MOBSF

ANDROID STATIC ANALYSIS REPORT

V. Anatomy (3.01)

File Name:	com.graphicvizion.visualAnatomy3D_70.apk
Package Name:	com.graphicvizion.visualAnatomy3D
Scan Date:	Aug. 29, 2025, 11:19 p.m.
App Security Score:	53/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	4	2	1	1

FILE INFORMATION

File Name: com.graphicvizion.visualAnatomy3D_70.apk
Size: 28.96MB
MD5: 2099ab836ce5be3267c58c4fc4860160
SHA1: 16a75119d98f10fcb8e70397925771a665cea3c1
SHA256: 2dfd8b5875cb9a259404a5d947f6c07b0d878c3501642155810ba144af650895

APP INFORMATION

App Name: V. Anatomy
Package Name: com.graphicvizion.visualAnatomy3D
Main Activity: com.unity3d.player.UnityPlayerActivity
Target SDK: 35
Min SDK: 28
Max SDK:
Android Version Name: 3.01
Android Version Code: 70

APP COMPONENTS

Activities: 5
Services: 4
Receivers: 1
Providers: 1
Exported Activities: 0
Exported Services: 1
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
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: 2024-01-29 11:05:57+00:00
Valid To: 2054-01-29 11:05:57+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xb0f1d0048cd199e52ae660073539a35e11d3d5f0
Hash Algorithm: sha256
md5: 5f2651d59275be6b31195f64f68e4689
sha1: 5ba68b09418e7ec71cc387e8ceb6a0fdf47adc9d
sha256: 72bae25d1efc8a935b8ea3d947ba4da1e62fde1ed02010c59e9267242cdbcfe1
sha512: 3bdff45892e5c7cebf0af4b5fa795d3df9165845db08a574353bfaf08b4bb6db9cb479d20f7b3e74b3e9757d5694c0e5e33c98f35a898d20934fe6f8fb8fb8b8
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 187c20eb7b85f44758073618fdda0f3a15576de3e34e1817e0422313ba34e0f7
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MANUFACTURER check Build.DEVICE check Build.TAGS check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</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: 0 | WARNING: 3 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 9, minSdk=28]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. 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.
3	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

CODE ANALYSIS

HIGH: 1 | WARNING: 1 | 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/a.java com/unity3d/player/AbstractC0050x.java com/unity3d/player/ViewOnHoverListenerC0032n0.java com/yasirkula/unity/NativeGallery.java com/yasirkula/unity/NativeGalleryMediaPickerFragment.java com/yasirkula/unity/NativeGalleryMediaPickerResultOperation.java com/yasirkula/unity/NativeGalleryPermissionFragment.java com/yasirkula/unity/NativeGalleryUtils.java org/fmod/FMODAudioDevice.java org/fmod/a.java
2	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	com/yasirkula/unity/NativeGallery.java com/yasirkula/unity/NativeGalleryUtils.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/SmileSoft/unityplugin/BuildConfig.java com/unity/purchasing/BuildConfig.java
4	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

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00192	Get messages in the SMS inbox	sms	com/yasirkula/unity/NativeGalleryUtils.java
00022	Open a file from given absolute path of the file	file	com/yasirkula/unity/NativeGallery.java com/yasirkula/unity/NativeGalleryMediaPickerResultOperation.java com/yasirkula/unity/NativeGalleryUtils.java
00013	Read file and put it into a stream	file	com/unity3d/player/t1.java com/yasirkula/unity/NativeGalleryMediaPickerResultOperation.java com/yasirkula/unity/NativeGalleryUtils.java
00191	Get messages in the SMS inbox	sms	com/yasirkula/unity/NativeGalleryUtils.java
00189	Get the content of a SMS message	sms	com/yasirkula/unity/NativeGalleryMediaPickerResultOperation.java
00188	Get the address of a SMS message	sms	com/yasirkula/unity/NativeGalleryMediaPickerResultOperation.java
00200	Query data from the contact list	collection contact	com/yasirkula/unity/NativeGalleryMediaPickerResultOperation.java
00201	Query data from the call log	collection calllog	com/yasirkula/unity/NativeGalleryMediaPickerResultOperation.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/yasirkula/unity/NativeGalleryMediaPickerResultOperation.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	4/25	android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE
Other Common Permissions	1/44	android.permission.FOREGROUND_SERVICE

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: Visual Anatomy 3D - Human body

Score: 3.6190476 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.graphicvizion.visualAnatomy3D

