ANDROID STATIC ANALYSIS REPORT

app_icon

Teladoc Health Patient (3.7.2)

File Name:	com.ith.patient_112.apk
Package Name:	com.ith.patient
Scan Date:	Aug. 30, 2025, 10:16 p.m.
App Security Score:	57/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	9	1	2	1

FILE INFORMATION

File Name: com.ith.patient_112.apk
Size: 3.35MB
MD5: 88c20d17842175c0a7e220bd372d4ca7
SHA1: 2c27eb11df160ad9da0180e03e8086ea2efbe412
SHA256: 1c0fc9b91e16757e8be51840717e02376ebab3eba000051b0d6db1b95e472836

APP INFORMATION

App Name: Teladoc Health Patient
Package Name: com.ith.patient
Main Activity: com.ith.client.main.MainActivity
Target SDK: 34
Min SDK: 21
Max SDK:
Android Version Name: 3.7.2

Android Version Code: 112

APP COMPONENTS

Activities: 1
Services: 1
Receivers: 1
Providers: 3
Exported Activities: 0
Exported Services: 0
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
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: 2019-05-23 21:04:44+00:00
Valid To: 2049-05-23 21:04:44+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xf7143281742e3e6fac8d69dc50b9bcd4b436a6ab
Hash Algorithm: sha256
md5: 33abe76d21bfdeaee5c68f2c64079ac4
sha1: 41042997a2ca8b4b7825b66f62d0a9b1ac2cdc74
sha256: 103087e6f88d0989bd9a1bb5c6ae8d12d1e9f42731e1b07830af0fd046d4b671
sha512: 9a8d017a4ab4f26a3addc5f5ae412e34516b5103701a19c185ccbafe3de84dc068f9c9e6581155ff207b70c0303a332d4813fdefa2e90837b6a9168708f9ecc2
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 3d22c837ab48c78e5d6e6ea099a14508ec1f3a44812eb1cccb78dd2966216c48
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADVERTISE	dangerous	required to advertise to nearby Bluetooth devices.	Required to be able to advertise to 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.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_MICROPHONE	normal	permits foreground services with microphone use.	Allows a regular application to use Service.startForeground with the type "microphone".
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
com.ith.patient.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

