



ANDROID STATIC ANALYSIS REPORT



 VOKA Anatomy Pro (6.1.1)

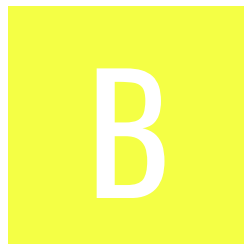
File Name: com.innowise.pathology3d_76.apk

Package Name: com.innowise.pathology3d

Scan Date: Aug. 30, 2025, 10:12 p.m.






App Security Score: 53/100 (MEDIUM RISK)

Grade:



Trackers Detection: 5/432

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
3	13	4	3	1

FILE INFORMATION

File Name: com.innowise.pathology3d_76.apk

Size: 37.57MB

MD5: f0bf95e5ca88a20c502bd64b70115459

SHA1: 1efe3c5d81bb292408a33c72feb7246b320dcc52

SHA256: 0360cb636177d952bc64d3259370324aede216f2847bf5fd7aa7b3a190788abe

APP INFORMATION

App Name: VOKA Anatomy Pro

Package Name: com.innowise.pathology3d

Main Activity: com.innowise.pathology3d.ui.app.AppActivity

Target SDK: 34

Min SDK: 26

Max SDK:

Android Version Name: 6.1.1

Android Version Code: 76

APP COMPONENTS

Activities: 21

Services: 9

Receivers: 6

Providers: 4

Exported Activities: 1

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: 2021-02-19 18:53:33+00:00

Valid To: 2051-02-19 18:53:33+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0x30e48e183df353e0393b91ea9e86863687d7e609

Hash Algorithm: sha256

md5: d2bcb66237f8196d5768c5af0a8c6614

sha1: f3b9f75e5b93f14a6cdc21e5ebcac8689205d041

sha256: cc2fbf5b9491ec44aaca65ecb16d8e0f739d41cf11b1e71a8fed5b78fa62aa1d

sha512: 89608d44091f4d9b291fadd105585ce56d0b370ad9c54801f5634833e87311fa92e0450e77d13348aac8c968a6391caa3d649ff59a04c1bea00247968835506f

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 0fbe396f3a7da39f3976244341d88f95b7e37c55a66960092a245d40477052a0

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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
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.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_AD_SERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	unknown	Unknown permission	Unknown permission from android reference
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	receive push notifications	Allows an application to receive push notifications from cloud.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.ACCESS_AD_SERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.innowise.pathology3d.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

FILE	DETAILS	
f0bf95e5ca88a20c502bd64b70115459.apk	FINDINGS	DETAILS
	Anti-VM Code	possible VM check
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check network operator name check ro.hardware check ro.kernel.qemu check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8 without marker (suspicious)

ACTIVITY	INTENT
com.innowise.pathology3d.ui.app.AppActivity	Schemes: https://, http://, Hosts: @string/links_domain_url,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.innowise.pathology3d,

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: 4 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	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	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	Activity (com.facebook.CustomTabActivity) 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	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.
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.

