MOBSF

ANDROID STATIC ANALYSIS REPORT

Telehealth (4.1.0)

File Name:	com.simplepractice.video_3185.apk
Package Name:	com.simplepractice.video
Scan Date:	Sept. 1, 2025, 9 a.m.
App Security Score:	57/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	9	3	3	1

FILE INFORMATION

File Name: com.simplepractice.video_3185.apk
Size: 14.7MB
MD5: 308d81b086afec80bf6df5c4b1eaf70f
SHA1: 9695e5e9ff11c1f4ddd4b633078d5077efa498da
SHA256: 7e7eb6efae2ece297dbc91e39759ea2f4b356cae486dd6c34bf74a755c78feaf

APP INFORMATION

App Name: Telehealth
Package Name: com.simplepractice.video
Main Activity: com.simplepractice.video.welcome.WelcomeActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 4.1.0

Android Version Code: 3185

APP COMPONENTS

Activities: 10
Services: 3
Receivers: 1
Providers: 5
Exported Activities: 2
Exported Services: 0
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Los Angeles, O=SimplePractice LLC, OU=Mobile Development, CN=Oleksandr Skrypnyk
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-09-04 15:50:41+00:00
Valid To: 2039-08-29 15:50:41+00:00
Issuer: C=US, ST=California, L=Los Angeles, O=SimplePractice LLC, OU=Mobile Development, CN=Oleksandr Skrypnyk
Serial Number: 0x54088a51
Hash Algorithm: sha1
md5: a8e261e4d8064c8ea423bf53a5a086c5
sha1: 43c3ea7d2e79606bffcbcba0fa6efc127a85f71a
sha256: 21e156783077337df5136575316c3ad7fae34f197f61ddc025870fb6f70fc299
sha512: 3ac450f1956e513aeb3ea3e474a4c0ceac38952049f05c4c2e0702812daa01ca2bbb2bc9d0a31159a7468a5728a32595c7dbf9663dfff0df5b5fbedb403dbf3e
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: f468ebb00b4c0e531f7ac30ea6f1fa89bca2b7cf3b3e0143960e27b9df53c456
Found 1 unique certificates

APPLICATION PERMISSIONS

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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.BROADCAST_STICKY	normal	send sticky broadcast	Allows an application to send sticky broadcasts, which remain after the broadcast ends. Malicious applications can make the phone slow or unstable by causing it to use too much memory.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
com.simplepractice.video.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference

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
network operator name check
possible ro.secure check</td></tr>
<tr><td>Compiler</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.simplepractice.video.welcome.WelcomeActivity	Schemes: simplepracticevideo://, https://, Hosts: room, simplepractice-video.m03.staging.simplepractice.com, simplepractice.page.link, video.simplepractice.com,
com.simplepractice.auth.AuthActivity	Schemes: telehealth-internal://,

NETWORK SECURITY

HIGH: **0** | WARNING: **1** | INFO: **0** | SECURE: **0**

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	warning	Base config is configured to trust system certificates.

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 3 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	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.
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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Activity (com.simplepractice.auth.AuthActivity) 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 (net.openid.appauth.RedirectUriReceiverActivity) 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 (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: **3** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				C0/b.java C2/a.java C2/b.java C2/c.java F1/A.java F1/i.java F1/l.java F1/m.java F1/p.java F1/w.java

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	G/u.java H1/a.java H2/d.java I/d.java I1/AbstractBinderC0604a.java I1/AbstractC0606c.java I1/AbstractC0627y.java I1/B.java I1/N.java I1/Q.java I1/S.java I1/T.java I1/V.java I1/b0.java I1/f0.java K2/f.java K2/n.java L1/b.java N2/g.java P4/a.java R/d.java S/c.java S/o.java T1/a.java U/f.java W1/f.java X/a.java X/c.java X/d.java X/f.java X1/a.java a4/h.java c0/d.java com/biba/bibacommon/ProxyConfig.java com/bugsnag/android/C0986q0.java com/bugsnag/android/I.java com/pairip/SignatureCheck.java com/pairip/VMRunner.java com/pairip/licensecheck/LicenseActivity.java com/pairip/licensecheck/LicenseClient.ja

