ANDROID STATIC ANALYSIS REPORT

app_icon

🤖 Beta-Medicate (7)

File Name:	com.BetaMedicate.beta_medicate_7.apk
Package Name:	com.BetaMedicate.beta_medicate
Scan Date:	Aug. 28, 2025, 10:34 p.m.
App Security Score:	**54/100 (MEDIUM RISK)**
Grade:	**B**

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	3	0	1	0

FILE INFORMATION

File Name: com.BetaMedicate.beta_medicate_7.apk
Size: 12.48MB
MD5: f719c82fd780f12dfc43bd703d9d4883
SHA1: 23e4d22c313a425a5f5153fb7fb8435d8f948eec
SHA256: 6b899ddc8a197397331325b38297c637d5da80b5f6979dbbf9a5f860344c33b9

APP INFORMATION

App Name: Beta-Medicate
Package Name: com.BetaMedicate.beta_medicate
Main Activity: com.example.beta_medicate.Splash_activity
Target SDK: 34
Min SDK: 21
Max SDK:
Android Version Name: 7
Android Version Code: 7

▦ APP COMPONENTS

Activities: 346
Services: 0
Receivers: 1
Providers: 1
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: 2023-08-03 13:50:52+00:00
Valid To: 2053-08-03 13:50:52+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x9c4c0067fc0a555524dce6b8c0ebdec4c4a03090
Hash Algorithm: sha256
md5: fac5b980991d1f9f3071e7849dfb8d0d
sha1: 9781752fde8cf6ce28e4a48547352e58ee303915
sha256: d3c852c4c64e71c7d3c6e9ef7d1030728fa9db833c2be59e9916a2f75042bde6
sha512: 588b0a655a1ac63710f63d8117cea95340c8be19bb7a5a24bea8ebd8f6f92e96515dfda17884ac7c0cea924062ae6364f8aaef368ffc0d15f2544c95a428e298
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: a7d78e16c278b787c3d08d5b47fde1ed44dfa6d0d3afba387acc25ce77284268
Found 1 unique certificates

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
com.BetaMedicate.beta_medicate.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

🔎 APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><td>FINDINGS</td><td>DETAILS</td></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>

🔒 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: **2** | 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.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	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

NO	ISSUE	SEVERITY	STANDARDS	FILES

🪪 NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

⠿ ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	0/25	
Other Common Permissions	0/44	

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

▶ PLAYSTORE INFORMATION

Title: Beta-Medicate

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

Developer Details: BioProtocol, 6704588962345395386, None, None, Steinerheim.Corp@proton.me,

Release Date: Aug 3, 2023 **Privacy Policy:** Privacy link

Description:

Steinerheim Corp. introduces Beta-Medicate, a comprehensive medical resource set for educational purposes only and designed for students, professionals, and enthusiasts alike. Delivering an extensive range of information across four critical domains of medical knowledge: Anatomy, Physiology, Pathology, and Pharmacology. Anatomy: Dive deep into the structures of the human body with our extensive descriptions of organs, systems, and tissues and explore our illustrative anatomical models to grasp the complexities of human anatomy with clarity and precision. Physiology: Understand how the body's systems function and interact with our in-depth physiology content. Our app offers comprehensive explanations of physiological processes, including homeostasis, organ function, and systemic interactions, helping you connect theoretical knowledge with practical understanding. Pathology: Our app offers extensive information about various diseases and conditions in the pathology section. Access detailed information on disease mechanisms, symptoms, diagnostics, and treatment options. Pharmacology: Master the science of drugs and their effects with our pharmacology module. From drug classifications and mechanisms of action to side effects and interactions, Beta-Medicate provides essential information to enhance your pharmacological knowledge. Key Features: - Detailed descriptions - Offline Access - Illustrative Anatomical modules (more are in development) Elevate your medical education with Beta-Medicate, where cutting-edge technology meets in-depth medical knowledge.

☰ SCAN LOGS

Timestamp	Event	Error
2025-08-28 22:34:27	Generating Hashes	OK
2025-08-28 22:34:27	Extracting APK	OK
2025-08-28 22:34:27	Unzipping	OK
2025-08-28 22:34:28	Parsing APK with androguard	OK

2025-08-28 22:34:28	Extracting APK features using aapt/aapt2	OK
2025-08-28 22:34:28	Getting Hardcoded Certificates/Keystores	OK
2025-08-28 22:34:29	Parsing AndroidManifest.xml	OK
2025-08-28 22:34:29	Extracting Manifest Data	OK
2025-08-28 22:34:29	Manifest Analysis Started	OK
2025-08-28 22:34:29	Performing Static Analysis on: Beta-Medicate (com.BetaMedicate.beta_medicate)	OK
2025-08-28 22:34:30	Fetching Details from Play Store: com.BetaMedicate.beta_medicate	OK
2025-08-28 22:34:31	Checking for Malware Permissions	OK
2025-08-28 22:34:31	Fetching icon path	OK
2025-08-28 22:34:31	Library Binary Analysis Started	OK
2025-08-28 22:34:32	Reading Code Signing Certificate	OK

2025-08-28 22:34:32	Running APKiD 2.1.5	OK
2025-08-28 22:34:35	Detecting Trackers	OK
2025-08-28 22:34:36	Decompiling APK to Java with JADX	OK
2025-08-28 22:34:44	Converting DEX to Smali	OK
2025-08-28 22:34:44	Code Analysis Started on - java_source	OK
2025-08-28 22:34:47	Android SBOM Analysis Completed	OK
2025-08-28 22:34:49	Android SAST Completed	OK
2025-08-28 22:34:49	Android API Analysis Started	OK
2025-08-28 22:34:54	Android API Analysis Completed	OK
2025-08-28 22:34:55	Android Permission Mapping Started	OK
2025-08-28 22:34:56	Android Permission Mapping Completed	OK

2025-08-28 22:34:56	Android Behaviour Analysis Started	OK
2025-08-28 22:34:59	Android Behaviour Analysis Completed	OK
2025-08-28 22:34:59	Extracting Emails and URLs from Source Code	OK
2025-08-28 22:35:03	Email and URL Extraction Completed	OK
2025-08-28 22:35:03	Extracting String data from APK	OK
2025-08-28 22:35:03	Extracting String data from Code	OK
2025-08-28 22:35:03	Extracting String values and entropies from Code	OK
2025-08-28 22:35:10	Performing Malware check on extracted domains	OK
2025-08-28 22:35:10	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.