

ANDROID STATIC ANALYSIS REPORT



WI Exposure Notification (minted1100011) File Name: WI Exposure Notification_vminted1100011_apkpure.com.xapk

Package Name: gov.wi.covid19.exposurenotifications

Average CVSS Score: 0

App Security Score: 100/100 (LOW RISK)

Scan Date: Feb. 20, 2022, 6:29 p.m.



File Name: WI Exposure Notification_vminted1100011_apkpure.com.xapk

Size: 3.6MB

MD5: 6f0c1dfefbe03dd7283f0acb8975daba

SHA1: 241a4bfe87ec5598e9796d5e0e0159bcb32b547d

SHA256: c79700c3670cbd5b34279c0ead414cb878d15863ab5a7be3dd4788ca6495c3a9

i APP INFORMATION

App Name: WI Exposure Notification

Package Name: gov.wi.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: 2020-12-09 23:29:32+00:00 Valid To: 2050-12-09 23:29:32+00:00

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

Serial Number: 0x146950243e436f205af464b7b975a61a3f7ba486

Hash Algorithm: sha256

md5: 572ee2b3302b8198828de574a7121cde

sha1: 56af2697b0ec10bd5a175e4e32a4d044a02bcf1c

sha256: f3e7d1752b302813da92a62402f1d1542a8050e663f8ca2820488b8ce5c3ad75

sha512: 8d110998380b53bb25b1a3287da060c858d65437e44d81f4a5996eda93fc5e12e71f94542a61e30bdda7921971a45c44eccc0709ccd6067bb16ba51b7d7698f8

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: a3d2635f5e8d3d5f77f294349042a702f28183ee5a8e33944851e38f47b86df8

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.

E 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-wi.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: 142.251.33.78 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: 13.35.122.32 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: 172.217.14.238 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
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

DOMAIN	STATUS	GEOLOCATION
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: 104.21.27.65 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
kotlinlang.org	good	IP: 65.8.68.111 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.

DOMAIN	STATUS	GEOLOCATION
g.co	good	IP: 172.217.14.206 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: 142.250.69.206 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

Т

DOMAIN	STATUS	GEOLOCATION
uwaterloo.ca	good	IP: 151.101.194.133 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
cloud.google.com	good	IP: 142.251.33.78 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
github.com	good	IP: 140.82.112.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
dhs.wisconsin.gov	good	IP: 165.189.157.136 Country: United States of America Region: Wisconsin City: Madison Latitude: 43.075230 Longitude: -89.380402 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.google.com	good	IP: 142.250.217.100 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
www.dhs.wisconsin.gov	good	IP: 165.189.157.136 Country: United States of America Region: Wisconsin City: Madison Latitude: 43.075230 Longitude: -89.380402 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

DOMAIN	STATUS	GEOLOCATION
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: 172.217.14.195 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
raw.githubusercontent.com	good	IP: 185.199.108.133 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map
encdn.prod.exposurenotification.health	good	IP: 104.212.67.108 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 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
tools.android.com	good	IP: 142.250.217.115 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
developer.android.com	good	IP: 172.217.14.238 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
play.google.com	good	IP: 142.250.69.206 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
source.android.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



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 https://www.dhs.wisconsin.gov/covid-19/app-privacy.htm https://www.dhs.wisconsin.gov/covid-19/index.htm https://dhs.wisconsin.gov/covid-19/notification.htm https://www.gstatic.com/prio-manifests/gov.wi.covid19.exposurenotifications.config.json https://www.dhs.wisconsin.gov/covid-19/close-contacts.htm https://www.dhs.wisconsin.gov/covid-19/symptoms.htm 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	
btRt://apiserver.encv.org/api/verify	FILE
https://www.dhs.wisconsin.gov/covid-19/notification.htm	
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#1.2.4	
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	
https://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	
https://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	
https://developer.android.com/jetpack/androidx/releases/savedstate#1.1.0	
https://developer.android.com/jetpack/androidx/releases/startup#1.0.0	
https://developer.android.com/jetpack/androidx/releases/work#2.7.0-rc01	
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	Android String Resource
http://github.com/google/auto	
http://findbugs.sourceforge.net/	
https://code.google.com/p/jsr-305/	
https://www.google.com	

harman Helling harman and the area	
https://github.com/google/dagger	FILE
blast//github.com/google/dagger/	FILE
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	
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	
btR1/opensource.org/licenses/MIT	FILE
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
exposurenotification@dhs.wisconsin	Android String Resource