NO	ISSUE	SEVERITY	STANDARDS	FILES
				va com/twilio/video/Logger.java com/xodee/client/audio/audioclient/AudioClient.java d/AbstractC1096d.java d3/AbstractC1105d.java d5/e.java e0/x.java e4/C1133b.java h0/AbstractC1254e.java i2/AbstractC1282a.java k2/C1317d.java l0/C1361c.java l2/AbstractC1365b.java n2/C1401g.java s0/C1741c.java s2/k.java tvi/webrtc/DefaultVideoEncoderFactory.java u2/p.java w/B.java w/J.java w5/a.java x1/C1887b.java y/K.java
2	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	Q4/B.java h5/d.java h5/h.java u4/AbstractC1813a.java u4/C1814b.java v4/C1836a.java
3	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	L3/b.java R0/c.java com/bugsnag/android/C0961h0.java com/bugsnag/android/C0968j1.java s1/g.java y1/k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	c5/g.java c5/h.java c5/m.java c5/n.java
5	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	com/simplepractice/shared/ui/session/ui/messaging/ChatMessageItemView.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	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	c3/e.java p1/C1654e.java
7	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/bugsnag/android/RootDetector.java u2/AbstractC1808c.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	I1/i0.java K3/c.java com/simplepractice/shared/ui/waitingroom/SessionPreviewActivity.java com/simplepractice/video/welcome/WelcomeActivity.java i3/e.java net/openid/appauth/d.java t3/C1772c.java
00191	Get messages in the SMS inbox	sms	com/simplepractice/video/welcome/WelcomeActivity.java
00056	Modify voice volume	control	org/amazon/chime/webrtc/audio/WebRtcAudioTrack.java org/amazon/chime/webrtc/voiceengine/WebRtcAudioTrack.java tvi/webrtc/audio/WebRtcAudioTrack.java tvi/webrtc/voiceengine/WebRtcAudioTrack.java
00091	Retrieve data from broadcast	collection	net/openid/appauth/AuthorizationManagementActivity.java
00102	Set the phone speaker on	command	k1/C1309a.java n1/e.java
00036	Get resource file from res/raw directory	reflection	K3/c.java Q0/e.java t3/C1772c.java
00013	Read file and put it into a stream	file	A1/b.java C1/i.java com/bugsnag/android/J0.java com/bugsnag/android/RootDetector.java com/bugsnag/android/u1.java k5/N.java p4/d.java y1/r.java

RULE ID	BEHAVIOUR	LABEL	FILES
00161	Perform accessibility service action on accessibility node info	accessibility service	e0/x.java
00173	Get bounds in screen of an AccessibilityNodeInfo and perform action	accessibility service	e0/x.java
00022	Open a file from given absolute path of the file	file	B1/d.java L0/a.java com/bugsnag/android/C0997v.java com/bugsnag/android/D0.java com/bugsnag/android/ndk/NativeBridge.java
00162	Create InetSocketAddress object and connecting to it	socket	c5/f.java c5/n.java
00163	Create new Socket and connecting to it	socket	c5/f.java c5/n.java
00183	Get current camera parameters and change the setting.	camera	com/twilio/video/CameraCapturer.java org/amazon/chime/webrtc/Camera1Session.java tvi/webrtc/Camera1Session.java
00096	Connect to a URL and set request method	command network	d3/C1103b.java r1/j.java r1/l.java
00089	Connect to a URL and receive input stream from the server	command network	com/bugsnag/android/J.java d3/C1103b.java r1/j.java r1/l.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	com/bugsnag/android/J.java d3/C1103b.java r1/j.java r1/l.java
00094	Connect to a URL and read data from it	command network	d3/C1103b.java
00108	Read the input stream from given URL	network command	d3/C1103b.java
00208	Capture the contents of the device screen	collection screen	org/amazon/chime/webrtc/ScreenCapturerAndroid.java tvi/webrtc/ScreenCapturerAndroid.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	I1/i0.java
00078	Get the network operator name	collection telephony	c3/l.java
00009	Put data in cursor to JSON object	file	c3/e.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://telehealth-simplepractice.firebaseio.com

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/424147367048/namespaces/firebase:fetch?key=AIzaSyD8Ubeyjh2GSXzOVb8aE7PNOKp70fJMHt8. This is indicated by the response: The response code is 403

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.RECORD_AUDIO, android.permission.CAMERA, android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_PHONE_STATE, android.permission.ACCESS_WIFI_STATE
Other Common Permissions	4/44	android.permission.FOREGROUND_SERVICE, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.BLUETOOTH, android.permission.BROADCAST_STICKY

