ANDROID STATIC ANALYSIS REPORT

NHS Test & Trace (3.0.0 (35))

File Name:	base.apk
Package Name:	uk.nhs.covid19.production
Average CVSS Score:	0
App Security Score:	100/100 (LOW RISK)
VirusTotal Detection:	0/62

FILE INFORMATION

File Name: base.apk
Size: 7.46MB
MD5: 34da20b74c36f2ba1b82f4f892b29212
SHA1: 880770cf8ca2d786cb907fd75cae9bf23e2a4acf
SHA256: f5e93050ccb5e86ebd581c9be7e4ec6e02c94151a9cbe08c2cab7824d20b2a82

APP INFORMATION

App Name: NHS Test & Trace
Package Name: uk.nhs.covid19.production
Main Activity: uk.nhs.nhsx.covid19.android.app.MainActivity
Target SDK: 29
Min SDK: 23
Max SDK:
Android Version Name: 3.0.0 (35)
Android Version Code: 35

APP COMPONENTS

Activities: 30
Services: 6
Receivers: 11
Providers: 1
Exported Activities: 0
Exported Services: 3
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: 2020-07-04 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

Certificate Status: Good
Description: Certificate looks good.

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	dangerous	full Internet access	Allows an application to create network sockets.
android.permission.BLUETOOTH	dangerous	create Bluetooth connections	Allows an application to view configuration of the local Bluetooth phone and to make and accept connections with paired 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.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	dangerous	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

VIRUSTOTAL SCAN

0 / 62 AVs found this file Malicious!

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.MANUFACTURER check Build.TAGS check FINDINGS: Compiler — DETAILS: dx
classes2.dex	FINDINGS / DETAILS

	Compiler: dx
classes3.dex	FINDINGS: DETAILS Anti-VM Code: Build.MANUFACTURER check Compiler: dx

MANIFEST ANALYSIS

ISSUE	SEVERITY	DESCRIPTION
App has a Network Security Configuration [android:networkSecurityConfig]	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.
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]	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.
Broadcast Receiver (uk.nhs.nhsx.covid19.android.app.receiver.AlarmRestarter) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
Broadcast Receiver (uk.nhs.nhsx.covid19.android.app.receiver.UpdateReceiver) is not Protected. An intent-filter exists.	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. The

		presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
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.
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.
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.

</> CODE ANALYSIS

ISSUE	SEVERITY	STANDARDS	FILES

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 v3.0.9 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.