HARDCODED SECRETS

POSSIBLE SECRETS
"define_plu_com_google_android_datatransporttransport_api" : ""
"define_plu_com_google_firebasefirebase_auth_interop" : ""
"define_plu_com_google_firebasefirebase_common" : ""
"define_plu_com_google_firebasefirebase_components" : ""
"define_plu_com_google_firebasefirebase_database_collection" : ""
"define_plu_com_google_firebasefirebase_datatransport" : ""



POSSIBLE SECRETS
"library_androidx_annotation_annotation_experimental_author" : "AOSP"
"library_androidx_appcompat_appcompat_author" : "AOSP"
"library_androidx_appcompat_appcompat_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"
"library_androidx_cursoradapter_cursoradapter_author" : "AOSP"
"library_androidx_customviewcustomview_author" : "AOSP"
"library_androidx_documentfiledocumentfile_author" : "AOSP"

POSSIBLE SECRETS
"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"
"library_androidx_lifecyclelifecycle_livedata_core_author" : "AOSP"
"library_androidx_lifecyclelifecycle_process_author" : "AOSP"
"library_androidx_lifecyclelifecycle_runtime_author" : "AOSP"

POSSIBLE SECRETS
"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_navigation_navigation_fragment_author" : "AOSP"
"library_androidx_navigation_navigation_runtime_author" : "AOSP"
"library_androidx_printprint_author" : "AOSP"
"library_androidx_recyclerviewrecyclerview_author" : "AOSP"
"library_androidx_resourceinspectionresourceinspection_annotation_author" : "AOSP"
"library_androidx_roomroom_common_author" : "AOSP"
"library_androidx_roomroom_guava_author" : "AOSP"
"library_androidx_roomroom_runtime_author" : "AOSP"
"library_androidx_savedstatesavedstate_author" : "AOSP"

POSSIBLE SECRETS
"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"
"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"

POSSIBLE SECRETS		
"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_materialmaterial_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_daggerdagger_author" : "Google, Inc."		
"library_com_google_daggerdagger_authorWebsite" : "https://www.google.com"		
"library_com_google_daggerdagger_lint_aar_author" : "Google, Inc."		
"library_com_google_daggerdagger_lint_aar_authorWebsite" : "https://www.google.com"		
"library_com_google_daggerhilt_android_author" : "Google, Inc."		
"library_com_google_daggerhilt_android_authorWebsite" : "https://www.google.com"		
"library_com_google_daggerhilt_core_author" : "Google, Inc."		
"library_com_google_daggerhilt_core_authorWebsite" : "https://www.google.com"		
"library_com_google_firebasefirebase_auth_interop_libraryArtifactId" : "com.google.firebase:firebase-auth-interop:18.0.0"		

POSSIBLE SECRETS "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" "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"

POSSIBLE SECRETS "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_libraryVersion": "17.0.8" "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"

POSSIBLE SECRETS "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_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" "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"

POSSIBLE SECRETS	
"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_guava_guava_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_protobuf_protobuf_javalite_authorWebsite" : "https://cloud.google.com"	
"library_com_googlecode_libphonenumber_libphonenumber_author" : "Shaopeng Jia, Lara Rennie"	
"library_com_googlecode_libphonenumberlibphonenumber_authorWebsite" : "http://www.google.com/"	
"library_com_jakewharton_threetenabpthreetenabp_author" : "Jake Wharton"	
"library_com_mikepenzaboutlibraries_core_author" : "Mike Penz"	
"library_com_mikepenzfastadapter_author" : "Mike Penz"	