<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.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible ro.secure check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.ith.client.main.MainActivity	Schemes: http://, https://, truclinicapp://, Hosts: *.visitnow.org, patient.visitnow.org, visitstaging.org, patient.visitstaging.org, master.visitstaging.org, patient.master.visitstaging.org, de.visitnow.org, patient.de.visitnow.org, ca.visitnow.org, patient.ca.visitnow.org, eu.visitnow.org, patient.eu.visitnow.org, uat.ca.visitnow.org, patient.uat.ca.visitnow.org, cat.eu.visitnow.org, patient.cat.eu.visitnow.org, patient.cat.visitnow.org, patient.cat.au.visitnow.org, patient.au.visitnow.org, patient.loadtesting.visitstaging.org, patient-ith.visitnow.org, patient-ith.master.visitstaging.org,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 1 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	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: **0** | WARNING: **5** | INFO: **1** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	com/ith/client/base/webview/ITHWebView.java com/ith/client/main/MainActivity.java com/ith/client/main/MainPresenter.java com/ith/client/main/webview/WVPresenter.java com/ith/client/service/ITHForegroundService.java d2/a.java e0/b.java i0/a.java i1/c.java io/sentry/android/core/u.java io/sentry/u5.java k/d.java l1/c.java l1/f.java moxy/PresenterStore.java n/f.java n1/b.java n1/d.java n1/e.java o1/a.java s0/a.java s0/b.java s0/c.java t/f.java t3/g.java u1/e.java v1/a.java w1/i.java z/c.java
2	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	x1/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	h3/a.java h3/b.java i3/a.java
4	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	io/sentry/android/core/e1.java
5	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	io/sentry/util/s.java
6	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	c2/b.java io/sentry/android/core/internal/util/p.java
7	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	moxy/MvpDelegate.java
8	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	c2/a.java io/sentry/android/core/internal/util/p.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	io/sentry/transport/o.java
00089	Connect to a URL and receive input stream from the server	command network	io/sentry/transport/o.java
00030	Connect to the remote server through the given URL	network	io/sentry/transport/o.java
00109	Connect to a URL and get the response code	network command	io/sentry/transport/o.java
00013	Read file and put it into a stream	file	io/sentry/android/core/SentryPerformanceProvider.java io/sentry/cache/b.java io/sentry/cache/c.java io/sentry/cache/e.java io/sentry/config/e.java io/sentry/k2.java io/sentry/m2.java io/sentry/util/e.java io/sentry/w.java okio/q.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	io/sentry/android/core/cache/b.java io/sentry/android/core/e1.java io/sentry/android/core/z.java io/sentry/cache/b.java io/sentry/cache/c.java io/sentry/cache/e.java io/sentry/k2.java io/sentry/m2.java io/sentry/p.java io/sentry/w.java io/sentry/z4.java
00012	Read data and put it into a buffer stream	file	io/sentry/cache/b.java io/sentry/cache/e.java io/sentry/config/e.java io/sentry/k2.java io/sentry/util/e.java io/sentry/w.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	c1/a.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/25	android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.INTERNET, android.permission.RECORD_AUDIO
Other Common Permissions	4/44	android.permission.BLUETOOTH, android.permission.FOREGROUND_SERVICE, android.permission.MODIFY_AUDIO_SETTINGS, 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
patient-mclarennowclinic.visitnow.org	ok	**IP:** 170.176.163.8 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
ca.visitnow.org	ok	**IP:** 170.176.163.6 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
patient.uat.ca.visitnow.org	ok	**IP:** 3.98.250.63 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map
cat.eu.visitnow.org	ok	**IP:** 35.157.234.7 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
patient-ith.visitnow.org	ok	**IP:** 170.176.163.8 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
patient.ca.visitnow.org	ok	**IP:** 170.176.163.6 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
master.visitstaging.org	ok	**IP:** 170.176.152.3 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
patient.visitstaging.org	ok	**IP:** 170.176.152.3 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
de.visitnow.org	ok	**IP:** 170.176.136.35 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
dev.visitstaging.org	ok	**IP:** 170.176.152.3 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
patient-ithdemo.master.visitstaging.org	ok	**IP:** 170.176.152.3 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
patient-upmcitaly.visitnow.org	ok	**IP:** 170.176.163.8 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
patient.eu.visitnow.org	ok	**IP:** 170.176.163.9 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
patient.master.visitstaging.org	ok	**IP:** 170.176.152.3 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
unmhealth.visitnow.org	ok	**IP:** 170.176.163.8 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
patient.pas-dev8.visitnow.org	ok	**IP:** 170.176.163.8 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
stonybrook.cat.visitnow.org	ok	**IP:** 170.176.163.15 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
patient.de.visitnow.org	ok	**IP:** 170.176.136.35 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cat.visitnow.org	ok	**IP:** 170.176.163.15 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
teladochealth.com	ok	**IP:** 104.18.39.140 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
mclarencarenow.visitnow.org	ok	**IP:** 170.176.163.8 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
patient.loadtesting.visitstaging.org	ok	**IP:** 170.176.152.1 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
patient-wmc.master.visitstaging.org	ok	**IP:** 170.176.152.3 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
upmcinitalia.cat.eu.visitnow.org	ok	**IP:** 35.157.234.7 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
patient-stonybrook.master.visitstaging.org	ok	**IP:** 170.176.152.3 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
eu.visitnow.org	ok	**IP:** 170.176.163.9 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
stonybrook.visitnow.org	ok	**IP:** 170.176.163.8 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
intouchhealth.com	ok	**IP:** 35.203.151.91 **Country:** United States of America **Region:** Oregon **City:** The Dalles **Latitude:** 45.594559 **Longitude:** -121.178680 **View:** Google Map
upmcinitalia.eu.visitnow.org	ok	**IP:** 170.176.163.9 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
visitstaging.org	ok	**IP:** 170.176.152.3 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
uat.ca.visitnow.org	ok	**IP:** 3.98.250.63 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map
patient.cat.au.visitnow.org	ok	**IP:** 54.252.21.176 **Country:** Australia **Region:** New South Wales **City:** Sydney **Latitude:** -33.867851 **Longitude:** 151.207321 **View:** Google Map
wmc.visitnow.org	ok	**IP:** 170.176.163.8 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
patient.cat.eu.visitnow.org	ok	**IP:** 35.157.234.7 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
patient.cat.visitnow.org	ok	**IP:** 170.176.163.15 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
patient-usc.master.visitstaging.org	ok	**IP:** 170.176.152.3 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
patient.visitnow.org	ok	**IP:** 170.176.163.8 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
patient-ith.master.visitstaging.org	ok	**IP:** 170.176.152.3 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
patient-mclarennowclinic.master.visitstaging.org	ok	**IP:** 170.176.152.3 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
patient.pas-dev1.visitnow.org	ok	**IP:** 170.176.163.8 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
visitnow.org	ok	**IP:** 170.176.163.8 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
patient-wmc.visitnow.org	ok	**IP:** 170.176.163.8 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
patient-ithdemo.visitnow.org	ok	**IP:** 170.176.163.8 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
patient-stonybrook.visitnow.org	ok	**IP:** 170.176.163.8 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
patient-bcvirtualvisit.master.visitstaging.org	ok	**IP:** 170.176.152.3 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
patient-usc.visitnow.org	ok	**IP:** 170.176.163.8 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
patient-upmcitaly.master.visitstaging.org	ok	**IP:** 170.176.152.3 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
pas-dev8.visitnow.org	ok	**IP:** 170.176.163.8 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
patient-bcvirtualvisit.visitnow.org	ok	**IP:** 170.176.163.8 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
patient.au.visitnow.org	ok	**IP:** 170.176.163.18 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
sentry.visitnow.org	ok	**IP:** 170.176.145.40 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
unmhealth.cat.visitnow.org	ok	**IP:** 170.176.163.15 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map
pas-dev1.visitnow.org	ok	**IP:** 170.176.163.8 **Country:** United States of America **Region:** California **City:** Goleta **Latitude:** 34.433716 **Longitude:** -119.862358 **View:** Google Map

