MOBSF

ANDROID STATIC ANALYSIS REPORT

GuideSafe™ (1.10.0)

File Name:	GuideSafe_v1.10.0_apkpure.com.xapk
Package Name:	gov.adph.exposurenotifications
Average CVSS Score:	0
App Security Score:	100/100 (LOW RISK)
Trackers Detection:	2/421
Scan Date:	Feb. 20, 2022, 5:50 p.m.

FILE INFORMATION

File Name: GuideSafe_v1.10.0_apkpure.com.xapk
Size: 6.7MB
MD5: 1a82d9ecb73ab8ec9bd3e45d57d9ad1e

SHA1: 7a62af26eeba17e490fcaa38d3141466c10d3587
SHA256: 8e459967de660e87d392f22ccb50db6a60993356ab9b32f5cca8f5595dc19ef6

APP INFORMATION

App Name: GuideSafe™
Package Name: gov.adph.exposurenotifications
Main Activity: org.pathcheck.covidsafepaths.SplashActivity
Target SDK: 30
Min SDK: 23
Max SDK:
Android Version Name: 1.10.0
Android Version Code: 2764

APP COMPONENTS

Activities: 3
Services: 5
Receivers: 10
Providers: 2
Exported Activities: 1
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: 2020-06-17 22:31:03+00:00
Valid To: 2050-06-17 22:31:03+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x34559a9233ea76e4a39d6ef8f182c318184ef5d3
Hash Algorithm: sha256
md5: 951d082ec9159def1d032cc94199f9f8
sha1: 974962fdf513a105ce302001df0c54d6e00d0318
sha256: 1af7cefc00c86199d353c13438a35793541dc7e68fe5441eb0d4319aca15d4ba
sha512: 54527a6fa8cb4f6eb6a9cd7d834d32d8583133daf363eb98a9827fe0b3479476435a03cf61a1d766f77024d1338c5609d201dfddf328d967dd3314b39037ebdf
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: d811855d67e90e074538d89adbba7a419f64a44b771f97964c584243046ea58a

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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

APKID ANALYSIS

FILE	DETAILS

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

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
org.pathcheck.covidsafepaths.MainActivity	Schemes: pathcheck://, https://, Hosts: exposureHistory, *.en.express,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Activity (org.pathcheck.covidsafepaths.MainActivity) is not Protected. [android:exported=true]	high	An Activity 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 (org.pathcheck.covidsafepaths.exposurenotifications.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.

NO	ISSUE	SEVERITY	DESCRIPTION
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.
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.

NO	ISSUE	SEVERITY	DESCRIPTION
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.
6	Broadcast Receiver (org.matomo.sdk.extra.InstallReferrerReceiver) is not Protected. [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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
notify.bugsnag.com	good	**IP:** 35.186.205.6 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
enconfig.blob.core.windows.net	good	**IP:** 52.239.170.100 **Country:** United States of America **Region:** Virginia **City:** Washington **Latitude:** 38.713451 **Longitude:** -78.159439 **View:** Google Map
bugsnag.com	good	**IP:** 65.8.68.91 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
issuetracker.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:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
covid-exposure-apim.azure-api.net	good	**IP:** 40.114.29.150 **Country:** United States of America **Region:** Virginia **City:** Washington **Latitude:** 38.713451 **Longitude:** -78.159439 **View:** Google Map
www.alabamapublichealth.gov	good	**IP:** 65.61.14.13 **Country:** United States of America **Region:** Pennsylvania **City:** Harrisburg **Latitude:** 40.270439 **Longitude:** -76.805458 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.guidesafe.org	good	**IP:** 34.215.37.29 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
sessions.bugsnag.com	good	**IP:** 35.190.88.7 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **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
cdn.projectaurora.cloud	good	**IP:** 35.244.172.56 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
docs.bugsnag.com	good	**IP:** 54.151.57.158 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
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
enanalytics.idm.uab.edu	good	**IP:** 40.87.2.37 **Country:** United States of America **Region:** Virginia **City:** Washington **Latitude:** 38.713451 **Longitude:** -78.159439 **View:** Google Map
realm.io	good	**IP:** 13.225.250.3 **Country:** Israel **Region:** Tel Aviv **City:** Tel Aviv **Latitude:** 32.080879 **Longitude:** 34.780571 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dph1.adph.state.al.us	good	**IP:** 216.226.176.99 **Country:** United States of America **Region:** Alabama **City:** Montgomery **Latitude:** 32.374321 **Longitude:** -86.311798 **View:** Google Map
encdn.prod.exposurenotification.health	good	**IP:** 104.212.67.116 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