POSSIBLE SECRETS "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" "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_licenseld": "Apache_2_0"

POSSIBLE SECRETS
"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_grpcgrpc_core_author" : "gRPC Contributors"
"library_io_grpcgrpc_core_authorWebsite" : "https://www.google.com"
"library_io_grpcgrpc_okhttp_author" : "gRPC Contributors"
"library_io_grpcgrpc_okhttp_authorWebsite" : "https://www.google.com"
"library_io_grpcgrpc_protobuf_lite_author" : "gRPC Contributors"
"library_io_grpcgrpc_protobuf_lite_authorWebsite" : "https://www.google.com"
"library_io_grpcgrpc_stub_author" : "gRPC Contributors"
"library_io_grpcgrpc_stub_authorWebsite" : "https://www.google.com"
"library_io_perfmarkperfmark_api_author" : "Carl Mastrangelo"
"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"

POSSIBLE SECRETS "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_licenseld": "Apache_2_0" "library_io_perfmark__perfmark_api_licenselds": "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/rese arch/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" "library_org_jetbrains_kotlin__kotlin_android_extensions_runtime_authorWebsite": "https://www.jetbrains.com" "library_org_jetbrains_kotlin_kotlin_stdlib_author": "Kotlin Team"

POSSIBLE SECRETS "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 \$5" "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"

POSSIBLE SECRETS

"settings_private_analytics_subtitle": "Exposure Notifications analytics sharing"



> PLAYSTORE INFORMATION

Title: WI Exposure Notification

Score: 3.2376237 Installs: 100,000+ Price: 0 Android Version Support: 5.0 and up Category: Medical Play Store URL: gov.wi.covid19.exposurenotifications

Developer Details: State of Wisconsin - Department of Health Services, State+of+Wisconsin+-+Department+of+Health+Services, None, None,

exposure.notifications.wi@gmail.com,

Release Date: Dec 21, 2020 Privacy Policy: Privacy link

Description:

WI Exposure Notification is the official COVID-19 exposure notification app in the State of Wisconsin supported by the Wisconsin Department of Health Services (WI DHS). WI Exposure Notification helps to contain the spread of COVID-19 by complementing the ongoing contact tracing programs carried out by the local and tribal public health agencies and DHS. Using WI Exposure Notification is voluntary and free of charge. It was built with your privacy and security in mind. The more people who install and use the app, the more effectively it can be in helping us contain the virus. Once you install and activate WI Exposure Notification and turn on Bluetooth, the app works in the background and exchanges anonymous signals with other devices. These signals, or keys, are long random strings of characters that are not tied to any personal information. Devices with the app installed will remember the keys generated by other devices nearby. The app will also record the signal strength, which is used to estimate the distance between two devices, as well as the duration and date of the exposure. To protect users' privacy, these keys are only kept on the user's own device. After 14 days, the keys are deleted. If a WI Exposure Notification user tests positive for COVID-19, they will receive a verification code from the State of Wisconsin. Users must activate the verification code that is only available from the State of Wisconsin in order to report a positive result via the app. This prevents people from falsely reporting positive results, which could generate false exposure notifications. WI DHS 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 to be trusted. When users choose to share a positive test result, this notifies other app users that were close enough to the infected person for a long enough period of time (approximately within 6 feet of someone for at least 15 minutes in a single day) that they are considered a close contact and at risk of infection. Anyone who receives a notification should follow the guidance in the app for next steps. WI DHS takes your privacy and confidentiality very seriously. This is why we chose to use the Apple and Google Exposure Notification API. No personal data or location tracking occurs within this app. WI DHS does not need to know where or who you are for WI Exposure Notification to work. The Wisconsin COVID Notice Privacy Policy is available at https://www.dhs.wisconsin.gov/covid-19/app-privacy.htm. Please note that WI Exposure Notification is intended for users ages 18 and up. The app was developed using the Google Apple Exposure Notification API through a collaboration between Google, Apple, and the Wisconsin Department of Health Services.

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.