MOBSF

ANDROID STATIC ANALYSIS REPORT

Anatomy Learning (2.1.449)

File Name:	com.AnatomyLearning.Anatomy3DViewer3_449.apk
Package Name:	com.AnatomyLearning.Anatomy3DViewer3
Scan Date:	Aug. 28, 2025, 10:33 p.m.
App Security Score:	38/100 (HIGH RISK)
Grade:	C

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	3	2	1	0

FILE INFORMATION

File Name: com.AnatomyLearning.Anatomy3DViewer3_449.apk
Size: 127.87MB
MD5: 34a6aac45a1497c23321113bcb644e94
SHA1: 0a02e8226931467310b5d00d905dff5ab804f5a2
SHA256: 0969131d5d185c87523000ee93372012556803185ec8eceefb67c0393a54556f

APP INFORMATION

App Name: Anatomy Learning
Package Name: com.AnatomyLearning.Anatomy3DViewer3
Main Activity: com.unity3d.player.UnityPlayerActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 2.1.449
Android Version Code: 449

APP COMPONENTS

Activities: 5
Services: 2
Receivers: 3
Providers: 2
Exported Activities: 0
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: CN=Rodrigo Blanco Salado, OU=AnatomyLearning, O=AnatomyLearning.com, L=Valladolid, ST=SPAIN, C=47014
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-03-20 17:39:11+00:00
Valid To: 2064-03-07 17:39:11+00:00
Issuer: CN=Rodrigo Blanco Salado, OU=AnatomyLearning, O=AnatomyLearning.com, L=Valladolid, ST=SPAIN, C=47014
Serial Number: 0x42809e65
Hash Algorithm: sha1
md5: 7d6eacc175ac226605f9df4d765f332f
sha1: 98e74bf503b988c249fea7feb4d02347f184d73f
sha256: 78005241986494eaff9536b47b751f0dbd83d029d60fbbd039041f6bcf396808
sha512: 076ce3ec372e72ac3a816e78e507906138fdcccfe216830e0757bc8d1f88f555dba83ec1ff20626297de88d01d0a79ce0384c7f5b965fd78730594c6158606b6
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 96d9035087029dd9eded7755c2115b1f4b79ea7466f2bdc58a826a444762d3b6
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check FINDINGS: Compiler — DETAILS: dexlib 2.x

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

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: 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	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.

NO	ISSUE	SEVERITY	DESCRIPTION
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

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

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	bitter/jnibridge/JNIBridge.java com/pairip/SignatureCheck.java com/pairip/VMRunner.java com/pairip/licensecheck3/LicenseClientV3.java com/unity3d/player/f.java com/unity3d/player/n.java com/yasirkula/unity/NativeShare.java com/yasirkula/unity/NativeShareCustomShareDialog.java com/yasirkula/unity/NativeShareFragment.java org/fmod/FMODAudioDevice.java org/fmod/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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/unity3d/player/UnityPlayer.java
3	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/unity/purchasing/BuildConfig.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/unity3d/player/n.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	2/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE
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.

HARDCODED SECRETS

POSSIBLE SECRETS
Vn3kj4pUblROi2S+QfRRL9nhsaO2uoHQg6+dpEtxdTE=
eABSQZhklOr/lTa0e3UfDb2D0CnWD7vQOQQfa885aAg=

PLAYSTORE INFORMATION

Title: Anatomy Learning - 3D Anatomy

Score: 4.335628 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.AnatomyLearning.Anatomy3DViewer3

Developer Details: 3D Medical OU, 5287006214478446580, None, http://anatomylearning.com, contact@anatomylearning.com,

Release Date: Mar 20, 2014 **Privacy Policy:** Privacy link

Description:

A true and totally 3D app for studying human anatomy, built on an advanced interactive 3D touch interface. Features: ★ You can rotate models to any angles and zoom in

and out ★ Remove structures to reveal the anatomical structures below them. ★ 3D location quizzes to test your knowledge ★ Switch on/off different anatomy systems ★ Both male and female reproductive systems are available ★ Support Spanish, French, German, Polish, Russian, Portuguese, Chinese and Japanese. Contents: ★ Bones ★ Ligaments ★ Joints ★ Muscles ★ Circulation (arteries, vein and heart) ★ Central nervous system ★ Peripheral nervous system ★ Sense organs ★ Respiratory ★ Digestive ★ Urinary ★ Reproductive (both male and female)

SCAN LOGS

Timestamp	Event	Error
2025-08-28 22:33:55	Generating Hashes	OK
2025-08-28 22:33:55	Extracting APK	OK
2025-08-28 22:33:55	Unzipping	OK
2025-08-28 22:33:55	Parsing APK with androguard	OK
2025-08-28 22:33:55	Extracting APK features using aapt/aapt2	OK
2025-08-28 22:33:55	Getting Hardcoded Certificates/Keystores	OK
2025-08-28 22:33:57	Parsing AndroidManifest.xml	OK

2025-08-28 22:33:57	Extracting Manifest Data	OK
2025-08-28 22:33:57	Manifest Analysis Started	OK
2025-08-28 22:33:57	Performing Static Analysis on: Anatomy Learning (com.AnatomyLearning.Anatomy3DViewer3)	OK
2025-08-28 22:33:58	Fetching Details from Play Store: com.AnatomyLearning.Anatomy3DViewer3	OK
2025-08-28 22:33:59	Checking for Malware Permissions	OK
2025-08-28 22:33:59	Fetching icon path	OK
2025-08-28 22:33:59	Library Binary Analysis Started	OK
2025-08-28 22:33:59	Reading Code Signing Certificate	OK
2025-08-28 22:33:59	Running APKiD 2.1.5	OK
2025-08-28 22:34:03	Detecting Trackers	OK
2025-08-28 22:34:04	Decompiling APK to Java with JADX	OK

2025-08-28 22:34:14	Converting DEX to Smali	OK
2025-08-28 22:34:14	Code Analysis Started on - java_source	OK
2025-08-28 22:34:14	Android SBOM Analysis Completed	OK
2025-08-28 22:34:17	Android SAST Completed	OK
2025-08-28 22:34:17	Android API Analysis Started	OK
2025-08-28 22:34:20	Android API Analysis Completed	OK
2025-08-28 22:34:20	Android Permission Mapping Started	OK
2025-08-28 22:34:22	Android Permission Mapping Completed	OK
2025-08-28 22:34:22	Android Behaviour Analysis Started	OK
2025-08-28 22:34:25	Android Behaviour Analysis Completed	OK
2025-08-28 22:34:25	Extracting Emails and URLs from Source Code	OK

2025-08-28 22:34:25	Email and URL Extraction Completed	OK
2025-08-28 22:34:25	Extracting String data from APK	OK
2025-08-28 22:34:25	Extracting String data from Code	OK
2025-08-28 22:34:25	Extracting String values and entropies from Code	OK
2025-08-28 22:34:26	Performing Malware check on extracted domains	OK
2025-08-28 22:34:26	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.