ANDROID STATIC ANALYSIS REPORT

COVIDWISE (1.5)

File Name:	gov.vdh.exposurenotification_1.5-157_minAPI23(nodpi)_apkmirror.com.apk
Package Name:	gov.vdh.exposurenotification
Average CVSS Score:	0
App Security Score:	100/100 (LOW RISK)
Scan Date:	Feb. 20, 2022, 5:45 p.m.

FILE INFORMATION

File Name: gov.vdh.exposurenotification_1.5-157_minAPI23(nodpi)_apkmirror.com.apk
Size: 9.32MB
MD5: 32425dc9fa8d2ce5a3cc0975836e97a5
SHA1: 752eac19932579c75770491d7fd8afbd85418797
SHA256: 1a1614af0c429039ae60f2e53658aea9d24928f6c325482f2dffb270059f7a5a

APP INFORMATION

App Name: COVIDWISE
Package Name: gov.vdh.exposurenotification
Main Activity: gov.vdh.exposurenotification.home.ExposureNotificationActivity
Target SDK: 29
Min SDK: 23
Max SDK:
Android Version Name: 1.5
Android Version Code: 157

APP COMPONENTS

Activities: 10
Services: 5
Receivers: 9
Providers: 1
Exported Activities: 1
Exported Services: 2
Exported Receivers: 2
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: 2020-06-04 20:14:52+00:00
Valid To: 2050-06-04 20:14:52+00:00

```
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xeb71940d3ffd38eede3bab5947d45105b3de262c
Hash Algorithm: sha256
md5: 911dbd564eb7e285085cce079d861d40
sha1: 06fd2ff99e83f24ee3dff6cba6d0eac7ee96a44f
sha256: 95f2d708e46381cceeda039feec2788270eb78fc74a923419693500dfffb3194
sha512: 8632b0f63da11c49d3bb02f7cd588cee7c928456df8dd1a4297af7ec3b3caf6844e737647cc6a5962f030aa6110eac4536c9b3d2009034d8bc954d007d243e17
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 7046af6dec75fb74a7b39415da504ae6f7f0a972026a54114f3b66c94038deca
```

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.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
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

<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.HARDWARE check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table></td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
gov.vdh.exposurenotification.home.ExposureNotificationActivity	Schemes: ens://,
gov.vdh.exposurenotification.ENNotifyOthers	Schemes: ens://, https://, Hosts: us-va.en.express,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Activity-Alias (gov.vdh.exposurenotification.ENNotifyOthers) is not Protected. [android:exported=true]	high	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
2	Broadcast Receiver (gov.vdh.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	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
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
logger-4o35rtqegq-uc.a.run.app	good	**IP:** 216.239.36.53 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.vdh.virginia.gov	good	**IP:** 107.162.163.43 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.602402 **Longitude:** -122.325996 **View:** Google Map
apps.vdh.virginia.gov	good	**IP:** 166.67.194.228 **Country:** United States of America **Region:** Virginia **City:** Chester **Latitude:** 37.349609 **Longitude:** -77.326714 **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
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
apps.apple.com	good	**IP:** 23.73.34.217 **Country:** Canada **Region:** Alberta **City:** Calgary **Latitude:** 51.050110 **Longitude:** -114.085289 **View:** Google Map
vax-agent-4o35rtqegq-uc.a.run.app	good	**IP:** 216.239.38.53 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
va-api-key-4o35rtqegq-uk.a.run.app	good	**IP:** 216.239.38.53 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
play.google.com	good	**IP:** 142.251.33.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
va-download-url-4o35rtqegq-uk.a.run.app	good	**IP:** 216.239.38.53 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
virtualagent-4o35rtqegq-uc.a.run.app	good	**IP:** 216.239.34.53 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

URLS

URL	FILE
https://prod.exposurenotification.health/v1/publish https://logger-4o35rtqegq-uc.a.run.app https://apps.vdh.virginia.gov/covidwise.html https://apiserver.encv.org/api/certificate https://va-api-key-4o35rtqegq-uk.a.run.app/ https://apiserver.encv.org/api/verify	gov/vdh/exposurenotification/BuildConfig.java
https://www.vdh.virginia.gov/coronavirus https://va-download-url-4o35rtqegq-uk.a.run.app https://prod.exposurenotification.health/v1/publish www.vdh.virginia.gov/coronavirus https://apps.apple.com/us/app/covidwise/id1518059690 https://play.google.com/store/apps/details?id=gov.vdh.exposurenotification https://vax-agent-4o35rtqegq-uc.a.run.app/ https://apiserver.encv.org/api/verify https://apps.vdh.virginia.gov/CWP https://virtualagent-4o35rtqegq-uc.a.run.app https://apps.vdh.virginia.gov/CWP.	Android String Resource

