ANDROID STATIC ANALYSIS REPORT

Covid Watch Arizona (2.1.11)

File Name:	gov.azdhs.covidwatch.android_2.1.11-201011_minAPI23(nodpi)_apkmirror.com.apk
Package Name:	gov.azdhs.covidwatch.android
Average CVSS Score:	0
App Security Score:	100/100 (LOW RISK)
Trackers Detection:	1/421
Scan Date:	Feb. 20, 2022, 5:16 p.m.

FILE INFORMATION

File Name: gov.azdhs.covidwatch.android_2.1.11-201011_minAPI23(nodpi)_apkmirror.com.apk
Size: 7.68MB
MD5: 6cfddf009c6e63792ab88c7ad487c2bd

SHA1: 7d2b24bfde7fed7f7105490bc07132a31df10a00
SHA256: ef37821c2c8e5fd6c01a138a8a02e7515382fc7c19b144fee312b6e8e08ccdfc

APP INFORMATION

App Name: Covid Watch Arizona
Package Name: gov.azdhs.covidwatch.android
Main Activity: org.covidwatch.android.ui.MainActivity
Target SDK: 30
Min SDK: 23
Max SDK:
Android Version Name: 2.1.11
Android Version Code: 201011

APP COMPONENTS

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

CERTIFICATE INFORMATION

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

Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-07-07 14:51:19+00:00
Valid To: 2050-07-07 14:51:19+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xadf6ca69defbe03d9b315a9cbd720fbd8642f91
Hash Algorithm: sha256
md5: 34b3ffad9a56d5f92eb6bb7db2026874
sha1: 81debed335171db99be8fe71f6c51107ed3d5b8d
sha256: b8186836289fa7ebf1b93ce4c78b52565849ea7557c287f1d7b8e87c2ec9fb89
sha512: a9ad6d3066c66c770f3e062c6dbf6ee03701588f85930a08b97079380cd49eb9d4f79c025da15eba574890f27b161a15c927741277fb099aa16b9c467fad7a74
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 9532fb8284be6da50bd71e36e4bb9c66752620343b93408e3014f3cf3f60a3eb

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

☰ APPLICATION PERMISSIONS

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

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
org.covidwatch.android.ui.MainActivity	Schemes: https://, Hosts: us-az.verify.wehealth.org, Mime Types: application/zip, Paths: /v,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Broadcast Receiver (org.covidwatch.android.receiver.ExposureNotificationReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.nearby.exposurenotification.EXPOSURE_CALLBACK [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
2	Service (com.google.android.gms.nearby.exposurenotification.WakeUpService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.nearby.exposurenotification.EXPOSURE_CALLBACK [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
4	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
5	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
app-measurement.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
pagead2.googlesyndication.com	good	**IP:** 142.251.33.66 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.cdc.gov	good	**IP:** 23.6.53.73 **Country:** Canada **Region:** Alberta **City:** Calgary **Latitude:** 51.050110 **Longitude:** -114.085289 **View:** Google Map
exposure.wehealth.org	good	**IP:** 34.120.167.115 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
schemas.android.com	good	No Geolocation information available.
verification.api.wehealth.org	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
help.wehealth.org	good	**IP:** 104.16.51.111 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebase.google.com	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
exposure.key.api.wehealth.org	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
www.wehealth.org	good	**IP:** 199.60.103.227 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.370129 **Longitude:** -71.086304 **View:** Google Map
www.google.com	good	**IP:** 142.250.69.196 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
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
azdhs.gov	good	**IP:** 65.8.68.72 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
www.covidwatch.org	good	**IP:** 199.60.103.29 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.370129 **Longitude:** -71.086304 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
org-wehealth.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
console.firebase.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
goo.gl	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
www.googleadservices.com	good	**IP:** 142.250.69.194 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.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
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

URLS

URL	FILE
https://www.wehealth.org/solutions/app	defpackage/g.java
https://www.wehealth.org/solutions/app	e/a/a/a/a.java
https://play.google.com/store/apps/details?id=com.google.android.gms	e/a/a/a/g.java
https://help.wehealth.org/hc/en-us/articles/360060539533-How-is-risk-calculated-	e/a/a/a/n/a.java