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
telehealth-simplepractice.firebaseio.com	ok	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
sessions.bugsnag.com	ok	**IP:** 35.190.88.7 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
docs.bugsnag.com	ok	**IP:** 18.155.173.70 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
video.simplepractice.com	ok	**IP:** 54.191.145.95 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
developer.android.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
secure.simplepractice.com	ok	**IP:** 35.155.44.99 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
api.mixpanel.com	ok	**IP:** 107.178.240.159 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
nearest-media-region.l.chime.aws	ok	**IP:** 99.77.189.2 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
plus.google.com	ok	**IP:** 216.58.211.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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
notify.bugsnag.com	ok	**IP:** 35.186.205.6 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.114.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	F1/v.java

TRACKERS

TRACKER	CATEGORIES	URL
Bugsnag	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/207

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://telehealth-simplepractice.firebaseio.com"
"google_api_key" : "AIzaSyD8Ubeyjh2GSXzOVb8aE7PNOKp70fJMHt8"
"google_crash_reporting_api_key" : "AIzaSyD8Ubeyjh2GSXzOVb8aE7PNOKp70fJMHt8"
759b1054a8013b791bfed66c8787fc12
85053bf24bba75239b16a601d9387e17
96990def30f5890559bfc12626b1a42d676b2b78a3f673664c3a9f886e205774
db3222ee3091a0736318a5876f43d3d2ff9cf1d126b41eb3c8413d0a41c6eccb
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
Vn3kj4pUblROi2S+QfRRL9nhsaO2uoHQg6+dpEtxdTE=

PLAYSTORE INFORMATION

Title: Telehealth by SimplePractice

Score: 4.469533 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.simplepractice.video

Developer Details: SimplePractice, SimplePractice, None, https://www.simplepractice.com, support@simplepractice.com,

Release Date: May 3, 2018 **Privacy Policy:** Privacy link

Description:

Attend your appointment without leaving your home or office, or car, or private outdoor spot. With Telehealth by SimplePractice, clients and clinicians can participate in 100% secure, HIPAA-compliant therapy sessions from anywhere. Start video appointments instantly, no login or password required.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 09:00:59	Generating Hashes	OK
2025-09-01 09:00:59	Extracting APK	OK
2025-09-01 09:00:59	Unzipping	OK
2025-09-01 09:01:00	Parsing APK with androguard	OK
2025-09-01 09:01:00	Extracting APK features using aapt/aapt2	OK
2025-09-01 09:01:00	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 09:01:02	Parsing AndroidManifest.xml	OK

2025-09-01 09:01:02	Extracting Manifest Data	OK
2025-09-01 09:01:02	Manifest Analysis Started	OK
2025-09-01 09:01:03	Reading Network Security config from network_security_config.xml	OK
2025-09-01 09:01:03	Parsing Network Security config	OK
2025-09-01 09:01:03	Performing Static Analysis on: Telehealth (com.simplepractice.video)	OK
2025-09-01 09:01:04	Fetching Details from Play Store: com.simplepractice.video	OK
2025-09-01 09:01:06	Checking for Malware Permissions	OK
2025-09-01 09:01:06	Fetching icon path	OK
2025-09-01 09:01:06	Library Binary Analysis Started	OK
2025-09-01 09:01:06	Reading Code Signing Certificate	OK
2025-09-01 09:01:06	Running APKiD 2.1.5	OK

2025-09-01 09:01:09	Detecting Trackers	OK
2025-09-01 09:01:10	Decompiling APK to Java with JADX	OK
2025-09-01 09:01:20	Converting DEX to Smali	OK
2025-09-01 09:01:20	Code Analysis Started on - java_source	OK
2025-09-01 09:01:21	Android SBOM Analysis Completed	OK
2025-09-01 09:01:24	Android SAST Completed	OK
2025-09-01 09:01:24	Android API Analysis Started	OK
2025-09-01 09:01:27	Android API Analysis Completed	OK
2025-09-01 09:01:28	Android Permission Mapping Started	OK
2025-09-01 09:01:34	Android Permission Mapping Completed	OK
2025-09-01 09:01:34	Android Behaviour Analysis Started	OK

2025-09-01 09:01:39	Android Behaviour Analysis Completed	OK
2025-09-01 09:01:39	Extracting Emails and URLs from Source Code	OK
2025-09-01 09:01:40	Email and URL Extraction Completed	OK
2025-09-01 09:01:40	Extracting String data from APK	OK
2025-09-01 09:01:40	Extracting String data from Code	OK
2025-09-01 09:01:40	Extracting String values and entropies from Code	OK
2025-09-01 09:01:42	Performing Malware check on extracted domains	OK
2025-09-01 09:01:46	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.