MOBSF

ANDROID STATIC ANALYSIS REPORT

SNAP Resupply (4.1.5)

File Name:	com.snapworx.snapmobile_102.apk
Package Name:	com.snapworx.snapmobile
Scan Date:	Sept. 1, 2025, 9:20 a.m.
App Security Score:	**62/100 (LOW RISK)**
Grade:	A

FINDINGS SEVERITY

HIGH	⚠ MEDIUM	INFO	✓ SECURE	HOTSPOT
1	4	3	2	1

FILE INFORMATION

File Name: com.snapworx.snapmobile_102.apk
Size: 24.49MB
MD5: 6c6eb9241b005c316e87776d0f563c95
SHA1: aba37634d22e39d5226be7d18e90eb6ef18fc12d
SHA256: 25957c8a8203fdac2e819b74869a601a7de417d34ef3dcc9235e215bfeb83322

APP INFORMATION

App Name: SNAP Resupply
Package Name: com.snapworx.snapmobile
Main Activity: crc6450cac17453c244da.MainActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 4.1.5
Android Version Code: 102

APP COMPONENTS

Activities: 3
Services: 5
Receivers: 4
Providers: 4
Exported Activities: 0
Exported Services: 0
Exported Receivers: 2
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=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-01-07 18:14:33+00:00
Valid To: 2049-01-07 18:14:33+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x592dce92a575d118ad4409911a3ee2de9711b54c
Hash Algorithm: sha256
md5: 4bd63f8cb8016193bdc8e885531cf415
sha1: 16e86e20049689cb2a4a0e8981be31a75d99135c
sha256: a9863c86dcb0885cea6835a78e0c04ca570461ad350c7d8ed0937a885139d912
sha512: 5dbbf956b9745326a5db7175261b693adbb72d6b6c23a1672ba1191da8213120422378c1fb520ba251aa18fec829da70ccd3ae54aef4c1867633525bfb14d1af
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 3c75e2430f854e20a88cf0e26ba5b3865fce38c171118559b225ccb43582b379
Found 1 unique certificates
```

APPLICATION PERMISSIONS

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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.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.
com.snapworx.snapmobile.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>6c6eb9241b005c316e87776d0f563c95.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table>
</td></tr>
</table>

<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.MANUFACTURER 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>Anti-VM Code</td><td>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

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: **1** | WARNING: **2** | 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	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.
3	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.

CODE ANALYSIS

HIGH: **0** | WARNING: **1** | INFO: **2** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.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	unner.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/ResourceUriLoader.java com/bumptech/glide/load/model/StreamEncoder.java com/bumptech/glide/load/resource/DefaultOnHeaderDecodedListener.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SingletonConnectivityRe

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/manager/SingletonConnectivityReceiver.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/microsoft/maui/glide/GlideLogging.java mono/android/incrementaldeployment/IncrementalClassLoader.java
2	This app listens to Clipboard changes. Some malware also listen to Clipboard changes.	info	OWASP MASVS: MSTG-PLATFORM-4	mono/android/content/ClipboardManager_OnPrimaryClipChangedListenerImplementor.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	com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/manager/RequestManagerRetriever.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/resource/bitmap/ImageReader.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://snapworx-2d7c4.firebaseio.com

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/883228298911/namespaces/firebase:fetch?key=AIzaSyAJon9HRVS5uoLch-tuxPRoPHMQ2xKtK7Q. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.CAMERA, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.WAKE_LOCK
Other Common Permissions	1/44	com.google.android.c2dm.permission.RECEIVE

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
snapworx-2d7c4.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

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://snapworx-2d7c4.firebaseio.com"
"google_api_key" : "AIzaSyAJon9HRVS5uoLch-tuxPRoPHMQ2xKtK7Q"
"google_crash_reporting_api_key" : "AIzaSyAJon9HRVS5uoLch-tuxPRoPHMQ2xKtK7Q"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
686479766013060971498190079908139321726943530014330540939446345918554318339765539424505774633321719753296399637136332111386476861244038034037280889270700 5449
23456789abcdefghjkmnpqrstvwxyz

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
115792089210356248762697446949407573529996955224135760342422259061068512044369
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
115792089210356248762697446949407573530086143415290314195533631308867097853951
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

PLAYSTORE INFORMATION

Title: SNAP Resupply

Score: 4.2909093 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.snapworx.snapmobile

Developer Details: Brightree LLC, Brightree+LLC, None, http://www.snapworxllc.com, PatientSupport@snapworx.com,

Release Date: Jan 7, 2019 **Privacy Policy:** Privacy link

Description:

SNAP Resupply allows patients to easily order their home medical supplies through the convenience of our mobile app. You can order supplies, track shipments, understand when you will next be eligible, change your insurance, update your contact information and more! If you are a patient who regularly receives home medical supplies and you want more control of the process – download the SNAP Resupply app today!

☰ SCAN LOGS

Timestamp	Event	Error
2025-09-01 09:20:39	Generating Hashes	OK
2025-09-01 09:20:39	Extracting APK	OK
2025-09-01 09:20:39	Unzipping	OK
2025-09-01 09:20:40	Parsing APK with androguard	OK
2025-09-01 09:20:40	Extracting APK features using aapt/aapt2	OK

2025-09-01 09:20:40	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 09:20:41	Parsing AndroidManifest.xml	OK
2025-09-01 09:20:42	Extracting Manifest Data	OK
2025-09-01 09:20:42	Manifest Analysis Started	OK
2025-09-01 09:20:42	Performing Static Analysis on: SNAP Resupply (com.snapworx.snapmobile)	OK
2025-09-01 09:20:42	Fetching Details from Play Store: com.snapworx.snapmobile	OK
2025-09-01 09:20:42	Checking for Malware Permissions	OK
2025-09-01 09:20:42	Fetching icon path	OK
2025-09-01 09:20:42	Library Binary Analysis Started	OK
2025-09-01 09:20:42	Reading Code Signing Certificate	OK
2025-09-01 09:20:43	Running APKiD 2.1.5	OK

2025-09-01 09:20:47	Detecting Trackers	OK
2025-09-01 09:20:49	Decompiling APK to Java with JADX	OK
2025-09-01 09:21:05	Converting DEX to Smali	OK
2025-09-01 09:21:05	Code Analysis Started on - java_source	OK
2025-09-01 09:21:06	Android SBOM Analysis Completed	OK
2025-09-01 09:21:09	Android SAST Completed	OK
2025-09-01 09:21:09	Android API Analysis Started	OK
2025-09-01 09:21:12	Android API Analysis Completed	OK
2025-09-01 09:21:12	Android Permission Mapping Started	OK
2025-09-01 09:21:14	Android Permission Mapping Completed	OK

2025-09-01 09:21:14	Android Behaviour Analysis Started	OK
2025-09-01 09:21:17	Android Behaviour Analysis Completed	OK
2025-09-01 09:21:17	Extracting Emails and URLs from Source Code	OK
2025-09-01 09:21:18	Email and URL Extraction Completed	OK
2025-09-01 09:21:18	Extracting String data from APK	OK
2025-09-01 09:21:18	Extracting String data from Code	OK
2025-09-01 09:21:18	Extracting String values and entropies from Code	OK
2025-09-01 09:21:21	Performing Malware check on extracted domains	OK
2025-09-01 09:21:22	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.