ANDROID STATIC ANALYSIS REPORT

UNC Health (3.6.0)

File Name:	org.unchealthcare.go_10451.apk
Package Name:	org.unchealthcare.go
Scan Date:	Sept. 1, 2025, 5:06 p.m.
App Security Score:	57/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	17	4	3	1

FILE INFORMATION

File Name: org.unchealthcare.go_10451.apk
Size: 56.39MB
MD5: 2e5fe6888c00ae95549059f68b98a3ca
SHA1: ecd00326fac1277b422c19ab88a1d524c248d7a0
SHA256: 9f42fffb5db9884f8b2207d5d93603db707489e01240181a105d2e95ae516a3f

APP INFORMATION

App Name: UNC Health
Package Name: org.unchealthcare.go
Main Activity: com.goziohealth.core.ui.startup.StartupActivity
Target SDK: 33
Min SDK: 28
Max SDK:
Android Version Name: 3.6.0

Android Version Code: 10451

APP COMPONENTS

Activities: 23
Services: 9
Receivers: 12
Providers: 3
Exported Activities: 3
Exported Services: 1
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-08-01 16:55:58+00:00
Valid To: 2049-08-01 16:55:58+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x4092b54819b069e29fb33672ccd89bb296587d01
Hash Algorithm: sha256
md5: c2c6593e96cad89f45b9a0c0366ee7cd
sha1: 7d72d69b88691bce55af2ea60ae28ae8b78be894
sha256: b7f8904f371a988c54f9dcd8c38efa2ecf369189c2d1d45bea974ffafa9ed62f
sha512: 1fb7ba0a6d0453bbccdc0c7e77745d79a9376e5d1a126a81ca83615fb34f4d91e1a6a6d182ff6788b6c8e32a9f42f6e387f7893ddb963e8a86a3efae5a974d9c
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: e9a10dbdf30253ce12bda0a3b14ae184b9a5f77695e2c4e97e778f6490495211
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
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.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
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	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.

PERMISSION	STATUS	INFO	DESCRIPTION
org.unchealthcare.go.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MANUFACTURER check Build.TAGS check SIM operator check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
network operator name check
possible ro.secure check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.auth0.android.provider.RedirectActivity	Schemes: @string/network_sso_scheme://, Hosts: gozio.auth0.com, gozio-dev.auth0.com, gozio-qa.us.auth0.com, gozio-mobile.us.auth0.com, gozio-stage.us.auth0.com, gozio-preprod.us.auth0.com, Path Prefixes: /android/org.unchealthcare.go/callback,

ACTIVITY	INTENT
com.goziohealth.core.ui.startup.DeepLinkActivity	Schemes: @string/default_deep_link_scheme://, @string/network_deep_link_scheme://, http://, https://, Hosts: @string/deep_link_domain_0, @string/deep_link_domain_1, @string/deep_link_domain_2, @string/deep_link_domain_3, @string/deep_link_domain_4, @string/deep_link_domain_5,

NETWORK SECURITY

HIGH: 0 | WARNING: 0 | INFO: 0 | SECURE: 0

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: 0 | WARNING: 8 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_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.
3	Activity (com.auth0.android.provider.RedirectActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity (com.goziohealth.core.ui.startup.DeepLinkActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [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.

NO	ISSUE	SEVERITY	DESCRIPTION
6	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.
7	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.
8	Activity (androidx.compose.ui.tooling.PreviewActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 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

HIGH: 1 | WARNING: 7 | INFO: 3 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES

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	L4/k.java N4/C0230f.java N4/C0254f.java N4/H.java N4/y.java Ua/C0152n.java a/C0620f.java a/C0809f.java a9/k.java c4/C1049d.java c4/C1272d.java coil/memory/MemoryCache$Key.java com/goziohealth/core/model/db/brand/BrandLabel.java com/goziohealth/core/model/db/place/MapLocation.java com/goziohealth/core/model/remote/cm/brand/CMLabel.java com/goziohealth/core/model/remote/cm/map/CMMapLocation.java com/newrelic/agent/android/SavedState.java com/newrelic/agent/android/distributedtracing/TracePayload.java com/newrelic/agent/android/harvest/AgentHealth.java com/newrelic/agent/android/harvest/HarvestConfiguration.java com/newrelic/agent/android/util/PersistentUUID.java p1/C1894q0.java p1/C2434q0.java x9/C0678e.java x9/C2959e.java
				A6/e.java A6/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				B0/i.java B0/j.java B3/e.java Ba/C0005b.java C0/ViewOnKeyListenerC0066j.java C0/p.java C0/r.java C2/d.java C4/a.java C5/f.java D1/e.java D2/e.java D2/o.java D3/E.java D3/F.java D3/K.java D3/t.java D3/x.java D6/a.java D6/d.java D6/h.java Da/l.java E2/f.java Ea/d.java F4/E.java F4/H.java F4/K.java F5/c.java F5/d.java F5/f.java H2/e.java H2/j.java H2/o.java I/f.java I0/f.java I0/h.java I2/C0126e.java I2/g.java I2/i.java I2/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				I2/n.java I2/x.java I2/z.java I3/f.java J3/a.java J4/d.java K2/a.java K2/c.java K2/d.java K2/e.java K2/f.java K2/p.java K4/d.java K4/e.java L5/AbstractC0143l.java L6/d.java Ma/k.java N2/T.java N2/Y.java N3/C0209j.java N3/C0220v.java N3/C0244v.java N3/E.java N4/A.java N4/n.java N4/q.java O4/h.java O4/i.java O5/a.java P2/h.java P4/c.java P6/b.java Q2/o.java R2/i.java R2/l.java R4/C0390h.java R4/C0392j.java R4/C0397o.java R4/C0478h.java R5/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	S1/w.java S2/c.java S3/c.java S8/c.java T3/C0457k.java T3/C0581k.java T3/v.java T4/b.java U3/q.java U4/B.java U4/C0481b.java U4/C0482c.java U4/H.java U4/i.java U4/m.java U4/q.java U4/s.java U4/w.java U6/c.java W2/o.java W4/a.java W4/g.java W4/j.java Wa/Y.java Y1/L.java Y4/s.java a0/d.java a5/h.java b3/AbstractC0972h0.java b3/C0961c.java b3/C0971h.java b3/C1004y.java b3/C1214y.java b3/H0.java b3/I0.java b3/M0.java b3/W.java b4/e.java b5/g.java c4/C1048c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				c4/l.java com/auth0/android/provider/AuthenticationActivity.java com/auth0/android/request/internal/j.java com/bumptech/glide/b.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/l.java com/bumptech/glide/n.java com/fasterxml/jackson/databind/ext/DOMSerializer.java com/fasterxml/jackson/databind/util/ClassUtil.java com/goziohealth/core/model/remote/api/appcenter/AttachmentLog.java com/goziohealth/core/model/remote/api/appcenter/ManagedLog.java com/goziohealth/search/GZMDebugResult.java com/newrelic/agent/android/AndroidAgentImpl.java com/newrelic/agent/android/NewRelic.java com/newrelic/agent/android/SavedState.java com/newrelic/agent/android/agentdata/AgentDataController.java com/newrelic/agent/android/analytics/AnalyticsControllerImpl.java com/newrelic/agent/android/analytics/EventManagerImpl.java com/newrelic/agent/android/crash/UncaughtExceptionHandler.java com/newrelic/agent/android/harvest/Harvest.java com/newrelic/agent/android/hybrid/data/DataController.java com/newrelic/agent/android/instrumentation/io/CountingInputStream.java com/newrelic/agent/android/logging/

