MobSF

ANDROID STATIC ANALYSIS REPORT

Covid Watch Arizona (2.1.11)

File Name:	Covid Watch Arizona_v2.1.11_apkpure.com.xapk
Package Name:	gov.azdhs.covidwatch.android
Average CVSS Score:	6.7
App Security Score:	45/100 (MEDIUM RISK)
Trackers Detection:	1/407
Scan Date:	Nov. 19, 2021, 6:01 p.m.

FILE INFORMATION

File Name: Covid Watch Arizona_v2.1.11_apkpure.com.xapk
Size: 3.56MB
MD5: 8447af2385f764352635fb0018e1ed11
SHA1: 7c44b4e2a6f16662e137e5c753117b9489c0cd03
SHA256: 2d6467e08887945b717c8a48eec1e8325967a640ff760525a7dbd3f09b129566

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 <7.0

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.
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.

NO	ISSUE	SEVERITY	DESCRIPTION
2	Service (com.google.android.gms.nearby.exposurenotification.WakeUpService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.nearby.exposurenotification.EXPOSURE_CALLBACK [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
3	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
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
1	The App uses an insecure Random Number Generator.	warning	CVSS V2: 7.5 (high) CWE: CWE-330 Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	m/b/c/i/c.java m/b/a/b/h/b/k9.java m/b/c/l/w/j.java m/b/c/l/s/t/b.java
				m/b/c/l/q/j.java m/b/a/b/d/i.java m/b/a/b/h/b/x9.java m/b/c/v/n.java m/b/a/b/g/g/m.java m/b/a/b/d/j/i/v.java m/b/a/b/a/a/a.java m/b/c/v/o.java m/b/a/b/g/f/k3.java m/b/a/b/d/x.java m/b/a/b/i/a.java m/b/c/v/p.java m/b/a/b/d/j/i/g0.java m/b/a/b/g/e/k.java m/b/c/v/u.java m/b/a/c/x/g.java m/b/a/b/c/q.java m/b/c/v/s.java m/b/a/b/g/f/i3.java m/b/a/b/c/r.java m/b/a/b/h/b/k9.java m/b/c/r/q.java m/b/a/b/g/f/q3.java m/b/a/b/h/b/k3.java m/b/a/b/c/c.java m/b/c/k/f.java m/b/c/r/v.jav

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	The App logs information. Sensitive information should never be logged.	info	CVSS V2: 7.5 (high) CWE: CWE-532 Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	a o/l0/l/d.java m/b/a/b/d/f.java m/b/c/t/b.java m/b/a/b/g/f/l3.java m/b/a/c/r/c.java m/b/a/b/c/t.java m/b/a/b/d/n/h.java m/b/c/r/b0.java o/l0/l/h.java m/b/a/b/g/f/f4.java m/b/a/b/h/b/u9.java m/b/a/b/g/f/g3.java m/b/a/b/d/j/i/e.java m/b/a/b/d/k/h0.java m/b/c/v/g.java m/b/c/t/f.java m/b/a/b/d/k/z0.java m/b/a/b/d/k/v.java m/b/c/t/p/b.java m/b/a/b/g/f/y2.java m/b/c/v/a.java m/b/a/b/g/f/m3.java m/b/a/b/d/g0.java m/b/a/b/d/j/i/i0.java m/b/a/b/g/f/g4.java m/b/a/b/a/a/c.java m/b/a/b/d/k/o0.java m/b/a/b/c/j.java m/b/a/b/c/p.java m/b/a/b/k/a.java m/b/a/b/g/f/p9.java m/b/c/r/n.java m/b/c/v/y.java m/b/c/r/a0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				m/b/a/c/u/b.java m/b/a/c/v/a.java m/b/c/v/r.java m/b/a/b/d/h.java m/b/a/b/c/m.java m/b/a/b/d/j/i/x.java m/b/c/l/t/w0/j.java m/b/a/c/c/g.java m/b/a/b/h/b/d9.java m/b/c/l/u/b.java m/a/a/a/a.java m/b/c/r/m.java m/b/a/b/d/b0.java m/b/a/b/g/f/f0.java m/b/a/a/i/d.java m/b/c/v/z.java m/b/a/b/d/k/e.java m/b/a/b/g/f/g.java m/b/c/r/d0.java m/b/c/r/i.java m/b/a/b/d/k/x.java m/b/c/t/q/c.java m/b/a/b/g/f/e3.java m/b/c/r/x.java m/b/c/v/v.java m/b/a/b/c/b.java m/b/a/b/d/k/b.java m/b/a/b/c/u.java m/b/c/v/c.java m/b/c/r/b.java m/b/a/b/d/k/s0.java m/b/c/c.java m/b/a/b/d/m/a.java m/b/a/b/c/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				m/b/a/b/d/e.java o/l0/c.java m/b/a/b/c/f.java m/b/a/b/d/n/d.java m/b/c/r/w.java m/b/a/b/d/p.java m/b/c/r/f.java m/b/a/a/j/q/k.java m/b/a/b/h/b/f3.java m/b/c/l/t/w0/l/a.java m/b/a/b/d/k/a1.java m/b/c/k/m.java m/b/a/b/c/y.java m/b/a/b/c/g.java m/b/a/b/a/a/b.java
3	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CVSS V2: 5.9 (medium) CWE: CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	m/b/a/b/h/b/x9.java m/b/a/a/j/t/i/w.java m/b/a/a/j/t/i/x.java m/b/a/b/h/b/j.java m/b/a/b/h/b/t9.java m/b/a/a/j/t/i/y.java m/b/a/b/h/b/d9.java m/b/a/a/j/t/i/z.java m/b/a/a/j/t/i/v.java m/b/a/b/h/b/e3.java m/b/a/b/d/n/d.java m/b/a/a/j/t/i/t.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	CVSS V2: 0 (info) OWASP MASVS: MSTG-NETWORK-4	o/l0/l/c.java o/l0/l/h.java o/l0/l/d.java o/l0/l/g.java
5	This App may have root detection capabilities.	secure	CVSS V2: 0 (info) OWASP MASVS: MSTG-RESILIENCE-1	m/b/a/b/g/f/i3.java
6	MD5 is a weak hash known to have hash collisions.	warning	CVSS V2: 7.4 (high) CWE: CWE-327 Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	m/b/a/b/h/b/k9.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	SHA-1 is a weak hash known to have hash collisions.	warning	CVSS V2: 5.9 (medium) CWE: CWE-327 Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	m/b/c/t/p/b.java m/b/c/r/n.java m/b/c/l/t/w0/j.java
8	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. This application is vulnerable to MITM attacks	high	CVSS V2: 7.4 (high) CWE: CWE-295 Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	m/b/c/l/w/e.java
9	App creates temp file. Sensitive information should never be written into a temp file.	warning	CVSS V2: 5.5 (medium) CWE: CWE-276 Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	m/b/c/t/p/c.java

