"library_androidx_viewpagerviewpager_author" : "AOSP"	
"library_androidx_workwork_runtime_author" : "AOSP"	
"library_com_google_androidannotations_author" : "The Android Open Source Projects"	

POSSIBLE SECRETS "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_licenseld": "Apache_2_0" "library com google android datatransport transport api licenselds": "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"

POSSIBLE SECRETS "library_com_google_dagger__hilt_core_author": "Google, Inc." "library_com_google_dagger__hilt_core_authorWebsite": "https://www.google.com" "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_licenseld": "ASDKL" "library_com_google_firebase__firebase_auth_interop_licenselds": "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_licenseld": "Apache_2_0" "library_com_google_firebase__firebase_common_licenselds": "Apache_2_0" "library com google firebase firebase components libraryArtifactId": "com.google.firebase:firebase-components:16.0.0"

POSSIBLE SECRETS "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_licenseld": "Apache_2_0" "library_com_google_firebase__firebase_components_licenselds": "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_licenseld": "Apache_2_0" "library com google firebase firebase database collection licenselds": "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": "" "library_com_google_firebase__firebase_datatransport_libraryName": "firebase-datatransport" "library com google firebase firebase datatransport library Version": "17.0.8"

POSSIBLE SECRETS "library_com_google_firebase__firebase_datatransport_licenseld": "Apache_2_0" "library_com_google_firebase__firebase_datatransport_licenselds": "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_ison_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_licenseld": "Apache_2_0" "library_com_google_firebase_firebase_encoders_json_licenselds": "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_licenseld": "Apache_2_0" "library_com_google_firebase_firebase_firestore_licenselds": "Apache_2_0" "library com google firebase protolite well known types libraryArtifactId": "com.google.firebase:protolite-well-known-types:17.1.0"

POSSIBLE SECRETS		
"library_com_google_firebaseprotolite_well_known_types_libraryDescription" : ""		
"library_com_google_firebaseprotolite_well_known_types_libraryName" : "protolite-well-known-types"		
"library_com_google_firebaseprotolite_well_known_types_libraryVersion" : "17.1.0"		
"library_com_google_firebaseprotolite_well_known_types_licenseld" : "Apache_2_0"		
"library_com_google_firebaseprotolite_well_known_types_licenselds" : "Apache_2_0"		
"library_com_google_guavafailureaccess_author" : "Kevin Bourrillion"		
"library_com_google_guavafailureaccess_authorWebsite" : "http://www.google.com"		
"library_com_google_guavaguava_author" : "Kevin Bourrillion"		
"library_com_google_guavaguava_authorWebsite" : "http://www.google.com"		
"library_com_google_guavalistenablefuture_author" : "Kevin Bourrillion"		
"library_com_google_guavalistenablefuture_authorWebsite" : "http://www.google.com"		
"library_com_google_protobuf_protobuf_javalite_author" : "Hao Nguyen"		
"library_com_google_protobufprotobuf_javalite_authorWebsite" : "https://cloud.google.com"		
"library_com_googlecode_libphonenumberlibphonenumber_author" : "Shaopeng Jia, Lara Rennie"		
"library_com_googlecode_libphonenumberlibphonenumber_authorWebsite" : "http://www.google.com/"		

POSSIBLE SECRETS "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, Matthew Hawthorn e, 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"

POSSIBLE SECRETS
"library_io_grpc_grpc_api_libraryVersion" : "1.28.0"
"library_io_grpcgrpc_api_libraryWebsite" : "https://github.com/grpc/grpc-java"
"library_io_grpc_grpc_api_licenseld" : "Apache_2_0"
"library_io_grpc_grpc_api_licenselds" : "Apache_2_0"
"library_io_grpc_grpc_api_owner" : "gRPC Contributors"
"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_grpcgrpc_stub_author" : "gRPC Contributors"
"library_io_grpc_grpc_stub_authorWebsite" : "https://www.google.com"
"library_io_perfmarkperfmark_api_author" : "Carl Mastrangelo"