EMAILS

EMAIL	FILE
4e6ba3cab3e2781a36bb@sentry.visitnow	com/ith/client/ITHApplication.java

TRACKERS

TRACKER	CATEGORIES	URL
Sentry	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/447

HARDCODED SECRETS

POSSIBLE SECRETS
624414ea45534e6ba3cab3e2781a36bb
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

PLAYSTORE INFORMATION

Title: Teladoc Health Patient

Score: 3.6831684 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.ith.patient

Developer Details: Teladoc, Inc., Teladoc,+Inc., None, https://teladochealth.com, support@visitnow.org,

Release Date: Sep 2, 2019 **Privacy Policy:** Privacy link

Description:

Teladoc Health is a telehealth platform that unifies virtual care delivery with a single patient experience. The Teladoc Health Patient App enables video communications with your healthcare provider on your Android device. Use of this App requires an individual invitation link delivered via email or SMS from your provider or access to a unique waiting room URL. Clicking on the invitation link or web site link will launch the App and allow access. If you are a patient, ask your doctor if you should download the Teladoc Health Patient App for your Android device. This App allows patients to: - Click a link from an appointment invitation of a visit now URL to input demographic information and complete the intake process associated with a specific visit. This process can include: - Medical questionnaires - Consent forms - Payment - Insurance

processing - Video consult with a medical provider - Patient survey, which will be available for the provider to review as a part of the visit encounter.

SCAN LOGS

Timestamp	Event	Error
2025-08-30 22:16:57	Generating Hashes	OK
2025-08-30 22:16:57	Extracting APK	OK
2025-08-30 22:16:57	Unzipping	OK
2025-08-30 22:16:57	Parsing APK with androguard	OK
2025-08-30 22:16:57	Extracting APK features using aapt/aapt2	OK
2025-08-30 22:16:57	Getting Hardcoded Certificates/Keystores	OK
2025-08-30 22:16:59	Parsing AndroidManifest.xml	OK
2025-08-30 22:16:59	Extracting Manifest Data	OK

2025-08-30 22:16:59	Manifest Analysis Started	OK
2025-08-30 22:16:59	Performing Static Analysis on: Teladoc Health Patient (com.ith.patient)	OK
2025-08-30 22:16:59	Fetching Details from Play Store: com.ith.patient	OK
2025-08-30 22:16:59	Checking for Malware Permissions	OK
2025-08-30 22:16:59	Fetching icon path	OK
2025-08-30 22:16:59	Library Binary Analysis Started	OK
2025-08-30 22:16:59	Reading Code Signing Certificate	OK
2025-08-30 22:17:00	Running APKiD 2.1.5	OK
2025-08-30 22:17:01	Detecting Trackers	OK
2025-08-30 22:17:02	Decompiling APK to Java with JADX	OK
2025-08-30 22:17:08	Converting DEX to Smali	OK

2025-08-30 22:17:08	Code Analysis Started on - java_source	OK
2025-08-30 22:17:08	Android SBOM Analysis Completed	OK
2025-08-30 22:17:14	Android SAST Completed	OK
2025-08-30 22:17:14	Android API Analysis Started	OK
2025-08-30 22:17:20	Android API Analysis Completed	OK
2025-08-30 22:17:21	Android Permission Mapping Started	OK
2025-08-30 22:17:26	Android Permission Mapping Completed	OK
2025-08-30 22:17:26	Android Behaviour Analysis Started	OK
2025-08-30 22:17:32	Android Behaviour Analysis Completed	OK
2025-08-30 22:17:32	Extracting Emails and URLs from Source Code	OK
2025-08-30 22:17:33	Email and URL Extraction Completed	OK

2025-08-30 22:17:33	Extracting String data from APK	OK
2025-08-30 22:17:33	Extracting String data from Code	OK
2025-08-30 22:17:33	Extracting String values and entropies from Code	OK
2025-08-30 22:17:33	Performing Malware check on extracted domains	OK
2025-08-30 22:17:37	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.