



# ANDROID STATIC ANALYSIS REPORT

app\_icon

 WatchPAT (3.2.1.2)

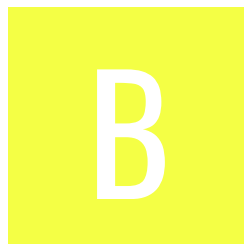
File Name: com.itamarmedical.watchpat\_493.apk

Package Name: com.itamarmedical.watchpat

Scan Date: Aug. 30, 2025, 10:15 p.m.






App Security Score: 50/100 (MEDIUM RISK)

Grade:



Trackers Detection: 1/432

## FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
4	16	1	3	1

## FILE INFORMATION

**File Name:** com.itamarmedical.watchpat\_493.apk

**Size:** 27.54MB

**MD5:** 00d587ef1633e0ea8299830988388fdd

**SHA1:** 14f73125d35e591db52f23c9ca592db4622ddd1b

**SHA256:** 1b1e8c8fb8d01914e63cdfc354f0890fc7a01e4078c7783379c7a9e1efc361c5

## APP INFORMATION

**App Name:** WatchPAT

**Package Name:** com.itamarmedical.watchpat

**Main Activity:** com.itamarmedical.watchpat.activities.MainActivity

**Target SDK:** 34

**Min SDK:** 29

**Max SDK:**

**Android Version Name:** 3.2.1.2

Android Version Code: 493

## APP COMPONENTS

Activities: 52

Services: 16

Receivers: 11

Providers: 2

Exported Activities: 1

Exported Services: 2

Exported Receivers: 3

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: 2018-07-26 10:53:17+00:00

Valid To: 2048-07-26 10:53:17+00:00

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

Serial Number: 0x2c77be06a3d77eabb3a71bbdc5b39b9adc562d6d

Hash Algorithm: sha256

md5: 7881eb1b1611abd002b868e5375412f0

sha1: 580fbf8a757a04725d006b73951f7800b63cdadb

sha256: b0b23fde70aab2b35cbc8176e71e2e15e389c0bcefb1a71bbe39603c998eed1a

sha512: 2fa12c3bea6db1bc81e01b12a9ea5d4b3eb203590242e6d20825e77ed2e15d5b9fda2bbd89a7d0bd54be40fa31726d4406ddb1ae1d35cb237723c62e8901e6a4

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 6b193caa40a3d48a64ec57f0e3424575413a589022281a14ad30a8725b3bffd

Found 1 unique certificates

## ☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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".
android.permission.FOREGROUND_SERVICE_CONNECTED_DEVICE	normal	enables foreground services with connected device use.	Allows a regular application to use Service.startForeground with the type "connectedDevice".
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
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.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.KILL_BACKGROUND_PROCESSES	normal	kill background processes	Allows an application to kill background processes of other applications, even if memory is not low.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
android.permission.BLUETOOTH_SCAN	dangerous	required for discovering and pairing Bluetooth devices.	Required to be able to discover and pair nearby Bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.itamarmedical.watchpat.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

## APKID ANALYSIS

FILE	DETAILS
------	---------

FILE	DETAILS	
00d587ef1633e0ea8299830988388fdd.apk	FINDINGS	DETAILS
	Anti-VM Code	possible VM check
classes.dex	FINDINGS	DETAILS
	yara_issue	yara issue - dex file recognized by apkid but not yara module
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check SIM operator check possible ro.secure check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	unknown (please file detection issue!)



ACTIVITY	INTENT
com.itamarmedical.watchpat.activities.MainActivity	Schemes: https://, Hosts: watchpat.page.link, sleepath.page.link, apps.apple.com,

## 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: 3 | WARNING: 6 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

NO	ISSUE	SEVERITY	DESCRIPTION
1	App Link assetlinks.json file not found [android:name=com.itamarmedical.watchpat.activities.MainActivity] [android:host=https://watchpat.page.link]	high	App Link asset verification URL (https://watchpat.page.link/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 200). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
2	App Link assetlinks.json file not found [android:name=com.itamarmedical.watchpat.activities.MainActivity] [android:host=https://sleepath.page.link]	high	App Link asset verification URL (https://sleepath.page.link/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: 200). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.

NO	ISSUE	SEVERITY	DESCRIPTION
3	App Link assetlinks.json file not found [android:name=com.itamarmedical.watchpat.activities.MainActivity] [android:host=https://apps.apple.com]	high	App Link asset verification URL (https://apps.apple.com/.well-known/assetlinks.json) not found or configured incorrectly. (Status Code: None). App Links allow users to redirect from a web URL/email to the mobile app. If this file is missing or incorrectly configured for the App Link host/domain, a malicious app can hijack such URLs. This may lead to phishing attacks, leak sensitive data in the URI, such as PII, OAuth tokens, magic link/password reset tokens and more. You must verify the App Link domain by hosting the assetlinks.json file and enabling verification via [android:autoVerify="true"] in the Activity intent-filter.
4	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [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. 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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	<p>Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: com.google.android.c2dm.permission.SEND [android:exported=true]</p>	warning	<p>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.</p>
6	<p>Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]</p>	warning	<p>A Service 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.</p>
7	<p>Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked.</p> <p>Permission: android.permission.DUMP [android:exported=true]</p>	warning	<p>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.</p>