HIGH: 1 | WARNING: 8 | INFO: 3 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A/f.java A/g.java A/h.java A/i.java A/k.java A/l.java A/m.java A/o.java A/u.java A0/c.java A1/i.java A2/b.java A5/c.java A5/d.java A6/n.java A8/j.java B/a.java B/e.java B0/d.java B2/g.java B2/h.java B3/h.java B3/l.java B3/n.java B3/o.java B8/d.java C0/a.java C2/b.java C3/l.java C3/r.java D1/B.java D1/C0332g.java D1/C0333h.java D1/r.java D1/s.java E0/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				F/i.java F/j.java F/o.java F/t.java F0/u.java F1/b.java F2/d.java G/a.java G0/g.java H/g.java H/k.java H2/f.java H2/g.java H2/i.java H5/a.java I/d.java I/f.java I/g.java I/l.java J0/b.java J3/f.java M/l.java M1/c.java N/a.java N0/s.java N1/r.java N1/u.java N2/a.java O0/a.java O2/Z.java O2/f2.java O2/t2.java O3/h.java O3/j.java P0/d.java P0/e.java Q/AbstractC0437b.java Q/C0436a.java Q/l.java Q/Y.java Q/r.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				Q1/c.java Q1/e.java Q2/a.java Q3/a.java Q3/c.java R0/a.java R2/a.java R3/c.java R3/d.java R3/e.java S0/h.java S0/i.java S0/k.java S0/p.java S0/y.java S1/a.java S3/c.java S3/d.java T/b.java T0/i.java T0/j.java T3/c.java T4/j.java U/k.java U0/d.java U0/i.java U2/f.java U3/A.java U3/C0467g.java U3/C0468h.java U3/C0469i.java U3/C0470j.java U3/C0471k.java U3/D.java U3/F.java U3/J.java U3/L.java U3/n.java U3/o.java U3/q.java U3/s.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	U3/w.java U3/x.java U3/z.java V/b.java V0/a.java V3/g.java W0/C0474c.java W0/d.java W0/g.java W0/w.java W0/x.java W0/y.java W3/d.java W3/g.java W3/j.java Y/c.java Y0/a.java Z0/A.java Z0/c.java Z0/d.java Z0/j.java Z0/k.java Z0/m.java Z0/n.java Z0/r.java Z0/y.java Z3/a.java a4/C0494a.java a4/c.java b2/C0595b.java b4/C0599c.java bitter/jnibridge/JNIBridge.java c4/b.java c4/e.java c4/f.java c6/C0631b.java com/apphud/sdk/ApphudLog.java com/appsflyer/internal/AFg1aSDK.java com/bumptechnology/glide/GeneratedAppGlideModuleImpl.java com/bumptechnology/glide/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/i.java com/bumptech/glide/load/data/k.java com/bumptech/glide/m.java com/bumptech/glide/manager/o.java com/bumptech/glide/n.java com/github/barteksc/pdfviewer/PDFView.java com/shockwave/pdfium/PdfiumCore.java com/unity3d/player/AbstractC0937u.java d1/C0943a.java d1/C0946d.java d1/C0952j.java e2/j.java g/ActivityC1015c.java g/f.java g/g.java g/p.java g0/C1017a.java h1/i.java h2/C1070a.java i0/b.java i1/h.java i7/CallableC1162a.java j2/c.java k/g.java k2/m.java m/C1257B.java m/C1266K.java m/C1268M.java m/C1277i.java m/C1278j.java m/C1291x.java m/Q.java m/T.java m/d0.java m1/C1295a.java moxy/PresenterStore.java n0/C1321a.java n1/C1329H.java n1/C1334e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				n1/C1344o.java n1/C1347r.java n1/C1352w.java n5/b.java o1/e.java o1/g.java o1/t.java o3/AbstractC1375a.java o4/c.java org/fmod/FMODAudioDevice.java org/fmod/a.java p0/C1390a.java p2/C1393a.java p2/C1394b.java q4/C1435b.java r1/e.java r3/C1451d.java r4/C1456c.java s1/e.java s1/f.java s3/C1484a.java t2/b.java t2/c.java t2/e.java t2/g.java t2/j.java t2/l.java t2/o.java t2/p.java t2/q.java t6/C1512c.java u1/c.java u2/C1526A.java u2/C1534e.java u2/C1535f.java u2/h.java u2/i.java u2/k.java u2/r.java u2/v.java u3/C1543g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				v/C1559c.java v0/g.java v0/h.java v0/i.java v0/j.java w/C1597c.java w/o.java w1/c.java w1/e.java w1/f.java w1/h.java w1/i.java w2/C1604d.java w2/u.java w2/w.java w5/C1623a.java x/f.java x2/AbstractC1642b.java x2/AbstractDialogInterfaceOnClickListenerC1662w.java x2/C1645e.java x2/C1659t.java x2/H.java x2/O.java x2/T.java x2/Z.java x2/b0.java x4/C1667A.java x4/C1682m.java x4/F.java x4/G.java x4/H.java x4/J.java x4/v.java z/AbstractC1719c.java z/AbstractC1720d.java z/AbstractC1721e.java z/C1717a.java z1/C1726a.java z4/c.java z4/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	A1/i.java K3/c.java N1/b.java O2/t2.java b8/AbstractC0613a.java b8/C0614b.java c8/C0634a.java com/appsflyer/internal/AFa1tSDK.java com/appsflyer/internal/AFb1cSDK.java com/appsflyer/internal/AFc1gSDK.java n1/C1340k.java
