ANDROID STATIC ANALYSIS REPORT

SlowCOVIDNC (1.6)

File Name:	SlowCOVIDNC_1.6_apkcombo.com.apk
Package Name:	gov.nc.dhhs.exposurenotification
Average CVSS Score:	6.3
App Security Score:	50/100 (MEDIUM RISK)
Scan Date:	Nov. 5, 2021, 4:47 p.m.

FILE INFORMATION

File Name: SlowCOVIDNC_1.6_apkcombo.com.apk
Size: 3.1MB
MD5: b69f2a404980f66f00ea1b8aa951621d
SHA1: 1d47a8aee251ee5521fce2e31e4464544690d7fc
SHA256: 683b42f6e5a708c48e1b708e81549511d2803654e82a92301f3b7072d7fbfd40

APP INFORMATION

App Name: SlowCOVIDNC
Package Name: gov.nc.dhhs.exposurenotification
Main Activity: gov.nc.dhhs.exposurenotification.home.ExposureNotificationActivity
Target SDK: 29
Min SDK: 23
Max SDK:
Android Version Name: 1.6
Android Version Code: 205

APP COMPONENTS

Activities: 9
Services: 5
Receivers: 9
Providers: 1
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: 2020-07-30 17:10:19+00:00
Valid To: 2050-07-30 17:10:19+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xf1b14be7ac27aa7267ad45909e9b4f0e667e7dbb
Hash Algorithm: sha256
md5: 38400a6f1c28a7f23c5fdda467bad6e4
sha1: e30fa31fde2c3dc64a507fbc29d6db8cf70e33d3
sha256: 940405f64d7e98e3329efbcf9e5f616a48b0c0c12ef03cc021fde1f04e949d7e
sha512:
94135e9f303e41b068fb92b608910b1cd9cccca55efcb1b26d6fada1ae64699dc993d4a28f11bcb606f229d2f8c56509377460f51e76aebb524fc32359b22083

