ANDROID STATIC ANALYSIS REPORT

NHS Covid-19 (4.26.1 (280))

File Name:	NHSCovid.apk
Package Name:	uk.nhs.covid19.production
Scan Date:	Feb. 25, 2022, 11:53 a.m.
App Security Score:	**49/100 (MEDIUM RISK)**
Grade:	B

FINDINGS SEVERITY

HIGH	WARNING	INFO	SECURE
3	10	2	2

FILE INFORMATION

File Name: NHSCovid.apk
Size: 10.19MB
MD5: ece5500bc433d1dfad866717664793fc
SHA1: fa241b71ad1473d9748df85cae71f717b7d20be1
SHA256: 4b6209ea8af0d37148f0259e76eb7ee470b30df424227ac86414f14aa058f932

APP INFORMATION

App Name: NHS Covid-19
Package Name: uk.nhs.covid19.production
Main Activity: uk.nhs.nhsx.covid19.android.app.MainActivity
Target SDK: 30
Min SDK: 23
Max SDK:
Android Version Name: 4.26.1 (280)
Android Version Code: 280

APP COMPONENTS

Activities: 69
Services: 6
Receivers: 17
Providers: 1
Exported Activities: 0
Exported Services: 3
Exported Receivers: 4
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: 2020-07-04 18:55:30+00:00
Valid To: 2050-07-04 18:55:30+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xe697f2187aff9a5aa236377780a72c06721a4189
Hash Algorithm: sha256
md5: 2a91c2cdc6f501eb18f8b7bbe740086f
sha1: 41210f20f44ab35390963ca074bb1ceb4f4f302f
sha256: 56049d25b3d20a6ae2583a90bef1b9d310d741f329596cfbcebaa108f08aabda
sha512: bc2be648d8fa403f8bd6257d98de2db6c9788e47d7fb70dc26dd1eedd93052629e702b67ad7b4451488b68b8a377500ee9bfb87285b1d90a01e8191a91e9d93a
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 077d6f5329cb4b516db631d1428df87557a0cb3be4f4058004059871090e8eed
```

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	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.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
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.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.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal		Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

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.MANUFACTURER check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</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 without marker (suspicious)</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
1	localhost	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
2	Broadcast Receiver (uk.nhs.nhsx.covid19.android.app.exposure.encounter.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]	warning	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	Broadcast Receiver (uk.nhs.nhsx.covid19.android.app.receiver.AlarmRestarter) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Broadcast Receiver (uk.nhs.nhsx.covid19.android.app.receiver.UpdateReceiver) is not Protected. An intent-filter exists.	warning	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
5	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]	warning	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.
6	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
7	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]	warning	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.
8	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]	warning	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	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	uk/nhs/nhsx/covid19/android/app/status/ResumeContactTracingNotificationTimeProvider.java uk/nhs/nhsx/covid19/android/app/testordering/RelevantTestResultProvider.java io/jsonwebtoken/JwsHeader.java uk/nhs/nhsx/covid19/android/app/qrcode/riskyvenues/RiskyVenueConfigurationProvider.java uk/nhs/nhsx/covid19/android/app/testordering/LatestTestResultProvider.java uk/nhs/nhsx/covid19/android/app/util/StrongBoxMigrationRetryStorage.java uk/nhs/nhsx/covid19/android/app/util/crashreporting/CrashReportProvider.java uk/nhs/nhsx/covid19/android/app/testordering/TestResultsProvider.java uk/nhs/nhsx/covid19/android/app/analytics/legacy/AnalyticsMetricsStorage.java uk/nhs/nhsx/covid19/android/app/state/StateStorage4_9.java uk/nhs/nhsx/covid19/android/app/remote/data/NHSTemporaryExposureKey.java uk/nhs/nhsx/covid19/android/app/common/postcode/PostalDistrictProvider.java uk/nhs/nhsx/covid19/android/app/availability/LastRecommendedNotificationAppVersionProvider.java uk/nhs/nhsx/covid19/android/app/exposure/keysdownload/LastDownloadedKeyTimeProvider.java uk/nhs/nhsx/covid19/android/app/exposure/encounter/ExposureNotificationTokensStorage.java
2	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	com/jeroenmols/featureflag/framework/RuntimeFeatureFlagProvider.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	uk/nhs/nhsx/covid19/android/app/qrcode/QrCodeParser.java timber/log/Timber.java
4	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	j$/util/concurrent/ThreadLocalRandom.java
5	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	uk/nhs/nhsx/covid19/android/app/browser/BrowserActivity.java
6	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	uk/nhs/nhsx/covid19/android/app/di/module/NetworkModule.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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 ['bluetooth', 'camera', '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 leverage platform-provided 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 not in accordance with FCS_COP.1.1(1), AES-ECB mode is being used.
13	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1/SHA-256/SHA-384/SHA-512 and message digest sizes 160/256/384/512 bits.
14	FCS_COP.1.1(3)	Selection-Based Security Functional Requirements	Cryptographic Operation - Signing	The application perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
15	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
16	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.
17	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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
18	FIA_X509_EXT.2.2	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	When the application cannot establish a connection to determine the validity of a certificate, the application allow the administrator to choose whether to accept the certificate in these cases or accept the certificate ,or not accept the certificate.