3	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	M1/a.java U3/C0467g.java q4/C1435b.java r4/C1456c.java
4	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/innowise/pathology3d/ui/main/profile/webpage/WebPageFragment.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/innowise/pathology3d/ui/main/modelviewer/screenshot/ScreenshotPreviewActivity.java com/innowise/pathology3d/ui/main/profile/webpage/WebPageFragment.java com/unity3d/player/UnityPlayer.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	A/e.java B0/c.java O2/C0386j.java O2/C0407q.java O2/I0.java O2/Q.java O2/f2.java O2/w2.java com/apphud/sdk/internal/a.java k2/m.java k2/q.java
7	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	Q0/g.java S0/e.java S0/o.java S0/v.java com/apphud/sdk/storage/SharedPreferencesStorage.java com/innowise/pathology3d/domain/models/user/PasswordConfirmValidType.java com/innowise/pathology3d/domain/models/user/PasswordValidType.java moxy/MvpDelegate.java
8	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	O2/t2.java o1/c.java w1/i.java
9	The file or SharedPreferences is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/appsflyer/internal/AFb1tSDK.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	A8/c.java A8/d.java A8/i.java A8/j.java
11	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	A1/b.java N1/t.java com/apphud/sdk/storage/SharedPreferencesStorage.java n1/C1322A.java n1/C1329H.java n1/C1331b.java u1/g.java
12	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	D1/J.java T4/l.java
13	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	B3/n.java U3/C0467g.java
14	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	q4/C1436c.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00003	Put the compressed bitmap data into JSON object	camera	n1/C1347r.java r1/e.java
00096	Connect to a URL and set request method	command network	A1/f.java b2/C0595b.java com/appsflyer/internal/AFd1hSDK.java com/appsflyer/internal/AFe1nSDK.java n1/C1347r.java
00009	Put data in cursor to JSON object	file	A/e.java n1/C1347r.java
00089	Connect to a URL and receive input stream from the server	command network	A1/f.java M1/c.java b2/C0595b.java com/appsflyer/internal/AFd1hSDK.java com/appsflyer/internal/AFe1nSDK.java com/bumptechnology/load/data/i.java n1/C1347r.java r4/C1456c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00109	Connect to a URL and get the response code	network command	A1/f.java O2/RunnableC0378g0.java O2/RunnableC0435z1.java b2/C0595b.java com/appsflyer/internal/AFd1hSDK.java com/appsflyer/internal/AFe1nSDK.java com/appsflyer/internal/AFf1iSDK.java com/bumptechnology/load/data/i.java n1/C1347r.java p2/C1394b.java r4/C1456c.java
00191	Get messages in the SMS inbox	sms	D1/B.java D1/C0326a.java com/appsflyer/internal/AFi1aSDK.java com/appsflyer/internal/AFi1bSDK.java com/appsflyer/internal/AFj1wSDK.java m/Q.java n1/C1347r.java
00014	Read file into a stream and put it into a JSON object	file	A1/a.java D1/C0332g.java F1/e.java U3/q.java W3/g.java q4/C1436c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	A5/d.java B0/f.java B3/o.java T4/j.java W3/g.java Z/q.java Z/v.java com/appsflyer/internal/AFg1eSDK.java r5/w.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	A1/a.java A6/n.java D1/C0332g.java F1/e.java I/l.java O0/a.java O0/b.java U3/C0467g.java U3/q.java W0/i.java W3/g.java W7/d.java Z/m.java Z/q.java Z0/s.java a4/C0494a.java b0/C0590d.java c0/f.java com/appsflyer/internal/AFb1jSDK.java com/unity3d/player/M.java e5/C0977a.java g/p.java g0/C1017a.java o1/e.java q4/C1436c.java s0/C1475c.java s0/C1478f.java w1/i.java
00005	Get absolute path of file and put it to JSON object	file	A5/d.java W3/g.java com/appsflyer/internal/AFg1eSDK.java