POSSIBLE SECRETS
"library_io_perfmarkperfmark_api_isOpenSource" : "true"
"library_io_perfmarkperfmark_api_libraryArtifactld" : "io.perfmark:perfmark-api:0.19.0"
"library_io_perfmarkperfmark_api_libraryDescription" : "PerfMark API"
"library_io_perfmarkperfmark_api_libraryName" : "perfmark:perfmark-api"
"library_io_perfmarkperfmark_api_libraryVersion" : "0.19.0"
"library_io_perfmarkperfmark_api_libraryWebsite" : "https://github.com/perfmark/perfmark"
"library_io_perfmarkperfmark_api_licenseld" : "Apache_2_0"
"library_io_perfmarkperfmark_api_licenselds" : "Apache_2_0"
"library_io_perfmarkperfmark_api_owner" : "Carl Mastrangelo"
"library_io_perfmarkperfmark_api_repositoryLink" : "https://github.com/perfmark/perfmark"
"library_org_checkerframeworkchecker_compat_qual_author" : "Michael Ernst, Werner M. Dietl, Suzanne Millstein"
"library_org_checkerframeworkchecker_compat_qual_authorWebsite" : "https://www.cs.washington.edu/, http://uwaterloo.ca/, https://www.cs.washington.edu/rese arch/plse/"
"library_org_codehaus_mojoanimal_sniffer_annotations_author" : "Kohsuke Kaw, Stephen Connolly"
"library_org_jetbrainsannotations_author" : "JetBrains Team"
"library_org_jetbrainsannotations_authorWebsite" : "http://www.jetbrains.com"

POSSIBLE SECRETS "library_org_jetbrains_kotlin__kotlin_android_extensions_runtime_author": "Kotlin Team" "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 spreads. They can't b e 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 your phone. %1

\$s"

POSSIBLE SECRETS

"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: MD COVID Alert

Score: 3.4 Installs: 100,000+ Price: 0 Android Version Support: 5.0 and up Category: Medical Play Store URL: gov.md.covid19.exposurenotifications

Developer Details: Maryland Department of Health, Maryland+Department+of+Health, None, None, MDH.MDCOVIDAlert@maryland.gov,

Release Date: Nov 3, 2020 Privacy Policy: Privacy link

Description:

MD COVID Alert is the official COVID-19 exposure-notifications software for the Maryland Department of Health. The app is an instance of Exposure Notifications Express platform developed by Apple and Google and configured by Maryland. Your personal use of MD COVID Alert will help anonymously alert Maryland residents who may have been near someone with a positive COVID-19 diagnosis. When you enable MD COVID Alert, you are doing your part to efficiently and effectively help your community slow the spread of COVID-19. How MD COVID Alert works: When devices with MD COVID Alert are in close contact, they exchange random identifiers using Bluetooth Low Energy (BLE). When someone tells their app that they tested positive for COVID-19, whoever received their random identifiers may receive an alert that they may have possibly been exposed to COVID-19. When a device receives random identifiers it date-stamps them and records their signal strength so that the Exposure Notification system can estimate how close the two devices were to each other and for how long. If the timeframe was at least 15 minutes and the estimated distance was within six feet, then the other user receives a notification of a possible exposure. Apple and Google's Exposure Notifications framework runs in the background, even when the MD COVID Alert app is closed. It will not drain the device battery at a rate that would occur with other apps that use normal Bluetooth and/or are open and running constantly. How MD COVID Alert Protects Your Privacy: Maryland takes your privacy and confidentiality very seriously. Apple and Google's framework is designed to avoid correlating any personal data and location information with the random identifiers that devices exchange. Maryland Department of Health does not want or need to know where or who you are for MD

COVID Alert to work. If you are close enough to another app user, your device's BLE will exchange random identifiers with that user. Laboratory results for all persons who test positive for COVID-19 are sent to Maryland Department of Health. This is not associated with the app. Our staff follows up with persons reported as positive, based on information provided within the laboratory report. As a courtesy to all app users, MD COVID ALert will verify positive tests and then provide MD COVID Alert users with a personal identifying number (PIN). You must use that PIN in order to report a positive result to the app. This prevents people from falsely reporting positive results, which could generate false exposure notifications. Maryland Department of Health wants all app users to feel confident that when a possible COVID-19 exposure is received via the app, that it is a real event. If you have the current Apple or Google operating system installed on your device, you may have noticed that Exposure Notifications are now included. You cannot enable this function until you have installed the MD COVID Alert app. Apple and Google will delete the exposure notification service tools from their respective operating systems once the pandemic reaches a point that public health no longer requires the use of this technology. Thank you for installing MD COVID Alert! Together, we can protect our family, friends, neighbors, and colleagues, and keep Maryland moving forward!

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.

© 2022 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.