ANDROID STATIC ANALYSIS REPORT

MI COVID Alert (1.4)

File Name:	MI COVID Alert_1.4_apkcombo.com.apk
Package Name:	gov.michigan.MiCovidExposure
Average CVSS Score:	6.6
App Security Score:	70/100 (MEDIUM RISK)
Scan Date:	Oct. 15, 2021, 2:20 a.m.

FILE INFORMATION

File Name: MI COVID Alert_1.4_apkcombo.com.apk
Size: 3.19MB
MD5: 7a09c47bfedfa7ae69fb22b455b065a6
SHA1: 2090ade76f5b2c68d34cb6d42650c24c71ad3814
SHA256: e85ec2bf31c642bc0bfcefa384c34dd29cae1229b0279af0a44df9d3251bfa6d

APP INFORMATION

App Name: MI COVID Alert
Package Name: gov.michigan.MiCovidExposure
Main Activity: gov.michigan.MiCovidExposure.home.ExposureNotificationActivity
Target SDK: 30
Min SDK: 23
Max SDK:
Android Version Name: 1.4
Android Version Code: 255

APP COMPONENTS

Activities: 10
Services: 5
Receivers: 9
Providers: 0
Exported Activities: 0
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: 2020-08-13 19:53:33+00:00
Valid To: 2050-08-13 19:53:33+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x410b351713ea12924dd9341f167cbf221293ef7d
Hash Algorithm: sha256
md5: 396aa5de7788a4ad7e5de69f368c81ee
sha1: 456f53b7f1c984055fc82481a1542e2e58d7a8e3
sha256: 95fced5a903e9d4c03149193ed8b2139a1da9a1a9d94e2af45ef7db330281610
sha512:
e30712752aac851f4e10ce55273d43efd084f79a0b41c266dd5ddcd9f3ac1221a390574aaa688a0d70d2117d222818f828f4a97b3bc376df1003581017053640

PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 51d808e6d836288907f9cbf68b5b9ca5b8903963cbb5804ea60c24afed7780b6

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.
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
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check FINDINGS: Compiler — DETAILS: r8

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Broadcast Receiver (gov.michigan.MiCovidExposure.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.
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	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
4	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 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	b/x/t.java c/b/a/a/d/m/j.java c/b/a/a/d/k/o/j0.java b/l/d/z.java c/b/a/a/g/h/d.java c/b/a/a/d/k/o/g.java c/b/a/a/g/h/a.java b/i/d/l.java c/b/a/a/d/m/b.java c/b/a/a/i/b/a.java c/a/b/x/h.java c/a/b/w.java c/b/a/a/d/g.java c/b/a/a/g/e/fa.java c/b/a/a/c/a.java
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CVSS V2: 7.4 (high) CWE: CWE-312 Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	gov/michigan/MiCovidExposure/notify/ShareDiagnosisActivity.java gov/michigan/MiCovidExposure/storage/ExposureNotificationSharedPreferences.java gov/michigan/MiCovidExposure/home/ExposureNotificationActivity.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	b/s/f.java
4	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	b/q/d.java b/s/l.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 implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity', 'bluetooth'].
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 implement functionality to encrypt sensitive data 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.
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_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys not in accordance with FCS_CKM.1.1(1) using key generation algorithm RSA schemes and cryptographic key sizes of 1024-bit or lower.
12	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode or AES-GCM (as defined in NIST SP 800-38D) and cryptographic key sizes 256-bit/128-bit.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
13	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
14	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
15	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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
proxy-pinverifier-hkv3eknupq-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
coronavirus.jhu.edu	good	**IP:** 13.107.246.40 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
mi-download-url-dyu6ojodva-uk.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
prod.exposurenotification.health	good	**IP:** 13.107.213.40 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
apps.apple.com	good	**IP:** 23.78.0.47 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
plus.google.com	good	**IP:** 142.250.65.174 **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.
somvpin-53xmcbdutq-uk.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
virtualagent-dyu6ojodva-uk.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
covid19.mdhhs.gov	good	No Geolocation information available.
www.michigan.gov	good	**IP:** 23.14.152.231 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.714272 **Longitude:** -74.005966 **View:** Google Map
logger-dyu6ojodva-uk.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

DOMAIN	STATUS	GEOLOCATION
play.google.com	good	**IP:** 172.217.165.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
mi-get-api-key-prod-d3ec2fgvuq-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
somhmac-53xmcbdutq-uk.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