NIAP ANALYSIS v1.3

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

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

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
goo.gl	good	**IP:** 142.251.32.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
exposure.key.api.wehealth.org	good	**IP:** 142.250.65.179 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
verification.api.wehealth.org	good	**IP:** 142.250.65.179 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
console.firebase.google.com	good	**IP:** 142.250.80.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	good	**IP:** 140.82.113.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
google.com	good	**IP:** 142.250.72.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	good	No Geolocation information available.
www.google.com	good	**IP:** 142.251.40.196 **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:** 142.250.80.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
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
pagead2.googlesyndication.com	good	**IP:** 142.250.80.66 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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
www.googleadservices.com	good	**IP:** 172.217.165.130 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.wehealth.org	good	**IP:** 199.60.103.29 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.370129 **Longitude:** -71.086304 **View:** Google Map
www.cdc.gov	good	**IP:** 184.85.20.232 **Country:** United States of America **Region:** New Jersey **City:** Newark **Latitude:** 40.735661 **Longitude:** -74.172371 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
plus.google.com	good	**IP:** 142.251.40.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
azdhs.gov	good	**IP:** 13.225.210.86 **Country:** United States of America **Region:** New Jersey **City:** Newark **Latitude:** 40.735661 **Longitude:** -74.172371 **View:** Google Map
www.covidwatch.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
play.google.com	good	**IP:** 142.250.176.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app-measurement.com	good	**IP:** 142.250.64.110 **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/o5.java
https://app-measurement.com/a	m/b/a/b/h/b/x2.java
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

URL	FILE
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
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: 3.75 **Installs:** 10,000+ **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:

Let your smartphone notify you of potential exposure to COVID-19—using fully anonymous Bluetooth signals—and help stop the spread of coronavirus throughout the state of Arizona. NEW Vaccine Support: In a single tap, you can easily access the most up-to-date and reliable information on how to get a vaccine within your chosen community. Get peace of mind and start rebuilding trust in your community with just one small step: Install this free app, released in partnership with the Arizona Department of Health Services (ADHS). Once you opt-in and enable exposure notifications on your phone, Covid Watch 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. The more people who download the app, the more effective we can be. We have now extended support statewide, so encourage your friends, family, and colleagues to install Covid Watch today. Together, we can slow the spread of COVID-19. Provided by Covid Watch, an Arizona non-profit organization dedicated to your health and privacy.WeHealth is a public benefit corporation and the developer of Covid Watch Arizona.

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.