URLS

URL	FILE
https://github.com/bugsnag/bugsnag-js	com/bugsnag/android/BugsnagReactNativePlugin.java
https://notify.bugsnag.com https://sessions.bugsnag.com	com/bugsnag/android/EndpointConfiguration.java
https://docs.bugsnag.com/platforms/android/ndk-link-errors	com/bugsnag/android/NdkPlugin.java
https://bugsnag.com	com/bugsnag/android/Notifier.java

URL	FILE
https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenFragment.java
https://github.com/software-mansion/react-native-screens/issues/17#issuecomment-424704067	com/swmansion/rnscreens/ScreenStackFragment.java
https://%s/	com/terveystalo/react_native/matomo_sdk/RNMatomoSdkModule.java
https://issuetracker.google.com/issues/36918154	io/realm/Realm.java
https://realm.io/news/android-installation-change/	io/realm/RealmConfiguration.java
https://enconfig.blob.core.windows.net/$web/android/v1.6.config.json https://play.google.com/store/apps/details?id=gov.adph.exposurenotifications https://enconfig.blob.core.windows.net/$web/ios/v1.config.json https://enconfig.blob.core.windows.net/$web/ios/v2.config.json https://www.alabamapublichealth.gov/covid19/ https://encdn.prod.exposurenotification.health https://covid-exposure-apim.azure-api.net https://www.guidesafe.org/guidesafe-exposure-notification-terms-of-service/ https://cdn.projectaurora.cloud/dev/cfg/v1.config.json https://cdn.projectaurora.cloud/dev/cfg/v1.6.config.json https://cdn.projectaurora.cloud/cfg https://dph1.adph.state.al.us/covid-19/ https://www.guidesafe.org/healthcheck-app/ https://apps.apple.com/us/app/guidesafe/id1519514691 https://www.alabamapublichealth.gov/covid19/prevention.html https://www.guidesafe.org/privacy-statement/ https://enanalytics.idm.uab.edu/matomo.php https://enconfig.blob.core.windows.net/$web/ https://www.guidesafe.org/exposure-notification-app/	org/pathcheck/covidsafepaths/BuildConfig.java
https://encdn.prod.exposurenotification.health/	org/pathcheck/covidsafepaths/exposurenotifications/nearby/DiagnosisKeyFileSubmitter.java

TRACKERS

TRACKER	CATEGORIES	URL
Bugsnag	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/207
Matomo (Piwik)	Analytics	https://reports.exodus-privacy.eu.org/trackers/138

PLAYSTORE INFORMATION

Title: GuideSafe

Score: 3.77 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** 6.0 and up **Category:** Medical **Play Store URL:** gov.adph.exposurenotifications

Developer Details: Alabama Department of Public Health, Alabama+Department+of+Public+Health, 201 Monroe Street Montgomery, Alabama 36104, None, alabamapublichealth@gmail.com,

Release Date: Aug 12, 2020 **Privacy Policy:** Privacy link

Description:

Use the GuideSafe™ Exposure Notification app to anonymously share a positive COVID-19 test result — and be anonymously notified of your own possible exposure to someone who later reports a positive COVID-19 test result — all without sharing anyone's identity. The app protects your privacy while giving you the power to protect your health, your family's and your community's. Using the app is easy: Step one: Download the GuideSafe™ Exposure Notification app and enable Bluetooth. Step two: If you have tested positive for COVID-19, you can choose to report it. Your test will be verified by the Alabama Department of Public Health. Step three: Those who may have been in close contact with you in the last 14 days will be notified they were near someone with a positive test, but they won't know who or where. Your identity and location remain completely anonymous, and your personal information isn't disclosed, no matter what. Why it's important Stopping the spread of COVID-19 is essential to helping our communities, schools and businesses reopen and stay open. When someone tests positive for COVID-19, contact tracers with the Alabama Department of Public Health will help notify those the person has been near — but they won't know every person's close contacts. The more people who use the app, the better the ability to notify those who have been exposed. How it works When you are within about six feet of others, phones using the GuideSafe™ Exposure Notification app exchange encrypted, anonymous codes via low-energy Bluetooth. If you test positive for COVID-19, those with whom you came in close contact — defined as within six feet for at least 15 minutes over the last 14 days — will get an anonymous notification that they were exposed. The notification they get is completely anonymous — they will not know who tested positive, the time, or the location — only the date of the possible exposure. Your privacy is our priority The GuideSafe™ Exposure Notification app was developed by the Alabama Department of Public Health in cooperation with the University of Alabama at Birmingham and MotionMobs, using technology from a collaboration between Apple and Google. Users of the app exchange anonymous codes among their phones using Bluetooth — no location data is ever stored or exchanged, and your personal

information is never shared.

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.