19	FCS_CKM.1.1(2)	Optional Security Functional Requirements	Cryptographic Symmetric Key Generation	The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.nhs.uk	ok	**IP:** 23.196.200.50 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
tools.ietf.org	ok	**IP:** 4.31.198.62 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 142.251.42.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
faq.covid19.nhs.uk	ok	**IP:** 51.141.44.139 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** Wales **City:** Cardiff **Latitude:** 51.480000 **Longitude:** -3.180000 **View:** Google Map
www.gov.uk	ok	**IP:** 151.101.188.144 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sip.test-and-trace.nhs.uk	ok	**IP:** 13.224.218.14 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
111.nhs.uk	ok	**IP:** 23.39.160.208 **Country:** France **Region:** Provence-Alpes-Cote-d'Azur **City:** Marseille **Latitude:** 43.296951 **Longitude:** 5.381070 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.250.67.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
gov.wales	ok	**IP:** 192.124.249.167 **Country:** United States of America **Region:** California **City:** Menifee **Latitude:** 33.679798 **Longitude:** -117.189484 **View:** Google Map
covid19.nhs.uk	ok	**IP:** 52.85.3.125 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 20.205.243.166 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
111.wales.nhs.uk	ok	**IP:** 5.79.9.102 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
llyw.cymru	ok	**IP:** 192.124.249.4 **Country:** United States of America **Region:** California **City:** Menifee **Latitude:** 33.679798 **Longitude:** -117.189484 **View:** Google Map
coronavirus.data.gov.uk	ok	**IP:** 13.107.246.59 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"url_local_authority" : "https://www.gov.uk/find-local-council"
"url_local_authority" : "https://www.gov.uk/find-local-council"
"local_authority_edit" : "   "
"local_authority_information_description" : "   "
"local_authority_information_title" : "   "
"local_authority_link" : "   "
"local_authority_title" : "   "
"local_statistics_main_screen_local_authority_lower_tier" : "   "
"multiple_local_authorities_description" : "   %s   GOV.UK "
"multiple_local_authorities_title" : "   "
"settings_my_area_local_authority" : "   "
"single_local_authority_description" : "   "
"single_local_authority_title" : "%1$s   %2$s"
"url_local_authority" : "https://www.gov.uk/find-local-council"

POSSIBLE SECRETS
"local_authority_edit" : "Edytuj"
"url_local_authority" : "https://www.gov.uk/find-local-council"
"url_local_authority" : "https://www.gov.uk/find-local-council"
"local_authority_edit" : "Editare"
"url_local_authority" : "https://www.gov.uk/find-local-council"
"local_authority_edit" : "Tafatir"
"url_local_authority" : "https://www.gov.uk/find-local-council"
"local_authority_edit" : "تعديل"
"url_local_authority" : "https://www.gov.uk/find-local-council"
"local_authority_edit" : "Düzenle"
"url_local_authority" : "https://www.gov.uk/find-local-council"
"local_authority_edit" : "ترميم"
"url_local_authority" : "https://www.gov.uk/find-local-council"
"url_local_authority" : "https://www.gov.uk/find-local-council"
"local_authority_edit" : "Golygu"

POSSIBLE SECRETS
"url_local_authority" : "https://www.gov.uk/find-local-council"

PLAYSTORE INFORMATION

Title: NHS COVID-19

Score: 4.29 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** 6.0 and up **Category:** Medical **Play Store URL:** uk.nhs.covid19.production

Developer Details: Department of Health and Social Care, Department+of+Health+and+Social+Care, None, https://covid19.nhs.uk/, NHSCovid-19AppStoreSupport@nhsbsa.nhs.uk,

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

Description:

The NHS COVID-19 app is the official contact tracing app for England and Wales and is one of the fastest ways of knowing if you're at risk from COVID-19. For your vaccination status (England only) use the separate NHS app, go to www.nhs.uk/app COVID-19 has not gone away, so it's important to remember the actions you can take to keep yourself and others safe. Everybody needs to continue to act carefully and remain cautious. Download the app to protect yourself and loved ones. The app uses proven privacy software developed by Apple and Google, designed so that nobody will know who or where you are. You can delete your data, or the app, at any time. The NHS COVID-19 app features: Alerts: Find out when you've been near other app users who have since tested positive for coronavirus. Latest information: Lets you know the level of coronavirus risk in your local area. Symptoms: Check if you have coronavirus symptoms and see if you need to order a test. Test: Get a test kit and register your results if you test positive. Available in English, Welsh, Arabic (Modern Standard), Bengali, Chinese (Simplified), Gujarati, Polish, Punjabi (Gurmukhi script), Romanian, Somali, Turkish and Urdu. The app can be used when travelling across England, Wales, Scotland, Northern Ireland, Jersey and Gibraltar, detecting contact tracing app users (regardless of them using different official apps), and alerting them if they have been in contact with someone who has tested positive for COVID-19 from a PCR test. The app has been built in collaboration with some of the most innovative organisations in the world. We have worked with medical experts, privacy groups, at-risk communities and we've shared knowledge with the teams working on similar apps in many countries. Protect your loved ones. Please download the app and keep it up to date. The app is UKCA marked as Class I medical device in the United Kingdom and developed in compliance with Medical Devices Regulations 2002 (SI 2002 No 618, as amended).

Report Generated by - MobSF v3.5.1 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.