Developer Details: GraphicViZion, 5301315483168732583, None, https://visualanatomy3d.app, info@graphicvizion.com,

Release Date: Feb 1, 2024 **Privacy Policy:** Privacy link

Description:

The free version provides access to the ligament and skeletal systems. Upgrade to the premium version to unlock all additional systems and features. Study human anatomy the easiest and fastest way; visually and interactively. The application is created and maintained by a team of enthusiastic medical professionals, visual artists, and programmers, to bring you the most reliable, detailed, and easiest anatomy app so you don't have to waste time. The free version comes with most features and the ligamental and skeletal system, premium membership (with a subscription) will unlock all other anatomical systems and detail models while also helping us update and improve the app. Features of Visual Anatomy 3D app: -Explore anatomical systems with high-detail and interactivity, offering a comprehensive understanding of human anatomy. -complete 3D anatomy quiz, including all systems (including 3D anatomy quizzes for each system, which can be filtered by body part). -Each separate 3D human anatomy part is accompanied by extensive, informative descriptions. -pronunciation for each 3D human anatomy part -Customize the app; three different color themes, font size, speed, visual settings etc. -Advanced search functionality to efficiently find specific 3D Human anatomy parts, images or detailed anatomy models. -Save and

load anatomy states -cross-platform functionality; one premium membership can be used across different platforms -cloud storages; store any anatomy notes or states in our cloud, and download them across different platforms. -Suitable for both landscape and portrait mode. -Isolate specific 3D anatomy parts for an in-depth study focus. -Draw directly on the screen for note-taking and share or save these notes for collaborative 3D human anatomy learning. Rediscover 3D human anatomy, download the app for free, and discover what it can mean for you! For any questions and/or feedback feel free to email us at any time: info@graphicvizion.com Terms of use: https://visualanatomy3d.app/app/policies/termsofuse.html Privacy policy: https://visualanatomy3d.app/app/policies/privacypolicy.html

SCAN LOGS

Timestamp	Event	Error
2025-08-29 23:19:49	Generating Hashes	OK
2025-08-29 23:19:49	Extracting APK	OK
2025-08-29 23:19:49	Unzipping	OK
2025-08-29 23:19:49	Parsing APK with androguard	OK
2025-08-29 23:19:49	Extracting APK features using aapt/aapt2	OK
2025-08-29 23:19:49	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 23:19:51	Parsing AndroidManifest.xml	OK

2025-08-29 23:19:51	Extracting Manifest Data	OK
2025-08-29 23:19:51	Manifest Analysis Started	OK
2025-08-29 23:19:51	Performing Static Analysis on: V. Anatomy (com.graphicvizion.visualAnatomy3D)	OK
2025-08-29 23:19:51	Fetching Details from Play Store: com.graphicvizion.visualAnatomy3D	OK
2025-08-29 23:19:52	Checking for Malware Permissions	OK
2025-08-29 23:19:52	Fetching icon path	OK
2025-08-29 23:19:52	Library Binary Analysis Started	OK
2025-08-29 23:19:52	Reading Code Signing Certificate	OK
2025-08-29 23:19:52	Running APKiD 2.1.5	OK
2025-08-29 23:19:54	Detecting Trackers	OK

2025-08-29 23:19:55	Decompiling APK to Java with JADX	OK
2025-08-29 23:19:59	Converting DEX to Smali	OK
2025-08-29 23:19:59	Code Analysis Started on - java_source	OK
2025-08-29 23:20:00	Android SBOM Analysis Completed	OK
2025-08-29 23:20:04	Android SAST Completed	OK
2025-08-29 23:20:04	Android API Analysis Started	OK
2025-08-29 23:20:08	Android API Analysis Completed	OK
2025-08-29 23:20:09	Android Permission Mapping Started	OK
2025-08-29 23:20:13	Android Permission Mapping Completed	OK
2025-08-29 23:20:13	Android Behaviour Analysis Started	OK

2025-08-29 23:20:17	Android Behaviour Analysis Completed	OK
2025-08-29 23:20:17	Extracting Emails and URLs from Source Code	OK
2025-08-29 23:20:17	Email and URL Extraction Completed	OK
2025-08-29 23:20:17	Extracting String data from APK	OK
2025-08-29 23:20:18	Extracting String data from Code	OK
2025-08-29 23:20:18	Extracting String values and entropies from Code	OK
2025-08-29 23:20:18	Performing Malware check on extracted domains	OK
2025-08-29 23:20:18	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.