RULE ID	BEHAVIOUR	LABEL	FILES
00114	Create a secure socket connection to the proxy address	network command	w8/g.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	D1/B.java D1/C0326a.java D1/J.java D1/K.java D1/N.java N1/b.java O2/C0420u1.java O2/RunnableC0411r1.java O2/f2.java O2/t2.java S1/a.java com/appsflyer/internal/AFb1tSDK.java com/appsflyer/internal/AFc1dSDK.java com/appsflyer/internal/AFc1sSDK.java com/appsflyer/internal/AFf1nSDK.java com/innowise/pathology3d/ui/main/profile/webpage/WebPageFragment.java com/innowise/pathology3d/ui/payment/subscription/SubscriptionActivity.java f6/C1004b.java u2/C1535f.java
00091	Retrieve data from broadcast	collection	D1/B.java N0/C.java N1/w.java O2/C0420u1.java com/appsflyer/internal/AFb1tSDK.java com/appsflyer/internal/AFc1sSDK.java

RULE ID	BEHAVIOUR	LABEL	FILES
00012	Read data and put it into a buffer stream	file	g0/C1017a.java o1/e.java w1/i.java
00036	Get resource file from res/raw directory	reflection	D1/C0326a.java D1/J.java D1/K.java D1/N.java com/appsflyer/internal/AFb1tSDK.java com/appsflyer/internal/AFf1jSDK.java com/appsflyer/internal/AFi1bSDK.java com/appsflyer/internal/AFi1cSDK.java m/Q.java u2/C1535f.java
00147	Get the time of current location	collection location	g/g.java
00075	Get location of the device	collection location	g/g.java
00115	Get last known location of the device	collection location	g/g.java
00162	Create InetAddress object and connecting to it	socket	A8/b.java A8/j.java
00163	Create new Socket and connecting to it	socket	A8/b.java A8/j.java
00004	Get filename and put it to JSON object	file collection	A/e.java F1/a.java U3/q.java p0/C1390a.java x1/C1640c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	O2/RunnableC0378g0.java com/bumptechnology/load/data/i.java
00108	Read the input stream from given URL	network command	O2/C0366c0.java O2/C0429x1.java
00125	Check if the given file path exist	file	D1/C0332g.java D1/C0333h.java x1/C1640c.java
00189	Get the content of a SMS message	sms	D1/B.java N/d.java com/appsflyer/internal/AFj1wSDK.java
00188	Get the address of a SMS message	sms	D1/B.java N/d.java com/appsflyer/internal/AFj1wSDK.java
00200	Query data from the contact list	collection contact	D1/B.java N/d.java com/appsflyer/internal/AFj1wSDK.java
00187	Query a URI and check the result	collection sms callog calendar	D1/B.java N/d.java
00201	Query data from the call log	collection callog	D1/B.java N/d.java com/appsflyer/internal/AFj1wSDK.java

RULE ID	BEHAVIOUR	LABEL	FILES
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	D1/B.java N/d.java R0/a.java com/appsflyer/internal/AFb1mSDK.java com/appsflyer/internal/AFj1wSDK.java
00015	Put buffer stream (data) to JSON object	file	D1/J.java
00078	Get the network operator name	collection telephony	D1/J.java com/appsflyer/internal/AFi1wSDK.java
00171	Compare network operator with a string	network	D1/J.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	D1/J.java D1/K.java f6/C1004b.java u2/C1535f.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	D1/B.java com/appsflyer/internal/AFb1mSDK.java com/appsflyer/internal/AFj1wSDK.java
00094	Connect to a URL and read data from it	command network	Z3/a.java
00192	Get messages in the SMS inbox	sms	com/appsflyer/internal/AFb1mSDK.java