URLS

URL	FILE
http://schemas.android.com/apk/res/android	b/b/k/i.java
https://plus.google.com/	c/b/a/a/d/m/i0.java
https://logger-dyu6ojodva-uk.a.run.app https://somhmac-53xmcbdutq-uk.a.run.app/certify_hmac https://somvpin-53xmcbdutq-uk.a.run.app/verify_pin https://mi-get-api-key-prod-d3ec2fgvuq-uc.a.run.app https://coronavirus.jhu.edu/region/us/michigan?embed	gov/michigan/MiCovidExposure/BuildConfig.java
https://covid19.MDHHS.gov. https://mi-download-url-dyu6ojodva-uk.a.run.app/ https://proxy-pinverifier-hkv3eknupq-uc.a.run.app/v1/publish https://prod.exposurenotification.health/v1/publish https://covid19.MDHHS.gov https://somvpin-53xmcbdutq-uk.a.run.app/verify_pin www.michigan.gov/coronavirus http://www.michigan.gov/coronavirus https://apps.apple.com/us/app/id1527644912 https://play.google.com/store/apps/details?id=gov.michigan.MiCovidExposure https://www.michigan.gov/coronavirus. https://virtualagent-dyu6ojodva-uk.a.run.app www.michigan.gov/coronavirus. https://www.michigan.gov/coronavirus	Android String Resource

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	c/b/a/a/d/y.java

HARDCODED SECRETS

POSSIBLE SECRETS
"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$s"
"key_server_download_base_uri" : "https://mi-download-url-dyu6ojodva-uk.a.run.app/"
"key_server_upload_proxy_uri" : "https://proxy-pinverifier-hkv3eknupq-uc.a.run.app/v1/publish"
"key_server_upload_uri" : "https://prod.exposurenotification.health/v1/publish"
"debug_matching_key_id_caption" : "Verification key ID"
"debug_matching_key_version_caption" : "Verification key version"
"debug_matching_provide_single_key_icon_description" : "Scan QR Code"
"debug_matching_public_key_caption" : "Public key"
"debug_matching_token_digits" : "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890"
"debug_matching_view_api_not_enabled" : "API must be enabled"
"debug_matching_view_item_key" : "KeyData: %1$s"
"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"

POSSIBLE SECRETS
"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: MI COVID Alert

Score: 2.96 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** 6.0 and up **Category:** Health & Fitness **Play Store URL:** gov.michigan.MiCovidExposure

Developer Details: State of Michigan, State+of+Michigan, None, http://www.michigan.gov/micovidalert, mdhhs-micovidalert@michigan.gov,

Release Date: Oct 9, 2020 **Privacy Policy:** Privacy link

Description:

MI COVID Alert is the COVID-19 exposure notification app supported by the Michigan Department of Health and Human Services (MDHHS), in partnership with SpringML, Google, and Apple. This app uses Bluetooth Low Energy (BLE) API framework created through a unique collaboration between Apple and Google. Your personal use of MI COVID Alert helps inform others of possible exposure to COVID-19 if they are suspected of having been within close proximity to someone who has tested positive. When you download MI COVID Alert, you are helping your community stay ahead of any potential surge in COVID-19 cases. How MI COVID Alert Works: Once downloaded, users of the app who have enabled it will exchange anonymous Bluetooth “keys” (random alpha-numeric codes that represent a Bluetooth signal) with other MI COVID Alert users. If someone reports that they tested positive for COVID-19, the app will search for other users who shared the Bluetooth Low Energy (BLE) signal. The BLE signals are date-stamped and MI COVID Alert 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. Names of users and locations of possible exposure are never tracked and never shared. The BLE framework within MI COVID Alert will run in the background, even if the exposure notification app is closed. It will not drain the device battery at a rate faster than other apps that use normal Bluetooth and/or are open and running continuously. How MI COVID Alert Protects Your Privacy: MDHHS takes your privacy very seriously. This is why we chose to use the Apple and Google BLE framework. No personal data or location tracking occurs within MI COVID Alert. MDHHS and local public health staff follow up with persons who have a positive COVID-19 laboratory report. Public health will provide MI COVID Alert users with a validation pin. That validation pin must be entered into the app to report a notification of possible exposure to other users. This prevents people from falsely reporting positive results, which could generate false exposure notifications. If you have the current Apple or Google operating system installed on your device, you may have noticed that Exposure Notifications are now included. You cannot enable this function until you have downloaded MI COVID Alert. 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 MI COVID Alert! Together, we can protect our family, friends, and communities.

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

APP SECURITY SCORE	RISK
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.