HARDCODED SECRETS

POSSIBLE SECRETS
"debug_matching_key_id_caption" : "Verification key ID"
"debug_matching_key_version_caption" : "Verification key version"

POSSIBLE SECRETS
"debug_matching_provide_single_key_icon_description" : "Scan QR Code"
"debug_matching_public_key_caption" : "Public key"
"debug_matching_token_digits" : "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890"
"debug_matching_view_api_not_enabled" : "API must be enabled"
"debug_matching_view_item_key" : "KeyData: %1$s"
"key_server_download_base_uri" : "https://va-download-url-4o35rtqegq-uk.a.run.app"
"key_server_upload_uri" : "https://prod.exposurenotification.health/v1/publish"
"key_upload_uri" : "https://prod.exposurenotification.health/v1/publish"
"debug_matching_key_id_caption" : "Verification key ID"
"debug_matching_key_version_caption" : "Verification key version"
"debug_matching_provide_single_key_icon_description" : "Scan QR Code"
"debug_matching_public_key_caption" : "Public key"
"debug_matching_token_digits" : "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890"
"debug_matching_view_api_not_enabled" : "API must be enabled"
"debug_matching_view_item_key" : "KeyData: %1$s"

PLAYSTORE INFORMATION

Title: COVIDWISE

Score: 3.4191616 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** 6.0 and up **Category:** Health & Fitness **Play Store URL:** gov.vdh.exposurenotification

Developer Details: VDH, VDH, 109 Governor Street, Richmond, Virginia 23219, http://covidwise.org, covidwise@vdh.virginia.gov,

Release Date: Jul 29, 2020 **Privacy Policy:** Privacy link

Description:

COVIDWISE is the official COVID-19 exposure notification app for the Commonwealth of Virginia’s Department of Health (VDH). The app was developed in partnership with SpringML using a Bluetooth Low Energy (BLE) API framework created through a unique collaboration between Apple and Google. Your personal use of COVIDWISE will significantly help inform Virginians suspected of having been within close proximity to someone with a positive COVID-19 diagnosis. When you download COVIDWISE, you are doing your part to efficiently and effectively help your community stay ahead of any potential resurgent trends in cases. This is vitally important as the business sector, healthcare industry, K-12 schools, institutions of higher education, religious organizations, sporting/recreation activities, and others rely on appropriate interventions to ensure the health of our communities and maintain economic viability. How COVIDWISE Works: If someone reports to the app that they tested positive, the signals from their app will search for other app users who shared that signal. The BLE signals are date-stamped and the app estimates how close the two devices were based on signal strength. 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. No names! No location! The BLE framework within COVIDWISE will run in the background, even if the exposure notification 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 COVIDWISE Protects Your Privacy: VDH takes your privacy and confidentiality very seriously. This is why we chose to use the Apple and Google BLE framework. No personal data or location tracking occurs within this app. In fact, there is no need for VDH to know where or who you are for COVIDWISE to work. If you are close enough to another app user, the BLE technology will share signals with that user. Laboratory results for all persons who test positive for COVID-19 are sent to VDH. This is not associated with the app. Our staff follows up with persons reported as positive, based on information provided within the laboratory report. Anonymously Share Positive Test Results With COVIDWISE: When VDH receives any positive COVID-19 lab result registered with a valid mobile phone number, we will automatically send a text message to that individual, which provides rapid notification and encourages them to stay home and away from other people. The text also lets individuals who have tested positive know they may retrieve an 8-digit verification code from the COVIDWISE Verification Portal at https://apps.vdh.virginia.gov/CWP. You must enter your last name, date of birth, and the phone number that matches the information from your registered COVID-19 test to verify your positive result. You may use that 8-digit verification code in order to anonymously report a positive result to the app. This prevents people from falsely reporting positive results, which could generate false exposure notifications. VDH 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. 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 downloading COVIDWISE! Together, we can protect our family, friends, neighbors, and colleagues, and keep Virginia 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.