NO	ISSUE	SEVERITY	DESCRIPTION
8	Activity (androidx.compose.ui.tooling.PreviewActivity) 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.
9	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: 8 | INFO: 1 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A5/a.java A5/c.java B5/c.java D4/a.java E4/a.java E8/l.java F1/b.java F5/g.java F8/d.java G1/b.java G1/c.java G1/g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				G7/g.java H4/c.java I1/AbstractComponentCallbacksC0235x.java I1/AnimationAnimationListenerC0223k.java I1/C.java I1/C0213a.java I1/C0217e.java I1/C0218f.java I1/C0222j.java I1/C0224l.java I1/DialogInterfaceOnCancelListenerC0228p.java I1/E.java I1/I.java I1/N.java I1/Q.java I1/V.java I1/h0.java I1/j0.java I1/n0.java I1/p0.java I6/h.java J1/c.java J6/ViewOnClickListenerC0342v0.java L2/g.java M/H0.java M5/d.java N1/b.java O1/b.java O1/d.java O3/J0.java O3/Q0.java O3/R0.java O3/T0.java O3/d1.java P5/d.java Q0/d.java Q5/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				R5/C.java S0/i.java S1/g.java S1/h.java S1/p.java S1/s.java T3/i.java T6/B0.java U2/ViewOnClickListenerC0708j.java U5/AbstractServiceC0727h.java U5/B.java U5/C.java U5/D.java U5/E.java U5/G.java U5/I.java U5/k.java U5/l.java U5/q.java U5/v.java U5/w.java U5/x.java U5/y.java U6/P.java V0/d.java V0/h.java V0/i.java V0/l.java V0/p.java V1/h.java V2/e.java W3/b.java X2/C0797d.java X2/E.java X2/L.java X2/T.java X2/X.java X2/h0.java X2/n0.java X2/r.java X3/a.java .....

NO	ISSUE	SEVERITY	STANDARDS	FILES
				X4/c.java X6/A.java X6/AbstractServiceConnectionC083 5l.java X6/C0822b0.java X6/C0830g.java X6/C0840q.java X6/DialogInterfaceOnClickListenerC0824c0.java X6/DialogInterfaceOnClickListenerC0827e.java X6/DialogInterfaceOnClickListenerC0838o.java X6/F.java X6/RunnableC0820a0.java X6/k0.java X6/n0.java X6/o0.java X6/r0.java X6/u0.java X6/w0.java Y2/B.java Y2/n.java Y2/p.java Y2/r.java Y2/s.java Y2/t.java Y3/a.java Y3/d.java Y3/i.java Z/e.java Z0/D.java Z5/B.java Z5/C0898n.java Z5/C0899o.java Z5/C0908y.java Z5/L.java Z5/N.java Z5/S.java Z5/T.java Z5/U.java



NO	ISSUE	SEVERITY	STANDARDS	FILES
1	<a href="#">The App logs information. Sensitive information should never be logged.</a>	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	Z5/V.java Z6/V.java a1/e.java a5/e.java a5/g.java b1/o.java b6/d.java b6/e.java b6/f.java b6/j.java b7/X.java c/RunnableC1092d.java c/RunnableC1099k.java c1/C1133f.java c3/AbstractC1142c.java com/chilkatsoft/CkLog.java com/itamarmedical/watchpat/WatchPATApp.java com/itamarmedical/watchpat/activities/BatteryActivity.java com/itamarmedical/watchpat/activities/DoneActivity.java com/itamarmedical/watchpat/activities/IdentificationActivity.java com/itamarmedical/watchpat/activities/PrepareActivity.java com/itamarmedical/watchpat/activities/QuickGuideActivity.java com/itamarmedical/watchpat/activities/RecordingActivity.java com/itamarmedical/watchpat/activities/ServiceActivity.java com/itamarmedical/watchpat/activities/SetChestActivity.java com/itamarmedical/watchpat/activities/SetDeviceActivity.java com/itamarmedical/watchpat/activities/SetFingerActivity.java com/itamarmedical/watchpat/activities/StartActivity.java com/itamarmedical/watchpat/activit