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://innowise-pathologies3d.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebase-remoteconfig.googleapis.com/v1/projects/613051155701/namespaces/firebase:fetch?key=AlzaSyDbNL3pj2AWSVwcaOTPeKl2CmOI5ljuPME. This is indicated by the response: {'state': 'NO_TEMPLATE'}

🔗 ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_EXTERNAL_STORAGE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.CAMERA, android.permission.WAKE_LOCK
Other Common Permissions	3/44	com.google.android.gms.permission.AD_ID, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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
graph-video.s	ok	No Geolocation information available.
www.googleadservices.com	ok	IP: 142.250.217.130 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
pathology3d.voka.io	ok	IP: 34.107.97.54 Country: Germany Region: Hessen City: Frankfurt am Main Latitude: 50.115520 Longitude: 8.684170 View: Google Map
sinapps.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
innowise-pathologies3d.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
issuetracker.google.com	ok	IP: 142.251.40.46 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
.facebook.com	ok	No Geolocation information available.
play.google.com	ok	IP: 142.250.188.238 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
graph.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
facebook.com	ok	IP: 31.13.70.36 Country: United States of America Region: California City: Los Angeles Latitude: 34.052231 Longitude: -118.243683 View: Google Map
sdlSDK.s	ok	No Geolocation information available.
github.com	ok	IP: 140.82.112.4 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
firebase.google.com	ok	IP: 142.250.176.14 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
sconversions.s	ok	No Geolocation information available.
simpresion.s	ok	No Geolocation information available.
smonitorsdk.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	IP: 142.250.217.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.google.com	ok	IP: 142.250.72.132 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
sgcdsdk.s	ok	No Geolocation information available.
sattr.s	ok	No Geolocation information available.
ssdk-services.s	ok	No Geolocation information available.
sadrevenue.s	ok	No Geolocation information available.
developers.facebook.com	ok	IP: 31.13.70.1 Country: United States of America Region: California City: Los Angeles Latitude: 34.052231 Longitude: -118.243683 View: Google Map

DOMAIN	STATUS	GEOLOCATION
sars.s	ok	No Geolocation information available.
app-measurement.com	ok	IP: 142.251.40.46 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
pagead2.googlesyndication.com	ok	IP: 142.251.40.34 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
docs.apphud.com	ok	IP: 104.16.242.118 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
sregister.s	ok	No Geolocation information available.
scdn-ssettings.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
firebaseinstallations.googleapis.com	ok	IP: 142.250.68.74 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
scdn-stestsettings.s	ok	No Geolocation information available.
aps-webhandler.appsflyer.com	ok	IP: 18.238.109.114 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
gateway.apphud.com	ok	IP: 148.251.96.177 Country: Germany Region: Bayern City: Nuremberg Latitude: 49.447781 Longitude: 11.068330 View: Google Map
slaunches.s	ok	No Geolocation information available.
sonelink.s	ok	No Geolocation information available.
ns.adobe.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
svalidate-and-log.s	ok	No Geolocation information available.
sapp.s	ok	No Geolocation information available.
catalog.voka.io	ok	IP: 34.107.97.54 Country: Germany Region: Hessen City: Frankfurt am Main Latitude: 50.115520 Longitude: 8.684170 View: Google Map
firebase-settings.crashlytics.com	ok	IP: 142.250.176.3 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
schemas.android.com	ok	No Geolocation information available.
sviap.s	ok	No Geolocation information available.
apphud.blob.core.windows.net	ok	IP: 52.239.221.36 Country: United States of America Region: Virginia City: Washington Latitude: 38.713451 Longitude: -78.159439 View: Google Map

DOMAIN	STATUS	GEOLOCATION
google.com	ok	IP: 142.250.176.14 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.facebook.com	ok	IP: 31.13.70.36 Country: United States of America Region: California City: Los Angeles Latitude: 34.052231 Longitude: -118.243683 View: Google Map
svalidate.s	ok	No Geolocation information available.
goo.gl	ok	IP: 142.250.217.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map