NO	ISSUE	SEVERITY	STANDARDS	FILES
				AndroidAgentLog.java com/newrelic/agent/android/logging/ConsoleAgentLog.java com/newrelic/agent/android/rum/ApplicationLifeCycle.java com/newrelic/agent/android/sample/Sampler.java com/newrelic/agent/android/stores/SharedPrefsAnalyticsAttributeStore.java com/newrelic/agent/android/tracing/ActivityTrace.java com/newrelic/agent/android/tracing/TraceMachine.java com/newrelic/agent/android/util/ExceptionHelper.java d4/g.java d4/l.java f/e.java f3/C1331c.java f6/AbstractC1339a.java f6/AbstractC1620a.java h3/C1377e.java i4/c.java i6/C1462d.java l4/AbstractC1550j.java l6/j.java p1/O0.java p3/C2455b.java p5/C1926a.java q3/b.java q3/c.java q3/g.java q5/d.java q5/j.java s6/o.java t6/f.java w0/AbstractC2180g.java w0/AbstractC2843g.java w0/C2176c.java w0/C2839c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				w7/C2221a.java x3/C2349e.java x5/t.java x5/v.java
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	y/RunnableC2292Y.java y6/AsyncTaskC2349b.java z3/C2389k.java z3/p.java Da/d.java Da/g.java Da/k.java Da/l.java
4	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	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	D3/L.java I3/b.java J1/e.java U3/E.java com/newrelic/agent/android/instrumentation/SQLiteInstrumentation.java p5/C1926a.java q5/d.java q5/i.java q5/j.java r5/C2028f.java r5/i.java r5/o.java
5	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	I4/AbstractC1550j.java
6	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	Y1/C0584k.java
7	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	P6/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
8	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	D4/d.java X8/d.java
9	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	com/newrelic/agent/android/util/Util.java f/e.java
10	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	V8/a.java
11	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	c4/C1048c.java
12	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/newrelic/agent/android/AndroidAgentImpl.java
13	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/newrelic/agent/android/ndk/AgentNDK.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	b/O.java com/fasterxml/jackson/databind/ser/std/FileSerializer.java com/goziohealth/core/data/repository/ManifestRepository.java com/newrelic/agent/android/ndk/AgentNDK.java com/newrelic/agent/android/ndk/ManagedContext.java f9/g.java i3/J.java i3/x.java ia/C0341F.java ia/C0362a0.java ia/C0376d2.java ia/W0.java o4/C1825a.java w7/t.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	I/f.java S8/c.java com/auth0/android/provider/BrowserPicker.java z3/p.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	B3/b.java B3/e.java B3/i.java Ba/C0005b.java C7/f.java Ia/t.java J4/d.java J4/f.java Ma/k.java S2/d.java U4/q.java Wa/Y.java b9/C0213d.java c4/C1048c.java com/fasterxml/jackson/core/TokenStreamFactory.java com/goziohealth/core/data/repository/ManifestRepository.java i3/C1441E.java i3/J.java i3/m.java ia/C0441u.java q3/g.java wa/C0670f.java wa/C0673i.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	S8/c.java
00036	Get resource file from res/raw directory	reflection	R4/C0397o.java S8/c.java l4/C1543c.java
00108	Read the input stream from given URL	network command	com/newrelic/agent/android/harvest/HarvestConnection.java com/newrelic/agent/android/payload/PayloadSender.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	N3/E.java W3/c.java c4/l.java com/goziohealth/core/data/receiver/AppChoiceReceiver.java com/goziohealth/core/ui/startup/StartupActivity.java
00112	Get the date of the calendar event	collection calendar	com/fasterxml/jackson/databind/util/StdDateFormat.java
00089	Connect to a URL and receive input stream from the server	command network	D6/a.java com/bumptech/glide/load/data/l.java com/newrelic/agent/android/harvest/HarvestConnection.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/l.java
00109	Connect to a URL and get the response code	network command	D6/a.java com/bumptech/glide/load/data/l.java com/newrelic/agent/android/agentdata/AgentDataSender.java com/newrelic/agent/android/crash/CrashSender.java com/newrelic/agent/android/harvest/HarvestConnection.java
00075	Get location of the device	collection location	Wa/Y.java
00137	Get last known location of the device	location collection	Wa/Y.java
00078	Get the network operator name	collection telephony	com/newrelic/agent/android/util/Connectivity.java
00162	Create InetSocketAddress object and connecting to it	socket	Da/c.java Da/l.java com/newrelic/agent/android/util/Reachability.java