URL	FILE
https://www.covidwatch.org/get_support https://www.cdc.gov/coronavirus/2019-ncov/index.html https://www.covidwatch.org https://azdhs.gov/documents/privacy-policy/covid-watch-application-privacy-policy.pdf	e/a/a/a/p/c.java
http://schemas.android.com/apk/res/android	l/h/c/b/h.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	m/b/a/b/a/a/b.java
https://plus.google.com/	m/b/a/b/d/k/c1.java
https://goo.gl/J1sWQy	m/b/a/b/g/f/f0.java
https://app-measurement.com/a	m/b/a/b/g/f/q8.java
https://firebase.google.com/support/guides/disable-analytics	m/b/a/b/h/b/c3.java
https://google.com/search?	m/b/a/b/h/b/k6.java
https://goo.gl/NAOOOI. https://goo.gl/NAOOOI	m/b/a/b/h/b/k9.java
www.google.com https://www.google.com	m/b/a/b/h/b/l6.java
https://www.googleadservices.com/pagead/conversion/app/deeplink?id_type=adid&sdk_version=%s&rdid=%s&bundleid=%s&retry=%s	m/b/a/b/h/b/m6.java
https://app-measurement.com/a	m/b/a/b/h/b/x2.java

URL	FILE
https://firebase.google.com/docs/database/ios/structure-data#best_practices_for_data_structure https://firebase.google.com/docs/database/android/retrieve-data#filtering_data https://github.com/firebase/firebase-android-sdk	m/b/c/l/q/h.java
https://console.firebase.google.com/.	m/b/c/l/s/g.java
https://firebase.google.com/support/privacy/init-options.	m/b/c/t/f.java
https://%s/%s/%s	m/b/c/t/q/c.java
https://verification.api.wehealth.org https://exposure.key.api.wehealth.org https://exposure.wehealth.org/US-AZ/index.txt https://exposure.wehealth.org	org/covidwatch/android/data/model/DefaultServerConfiguration.java
https://www.covidwatch.org/get_support	org/covidwatch/android/ui/BaseViewModelFragment.java
https://www.wehealth.org/solutions/app	org/covidwatch/android/ui/onboarding/FinishedOnboardingFragment.java
https://www.wehealth.org/solutions/app	org/covidwatch/android/ui/onboarding/OnboardingFragment.java
https://www.wehealth.org/solutions/app	org/covidwatch/android/ui/reporting/DiagnosisSharedFragment.java
https://www.wehealth.org/solutions/app	org/covidwatch/android/ui/settings/SettingsFragment.java
https://www.covidwatch.org/get_support	org/covidwatch/android/work/ProvideDiagnosisKeysWork.java

URL	FILE
https://org-wehealth.firebaseio.com	Android String Resource

FIREBASE DATABASES

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

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	m/b/a/b/d/w.java

TRACKERS

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

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://org-wehealth.firebaseio.com"
"google_api_key" : "AIzaSyCDRgryU23aIscgnYCZ7FP9bJZ2BMOdaf4"
"google_crash_reporting_api_key" : "AIzaSyCDRgryU23aIscgnYCZ7FP9bJZ2BMOdaf4"

PLAYSTORE INFORMATION

Title: Covid Watch Arizona

Score: 3.04 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** 6.0 and up **Category:** Medical **Play Store URL:** gov.azdhs.covidwatch.android

Developer Details: ADHS-Arizona Department of Health Services, ADHS-Arizona+Department+of+Health+Services, 150 N 18TH AVE, https://covidwatch.org, contact@covidwatch.org,

Release Date: Aug 19, 2020 **Privacy Policy:** Privacy link

Description:

As new COVID-19 variants arise, continue to protect yourself, your loved ones, and community through safe, private, and anonymous exposure notifications with the Covid Watch Arizona App. Once you opt-in and enable exposure notifications on your phone, Covid Watch Arizona starts working immediately to detect if you come into close proximity with someone who has tested positive for COVID-19. The app is completely anonymous and works in the background without ever needing to know your location or personal information. It’s simple, safe, and secure. Get immediate access to the most up-to-date and reliable information on how to protect yourself from new variants, including how to get a vaccine and where to get tested within your chosen community. The more people who download the app, the more effective we can be. We support this app statewide with customizations for specific counties, universities, Tribal Nations, and other communities. So encourage your friends, family, and colleagues to install Covid Watch Arizona today. Together, we can slow the spread of COVID-19. Provided by WeHealth Solutions, a public benefit corporation and the developer of Covid Watch Arizona, with a mission to end the threat and burden of infectious diseases. Released in partnership with the Arizona Department of Health Services (ADHS).

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.