EMAIL	FILE
u0013android@android.com0 u0013android@android.com	u2/o.java
info@voka.io	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"base_api_url" : "https://pathology3d.voka.io/api/"

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "27115fdb3b0d41cda6e4dcd4c20a9d23"
"facebook_client_token" : "e6bfb8de9c81cd75f2c0aa60825bbd1c"
"firebase_database_url" : "https://innowise-pathologies3d.firebaseio.com"
"google_api_key" : "AlzaSyDbNL3pj2AWSVwcaOTPekI2CmOI5IjuPME"
"google_crash_reporting_api_key" : "AlzaSyDbNL3pj2AWSVwcaOTPekI2CmOI5IjuPME"
"licensing_public_key" : "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAm8KTH4Zt3Frz/nLusDaXz0iPXjz8fJMeWaq3gTVzTbK/aixMXvT/P6Nm5pXP1nUliocccOFy5MDba11jXpJUd371Vcs/iQ08layCpGZGa+vyZ63HMir9a+wQ1CXGRF2ws+s3krNwQ8o6laBps4t7MBMEQ4VOzIgnqAeJdA+mJmdmaauEWnpNiCMpSn0mfyXEkVu7S/cjqwG5oCoN91OD0cxwdmFAhCleXKdqnnFvMYhNO7q/ei7t5nUZYK2f+PTFqYqT6DY3xPVQ8XnalB3zCH/VUoUJv6+CNpzVxomhIXA/xzPr/eUE/XYUO3vWTzPXId4wEiFsgBWJlfxZMm+vZWIDAQAB"
"login_password" : "Password"
"registration_password" : "Password*"
"com_facebook_device_auth_instructions" : "facebook.com/device□□□□□□□□□□□□□□□□□□□□"
"login_password" : "Passwort"
"registration_password" : "Passwort*"
"login_password" : "Пароль"
"registration_password" : "Пароль*"
"com_facebook_device_auth_instructions" : "□□facebook.com/device□□□□□□□□□□□□"

POSSIBLE SECRETS
3BAF59A2E5331C30675FAB35FF5FFF0D116142D3D4664F1C3CB804068B40614F
308203c7308202afa003020102021500dc286b43b4ea12039958a00a6655eb84720e46c9300d06092a864886f70d01010b05003074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f6964301e170d3137303830343136353333375a170d3437303830343136353333375a3074310b3009060355040613025553311330110603550408130a43616c69666f726e6961311630140603550407130d4d6f756e7461696e205669657731143012060355040a130b476f6f676c6520496e632e3110300e060355040b1307416e64726f69643110300e06035504031307416e64726f696430820122300d06092a864886f70d01010105000382010f003082010a02820101008998646f47fc333db09644c303104ed183e904e351152aa66a603b77f63389d45d6fcffae3c94fadf1f28038e265d697fea347327f9081a7f0b9074d5b148db5bf357c611a77f87f844a15068818bdcd5b21d187e93fa2551676170eedce04a150c35ec0a791eef507fa9b406573c36f6f207764842e5677e35a281a422659e91e26eb4fecfb053b5c936d0976c37f8757adb57a37953da5844ea350695854d343a61ad341b63a1c425d22855af7ebfee018e1736cee98536be5b9947f288e2a26f99eb9f91b5de93fecc513019d2e90f12b38610d1f02eaa81deca4ce91c19cbce36d6c3025ce2432b3d178616beafaf437c08451bc469c6bc6f4517a714a5b0203010001a350304e300c0603551d13040530030101ff301d0603551d0e0416041419a864c0f2618c67c803a23da909bc70521f269b301f0603551d2304183016801419a864c0f2618c67c803a23da909bc70521f269b300d06092a864886f70d01010b050003820101005403fc56fdefc440376a0337815002b96a15bffc2fe42de6c58f52fae4d80652e3704455b885409eef81ffbb4c44dba104b6b8e24c9e2e0e7a04338ee73baa5b71bfb4488f8e04bef3d0eaf7d43aa42b03b278c33cc1f0dd3802571624baa161d851fab37db4bc92b9094b6885dff62b400ecd81f069d56a1be1db46d8198c50c9628cdb6e38686ef640fd386775f50376f957e24ea45ed1942968f20c82f189607fdb22f11cfdfd0760a77a60ceb3416cfb3f48f13f9f83f3834a01001750a7c78bc1fd81f0b53a7c41dcba9f5a0118259d083c32bb9ebb84d645d6f6b9c31923d8ab70e7f0a25940ecc9f4945144419f86e8c421d3b99774f4b8f3d09262e7
FFE391E0EA186D0734ED601E4E70E3224B7309D48E2075BAC46D8C667EAE7212
FBA3AF4E7757D9016E953FB3EE4671CA2BD9AF725F9A53D52ED4A38EAAA08901
c56fb7d591ba6704df047fd98f535372fea00211
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
470fa2b4ae81cd56ecbcd9735803434cec591fa
32d246d2e182b04a03958815e10e74f9
2f46a95533f432402eb5fb13e48d0cb7
df6b721c8b4d3b6eb44c861d4415007e5a35fc95