PublicKey Algorithm: rsa
Bit Size: 4096
```

Fingerprint: 2cb7f6606f0acde4ee0ae44b754a0f37a402af1885c8ff2cf5375d47fb08fc20

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

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Broadcast Receiver (gov.nc.dhhs.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.
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	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/r/l.java b/p/d.java
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	c/b/a/a/c/n/c.java c/b/a/a/c/g.java c/b/a/a/c/l/l.java c/b/a/a/f/b/a.java c/b/a/a/c/l/b.java b/l/d/q.java c/b/a/a/c/k/o/m0.java c/a/b/x/h.java c/a/b/w.java c/b/a/a/e/c/fa.java b/i/d/k.java c/b/a/a/c/k/o/g.java
3	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	e/b/f/b.java
4	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/nc/dhhs/exposurenotification/storage/ExposureNotificationSharedPreferences.java gov/nc/dhhs/exposurenotification/onboarding/HowItWorksActivity.java gov/nc/dhhs/exposurenotification/notify/ShareDiagnosisActivity.java gov/nc/dhhs/exposurenotification/home/ExposureNotificationActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	IP Address disclosure	warning	CVSS V2: 4.3 (medium) CWE: CWE-200 Information Exposure OWASP MASVS: MSTG-CODE-2	gov/nc/dhhs/exposurenotification/nearby/ProvideDiagnosisKeysWorker.java
6	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/r/f.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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.
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
ncdhhs.gov	good	**IP:** 52.204.9.77 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
logger-vakbimwq5a-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
schemas.android.com	good	No Geolocation information available.
covid19.ncdhhs.gov	good	**IP:** 13.225.63.12 **Country:** United States of America **Region:** New Jersey **City:** Newark **Latitude:** 40.735661 **Longitude:** -74.172371 **View:** Google Map
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
plus.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
totaldownloads-vakbimwq5a-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
ncdhhs-covid19-dtra.powerappsportals.us	good	**IP:** 52.238.74.74 **Country:** United States of America **Region:** Texas **City:** San Antonio **Latitude:** 29.424120 **Longitude:** -98.493629 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
files.nc.gov	good	**IP:** 13.33.46.51 **Country:** United States of America **Region:** New Jersey **City:** Newark **Latitude:** 40.735661 **Longitude:** -74.172371 **View:** Google Map
play.google.com	good	**IP:** 142.251.35.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
prod.exposurenotification.health	good	**IP:** 13.107.246.40 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
exposurenotification.ncpublichealth.com	good	**IP:** 207.4.134.249 **Country:** United States of America **Region:** North Carolina **City:** Raleigh **Latitude:** 35.851063 **Longitude:** -78.632027 **View:** Google Map
apps.apple.com	good	**IP:** 23.64.60.25 **Country:** United States of America **Region:** New Jersey **City:** Edison **Latitude:** 40.518719 **Longitude:** -74.412102 **View:** Google Map
nc-download-url-vakbimwq5a-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-vakbimwq5a-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
www.google.com	good	**IP:** 142.251.40.228 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.ncdhhs.gov	good	**IP:** 13.225.63.23 **Country:** United States of America **Region:** New Jersey **City:** Newark **Latitude:** 40.735661 **Longitude:** -74.172371 **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/c/l/e0.java
https://logger-vakbimwq5a-uk.a.run.app https://exposurenotification.ncpublichealth.com https://proxy-pinverifier-hkv3eknupq-uc.a.run.app https://totaldownloads-vakbimwq5a-uk.a.run.app	gov/nc/dhhs/exposurenotification/BuildConfig.java
https://play.google.com/store/apps/details?id=gov.nc.dhhs.exposurenotification	gov/nc/dhhs/exposurenotification/common/NotificationHelper.java
https://files.nc.gov/covid/slowcovidnc.html	gov/nc/dhhs/exposurenotification/home/StatsHomeFragment.java
https://play.google.com/store/apps/details?id=gov.nc.dhhs.exposurenotification http://www.google.com	gov/nc/dhhs/exposurenotification/nearby/ProvideDiagnosisKeysWorker.java
https://www.ncdhhs.gov/divisions/public-health/county-health-departments. https://covid19.ncdhhs.gov https://nc-download-url-vakbimwq5a-uk.a.run.app https://prod.exposurenotification.health https://covid19.ncdhhs.gov. https://exposurenotification.ncpublichealth.com https://proxy-pinverifier-hkv3eknupq-uc.a.run.app https://ncdhhs-covid19-dtra.powerappsportals.us/en-US/ https://www.ncdhhs.gov/divisions/public-health/county-health-departments https://covid19.ncdhhs.gov/about-covid-19/testing/find-my-testing-place https://covid19.ncdhhs.gov/slowcovidnc-privacy-policy https://apps.apple.com/us/app/slowcovidnc/id1526471580 https://play.google.com/store/apps/details?id=gov.nc.dhhs.exposurenotification&hl=en_US https://ncdhhs.gov/slowcovidncpin https://virtualagent-vakbimwq5a-uk.a.run.app	Android String Resource

✉ EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	c/b/a/a/c/x.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$s"
"key_server_download_base_uri" : "https://nc-download-url-vakbimwq5a-uk.a.run.app"
"key_server_upload_uri" : "https://prod.exposurenotification.health"
"revision_token_alert_title" : "Keys already submitted"
"debug_matching_key_id_caption" : "Verification key ID"
"debug_matching_key_version_caption" : "Verification key version"
"debug_matching_provide_single_key_icon_description" : "Scan QR Code"
"debug_matching_public_key_caption" : "Public key"
"debug_matching_token_digits" : "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890"
"debug_matching_view_api_not_enabled" : "API must be enabled"
"debug_matching_view_item_key" : "KeyData: %1$s"
"revision_token_alert_title" : "Claves ya enviadas"

PLAYSTORE INFORMATION

Title: SlowCOVIDNC

Score: 3.2518518 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** 6.0 and up **Category:** Health & Fitness **Play Store URL:** gov.nc.dhhs.exposurenotification

Developer Details: NC Department of Health and Human Services, NC+Department+of+Health+and+Human+Services, None, https://covid19.ncdhhs.gov/SlowCOVIDNC, NCHealthIT@dhhs.nc.gov,

Release Date: Sep 15, 2020 **Privacy Policy:** Privacy link

Description:

SlowCOVIDNC is the official COVID-19 Exposure Notification app for the North Carolina Department of Health and Human Services (NCDHHS). It allows users to know if they may have been in close contact with someone who has shared a positive COVID-19 test result through the app. Users can anonymously share a positive COVID-19 test result to help slow the spread of COVID-19. NCDHHS created this app so that North Carolinians can do their part to protect their community and slow the spread of the virus. HOW SLOWCOVIDNC WORKS? Step 1: Download the SlowCOVIDNC Exposure Notification app. Enable Bluetooth and Exposure notifications. Step 2: After opting-in to receive notifications, the app will generate an anonymous token for your device. A token is a string of random letters and numbers that is used to represent a phone for a short period of time. This ensures your privacy and security are protected. These individual tokens change every 10-20 minutes and are never linked to your identity or location. Step 3: Through Bluetooth, your phone and the phones around you with the SlowCOVIDNC app are working in the background (without draining your battery or data) to exchange these anonymous tokens every few minutes. As a result, devices can remember how long they are near each other. Phones also record the Bluetooth signal strength of their exchanges in order to estimate how far apart they are. Step 4: SlowCOVIDNC periodically downloads tokens from the server that have been uploaded from the devices of users who have tested positive. Your phone then uses its records of the signal strength and duration of exposures with those tokens to conduct a risk calculation and determine if you have met a threshold for notification. Step 5: If you have tested positive for COVID-19, you may obtain your PIN from your local public health department and submit that into the app. This voluntary and anonymous reporting notifies others who have downloaded the app and may have been in close contact with you in the last 14 days that they might be at risk. HOW SLOWCOVIDNC PROTECTS YOUR PRIVACY? Using SlowCOVIDNC is entirely voluntary, and you can enable or disable it at any time. When using SlowCOVIDNC, your privacy will be protected. Tokens will collect and share date, time, signal strength and duration of proximity. No location data or personally identifiable data will ever be collected or stored. By enabling Bluetooth and Exposure Notifications, you can anonymously share a positive COVID-19 test result to help slow the spread of COVID-19. You may also be notified if you have been in close contact with someone who has shared a positive COVID-19 test result. Learn more about how your privacy is protected and our privacy policy on the NCDHHS website. Thank you for downloading SlowCOVIDNC. Together, we can slow the spread of COVID-19!

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.