RULE ID	BEHAVIOUR	LABEL	FILES
00163	Create new Socket and connecting to it	socket	Da/c.java Da/l.java com/newrelic/agent/android/util/Reachability.java
00012	Read data and put it into a buffer stream	file	com/goziohealth/core/data/repository/ManifestRepository.java ia/C0441u.java q3/g.java
00096	Connect to a URL and set request method	command network	D6/a.java com/newrelic/agent/android/agentdata/AgentDataSender.java com/newrelic/agent/android/harvest/HarvestConnection.java
00125	Check if the given file path exist	file	X1/h0.java
00094	Connect to a URL and read data from it	command network	Ma/k.java com/newrelic/agent/android/harvest/HarvestConnection.java
00014	Read file into a stream and put it into a JSON object	file	c4/C1048c.java
00009	Put data in cursor to JSON object	file	c4/C1048c.java
00033	Query the IMEI number	collection	com/newrelic/agent/android/util/PersistentUUID.java
00046	Method reflection	reflection	Da/c.java
00026	Method reflection	reflection	Da/c.java
00114	Create a secure socket connection to the proxy address	network command	ya/C0694l.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://unc-connect-b224b.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/782236719235/namespaces/firebase:fetch?key=AIzaSyALcOU67jsp7huZ4pEsL2eO_6sUVVCc4rI. This is indicated by the response: The response code is 403

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.INTERNET, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.VIBRATE, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	5/44	android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.

Other Common Permissions:
Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
ns.adobe.com	ok	No Geolocation information available.
navis.goziohealth.com	ok	**IP:** 34.197.64.106 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
github.com	ok	**IP:** 140.82.113.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 142.250.217.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
unc-connect-b224b.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
www.slf4j.org	ok	**IP:** 31.97.181.89 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Bowness-on-Windermere **Latitude:** 54.363312 **Longitude:** -2.918590 **View:** Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.
apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
data.goziohealth.com	ok	**IP:** 54.159.132.120 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.250.74.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gle	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
www.example.com	ok	**IP:** 23.220.73.43 **Country:** Colombia **Region:** Antioquia **City:** Medellin **Latitude:** 6.251840 **Longitude:** -75.563591 **View:** Google Map

EMAILS

EMAIL	FILE
user@example.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
New Relic	Analytics	https://reports.exodus-privacy.eu.org/trackers/130
Segment	Profiling, Analytics	https://reports.exodus-privacy.eu.org/trackers/62

HARDCODED SECRETS

POSSIBLE SECRETS
"content_description_push_token_options" : "Options"
"copy_push_token" : "Copy"
"firebase_database_url" : "https://unc-connect-b224b.firebaseio.com"
"google_api_key" : "AIzaSyALcOU67jsp7huZ4pEsL2eO_6sUVVCc4rI"

POSSIBLE SECRETS
"google_crash_reporting_api_key" : "AIzaSyALcOU67jsp7huZ4pEsL2eO_6sUVVCc4rI"
"iv_gozio_api" : "bae4587284c3a87f267c0e1a9c8f9977"
"key_gozio_api" : "RsRa/ImIh3vkpXcdI0jLATnwlb/uLdQ3x8G30Ddz3wI="
"key_segment" : "6OqFol9baKJ4fLjDPNMc1w1YQiiOB/y+Y6CV4XS5/w9wPLVp/h83ONE8JFuJVvpP"
"maps_api_key" : "AIzaSyDvM2I46YVEydEAHEHnjsa4pBL0aZHeZhY"
"push_token_pending" : "Pending..."
"push_token_registered" : "Registered"
"push_token_resetting" : "Resetting..."
"reset_push_token" : "Reset"
389C9738-A761-44DE-8A66-1668CFD67DA1
97c5e095a884f51ab79e1bfbfc0bd9f1
d67afc830dab717fd163bfcb0b8b88423e9a1a3b
0add16db-0418-4fcc-a5f0-657bae540e39
09e00992cd801d0865e4789f0f707938ea00eef00dec3ca65cc6bc172903f6bd
7212a589c0f8cd3a8d6aab50ca46f49d

POSSIBLE SECRETS
7d73d21f1bd82c9e5268b6dcf9fde2cb

PLAYSTORE INFORMATION

Title: UNC Health

Score: 4.33 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** org.unchealthcare.go

Developer Details: UNC Health Care, UNC+Health+Care, None, None, unchc.news@gmail.com,

Release Date: Sep 10, 2019 **Privacy Policy:** Privacy link

Description:

At UNC Health, we are always looking for ways to improve the experience of our patients and visitors. We want to be there to help you at every step of your health care journey, including finding your way through our facilities. That is why we created the UNC Health app. This wayfinding app will make it easier for those visiting UNC Medical Center and UNC REX Healthcare by providing turn-by-turn navigation from your front door to our front desk, parking support and real time indoor guidance. The app also brings together resources to help you access care easily, whether that's seeing the urgent care location nearest you with the shortest wait times, or helping you find a provider anywhere in our system. Special features include: • GPS enabled turn-by-turn navigation to UNC Health Care locations • Find a convenient parking spot and set a parking reminder at UNC Medical Center and UNC REX Healthcare • Real-time indoor step-by-step directions to get you to where you need to go at UNC Medical Center and UNC REX Healthcare • Sign up or connect with My UNC Chart to make an appointment and for appointment reminders • Get in line for an on demand Virtual Care Now video visit with a UNC Health primary care provider 6 a.m. – 10 p.m 7 days per week, 365 days per year, without leaving your home or office. NOTE: This will not be your own primary care or specialist provider. • Find a Doctor: find information about more than 3000 UNC Health Care providers • Pay your bill online • Subscribe to UNC Health Talk to get free health tips and patient stories once a month

SCAN LOGS

Timestamp	Event	Error
2025-09-01 17:06:52	Generating Hashes	OK

2025-09-01 17:06:52	Extracting APK	OK
2025-09-01 17:06:52	Unzipping	OK
2025-09-01 17:06:52	Parsing APK with androguard	OK
2025-09-01 17:06:53	Extracting APK features using aapt/aapt2	OK
2025-09-01 17:06:53	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 17:06:55	Parsing AndroidManifest.xml	OK
2025-09-01 17:06:55	Extracting Manifest Data	OK
2025-09-01 17:06:55	Manifest Analysis Started	OK
2025-09-01 17:06:55	Reading Network Security config from network_security_config.xml	OK
2025-09-01 17:06:55	Parsing Network Security config	OK
2025-09-01 17:06:55	Performing Static Analysis on: UNC Health (org.unchealthcare.go)	OK

2025-09-01 17:06:57	Fetching Details from Play Store: org.unchealthcare.go	OK
2025-09-01 17:06:58	Checking for Malware Permissions	OK
2025-09-01 17:06:58	Fetching icon path	OK
2025-09-01 17:06:59	Library Binary Analysis Started	OK
2025-09-01 17:06:59	Reading Code Signing Certificate	OK
2025-09-01 17:06:59	Running APKiD 2.1.5	OK
2025-09-01 17:07:02	Detecting Trackers	OK
2025-09-01 17:07:03	Decompiling APK to Java with JADX	OK
2025-09-01 17:07:20	Decompiling with JADX failed, attempting on all DEX files	OK
2025-09-01 17:07:20	Decompiling classes2.dex with JADX	OK
2025-09-01 17:07:29	Decompiling classes.dex with JADX	OK

2025-09-01 17:08:06	Decompiling with JADX failed for classes.dex	OK
2025-09-01 17:08:06	Decompiling classes2.dex with JADX	OK
2025-09-01 17:08:14	Decompiling classes.dex with JADX	OK
2025-09-01 17:09:59	Decompiling with JADX failed for classes.dex	OK
2025-09-01 17:10:00	Some DEX files failed to decompile	OK
2025-09-01 17:10:00	Converting DEX to Smali	OK
2025-09-01 17:10:00	Code Analysis Started on - java_source	OK
2025-09-01 17:10:04	Android SBOM Analysis Completed	OK
2025-09-01 17:10:13	Android SAST Completed	OK
2025-09-01 17:10:13	Android API Analysis Started	OK
2025-09-01 17:10:23	Android API Analysis Completed	OK

2025-09-01 17:10:24	Android Permission Mapping Started	OK
2025-09-01 17:10:32	Android Permission Mapping Completed	OK
2025-09-01 17:10:32	Android Behaviour Analysis Started	OK
2025-09-01 17:10:44	Android Behaviour Analysis Completed	OK
2025-09-01 17:10:44	Extracting Emails and URLs from Source Code	OK
2025-09-01 17:10:48	Email and URL Extraction Completed	OK
2025-09-01 17:10:48	Extracting String data from APK	OK
2025-09-01 17:10:48	Extracting String data from Code	OK
2025-09-01 17:10:48	Extracting String values and entropies from Code	OK
2025-09-01 17:10:52	Performing Malware check on extracted domains	OK
2025-09-01 17:10:54	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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.

© 2025 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.