POSSIBLE SECRETS
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
E3F9E1E0CF99D0E56A055BA65E241B3399F7CEA524326B0CDD6EC1327ED0FDC1
QWyH6ULmc7w47rTYZNbgfMSQmgCxPS
9b8f518b086098de3d77736f9458a3d2f6f95a37
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
cc2751449a350f668590264ed76692694a80308a

PLAYSTORE INFORMATION

Title: VOKA 3D Anatomy & Pathology

Score: 4.076923 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** [com.innowise.pathology3d](https://play.google.com/store/apps/details?id=com.innowise.pathology3d)

Developer Details: Factory of innovations and solutions LLC, Factory+of+innovations+and+solutions+LLC, None, <https://voka.io/>, info@voka.io,

Release Date: Feb 19, 2021 **Privacy Policy:** [Privacy link](#)

Description:

VOKA Anatomy Pro is a unique complete catalog of medically accurate 3D models of human anatomy and pathologies, including rare diseases. This mobile atlas is designed to be always at hand for medical students, lecturers, and doctors: to view the models on the required scale, from any angle, both inside and out. It provides additional clarity to pathology understanding and learning, making it much easier. Our focus is to provide visible, really true-to-life three-dimensional visualization of human applied e-anatomy and pathologies. Each and every 3D anatomy model is developed in close cooperation with top-notch medical professionals of research centers, based on actual DICOM data from CT/MRI, thought out to the very smallest detail, and verified by the medical advisory board. All 3D models are labeled, dissected, and segmented to facilitate configuration meeting any visualization needs. For instance, you can hide the outer membrane, which opens up the maximum field of view of the pathology and facilitates understanding its anatomy. In addition to all possible types of pathologies (larynx, spasticity), each category of the catalog includes smart reference anatomy 3D models of healthy organs. VOKA CT. Anatomy Pro 5 visualizer map is empowered with an AR mode that lets you overlay virtual 3D men models on the real world and study human head, circulatory systems, nose, skull, spine, thoracic, foot, cranial nerves - anatomy & pathologies in augmented reality. Enjoy a truly immersive experience while memorizing complex anatomy structures in motion! In the app, you will also find medical articles that describe the types and

subtypes of pathologies from an anatomical point of view, c. linical presentation, trail guide and treatment methods. Use them to prepare easy for classes or refresh your knowledge, save materials in your personal collections and share with mates. VOKA Anatomy Pro: ✓ full-scale visual immersion in the 3D man anatomy and pathologies ✓ the highest level of medical precision ✓ astonishingly lifelike 3D graphics structure ✓ a lightweight app with full functionality The app is recommended for: ✓ medical students to use dictionary, study, to make it easier to learn vascular, vertebrae, musculoskeletal, visualize human anatomy (pelvic, liver, joints, vertebral column, ligament etc.) and pass exams ✓ lecturers for lectures to teach, and practical classes in online and offline modes ✓ medical specialists to provide patients with a better understanding of their health conditions The latest release includes over 700 male and female pathology and anatomy 3D models: ✓ Aanatomy ✓ Congenital heart defects; ✓ Acquired heart diseases; ✓ Gynaecology; ✓ Otorhinolaryngology; ✓ Dentistry; ✓ New categories, quiz, flashcards, classic images, 4, 4d+, 5d in regular app updates. Features: ✓ zooming surface in/out to examine each anatomical parts or detail inside and outside 3D model ✓ 360° rotation to view 3D models from any angle ✓ isolating and hiding anatomical structures to focus on the essentials ✓ reading basic text information to elements on the model ✓ the opportunity to pocket study the names of muscles, anatomical structures and their nesting ✓ saving the necessary materials to my personal collections for quick access ✓ sharing links for useful 3rd biology, pathology models and articles with fellows ✓ fast speed and convenient search through all the materials biology ✓ AR mode to display 3D pathologies in a real-world environment, e .g. on a mannequin Available in 3b languages: ✓ English ✓ German ✓ Russian Download VO KA Anatomy Pro Clinical Skeletal Anatomyka for FREE and get all pathology or muscular 3D models on your mobile phone. Always with you, to use it offline, anywhere and anytime you like!

☰ SCAN LOGS

Timestamp	Event	Error
2025-08-30 22:12:50	Generating Hashes	OK
2025-08-30 22:12:51	Extracting APK	OK
2025-08-30 22:12:51	Unzipping	OK
2025-08-30 22:12:51	Parsing APK with androguard	OK
2025-08-30 22:12:51	Extracting APK features using aapt/aapt2	OK

2025-08-30 22:12:51	Getting Hardcoded Certificates/Keystores	OK
2025-08-30 22:12:53	Parsing AndroidManifest.xml	OK
2025-08-30 22:12:53	Extracting Manifest Data	OK
2025-08-30 22:12:53	Manifest Analysis Started	OK
2025-08-30 22:12:53	Performing Static Analysis on: VOKA Anatomy Pro (com.innowise.pathology3d)	OK
2025-08-30 22:12:54	Fetching Details from Play Store: com.innowise.pathology3d	OK
2025-08-30 22:12:54	Checking for Malware Permissions	OK
2025-08-30 22:12:54	Fetching icon path	OK
2025-08-30 22:12:54	Library Binary Analysis Started	OK
2025-08-30 22:12:54	Reading Code Signing Certificate	OK
2025-08-30 22:12:54	Running APKiD 2.1.5	OK

2025-08-30 22:12:57	Detecting Trackers	OK
2025-08-30 22:12:58	Decompiling APK to Java with JADX	OK
2025-08-30 22:13:11	Converting DEX to Smali	OK
2025-08-30 22:13:11	Code Analysis Started on - java_source	OK
2025-08-30 22:13:13	Android SBOM Analysis Completed	OK
2025-08-30 22:13:21	Android SAST Completed	OK
2025-08-30 22:13:21	Android API Analysis Started	OK
2025-08-30 22:13:28	Android API Analysis Completed	OK
2025-08-30 22:13:29	Android Permission Mapping Started	OK
2025-08-30 22:13:35	Android Permission Mapping Completed	OK
2025-08-30 22:13:35	Android Behaviour Analysis Started	OK

2025-08-30 22:13:44	Android Behaviour Analysis Completed	OK
2025-08-30 22:13:44	Extracting Emails and URLs from Source Code	OK
2025-08-30 22:13:47	Email and URL Extraction Completed	OK
2025-08-30 22:13:47	Extracting String data from APK	OK
2025-08-30 22:13:47	Extracting String data from Code	OK
2025-08-30 22:13:47	Extracting String values and entropies from Code	OK
2025-08-30 22:13:49	Performing Malware check on extracted domains	OK
2025-08-30 22:13:58	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.

© 2025 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).