NO	ISSUE	SEVERITY	STANDARDS	FILES
				<div>ies/UploadingActivity.java</div> <div>com/itamarmedical/watchpat/activities/VideoPlayerActivity.java</div> <div>com/itamarmedical/watchpat/activities/WelcomeActivity.java</div> <div>com/itamarmedical/watchpat/services/BLEService.java</div> <div>com/itamarmedical/watchpat/services/SFTPService.java</div> <div>com/itamarmedical/watchpat/services/TransactionService.java</div> <div>d1/AbstractC1220c.java</div> <div>d3/C1242g.java</div> <div>d5/v.java</div> <div>e3/C1315a.java</div> <div>f/h.java</div> <div>g/C1465b.java</div> <div>g1/AbstractC1474b.java</div> <div>g1/RunnableC1473a.java</div> <div>g3/x.java</div> <div>g4/e.java</div> <div>g4/n.java</div> <div>h4/C1576b.java</div> <div>h4/C1577c.java</div> <div>h4/e.java</div> <div>h4/f.java</div> <div>h4/i.java</div> <div>h4/j.java</div> <div>h4/k.java</div> <div>h4/m.java</div> <div>h4/n.java</div> <div>h7/C1617c.java</div> <div>h7/C1618d.java</div> <div>h7/C1619e.java</div> <div>h7/C1621g.java</div> <div>h7/RunnableC1616b.java</div> <div>h7/RunnableC1626l.java</div> <div>h7/n.java</div> <div>h7/o.java</div> <div>h7/p.java</div> <div>h7/q.java</div>

NO	ISSUE	SEVERITY	STANDARDS	FILES
				<div>i/AbstractActivityC1662l.java</div> <div>i/AbstractC1667q.java</div> <div>i/C1631A.java</div> <div>i/C1644N.java</div> <div>i/C1676z.java</div> <div>i/HandlerC1655e.java</div> <div>i/LayoutInflaterFactory2C1635E.java</div> <div>i/RunnableC1641K.java</div> <div>i4/AbstractC1707e.java</div> <div>i4/C1706d.java</div> <div>i4/h.java</div> <div>i4/j.java</div> <div>i4/l.java</div> <div>i7/C1715b.java</div> <div>i7/C1717d.java</div> <div>j1/C1728b.java</div> <div>j1/C1746n.java</div> <div>j1/l.java</div> <div>j1/T.java</div> <div>j1/p0.java</div> <div>j1/t0.java</div> <div>j3/C1791j.java</div> <div>j3/v.java</div> <div>k/C1821i.java</div> <div>k/C1822j.java</div> <div>k3/n.java</div> <div>k4/C1854f.java</div> <div>k4/G.java</div> <div>k4/HandlerC1852d.java</div> <div>k4/u.java</div> <div>k4/w.java</div> <div>l/C1898o.java</div> <div>l4/AbstractC1915f.java</div> <div>l4/C1907B.java</div> <div>l4/C1914e.java</div> <div>l4/E.java</div> <div>l4/G.java</div> <div>l4/n.java</div> <div>l4/q.java</div> <div>l4/y.java</div> <div>l4/z.java</div>

NO	ISSUE	SEVERITY	STANDARDS	FILES
				I5/AbstractC1921b.java I5/e.java I5/g.java I7/C.java I7/C1935A.java I7/C1941f.java I7/C1944i.java I7/C1952q.java I7/C1953s.java I7/C1954t.java I7/C1955u.java I7/C1958x.java I7/E.java I7/G.java I7/H.java I7/J.java I7/K.java I7/L.java I7/S.java I7/T.java I7/V.java I7/Z.java I7/b0.java I7/d0.java I7/e0.java m/AbstractC2041f1.java m/C2012U.java m/C2083v.java m/C2087x.java m/DialogInterfaceOnClickListenerC1999N.java m/RunnableC2051j.java m/ViewOnClickListenerC2038e1.java a m/u1.java m2/m.java n2/g.java n2/j.java o1/C2199b.java o1/C2200c.java o2/AbstractC2204b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o4/C2217a.java o5/k.java o5/h.java o5/l.java p1/C2245o.java p4/AbstractC2255d.java q1/C2281c.java q4/AbstractC2290a.java q5/C2292a.java r3/e.java r3/g.java r5/C2341b.java r5/C2342c.java s3/AbstractC2367f.java s3/C2364c.java s3/C2366e.java s3/C2370i.java s3/C2373l.java s3/C2381t.java s4/AbstractC2383a.java s4/b.java s4/d.java t1/C2465e.java t3/AbstractC2481l.java t3/RunnableC2475f.java t5/b.java u0/C2575w.java u0/Q.java u5/AbstractC2608g.java u5/C2610i.java u5/C2616o.java u5/C2618q.java u5/C2619r.java u5/C2620s.java u5/C2621t.java u5/C2624w.java u5/C2626y.java u5/CallableC2612k.java u5/CallableC2613l.java u5/CallableC2617p.java u5/EnumC2607f.iava

NO	ISSUE	SEVERITY	STANDARDS	FILES
				u5/RunnableC2614m.java v5/C2789d.java v5/g.java v5/l.java w5/C.java y5/C3188a.java z0/C3259b.java z5/C3317a.java z5/C3318b.java
2	<a href="#">Files may contain hardcoded sensitive information like usernames, passwords, keys etc.</a>	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	E0/O.java G3/c.java M/C0436l0.java T1/a.java s3/C2365d.java s8/O.java
3	<a href="#">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.</a>	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	I1/C0218f.java X1/g.java X1/m.java X1/u.java X3/a.java Y3/d.java Y3/i.java Z3/h.java Z3/n.java d3/C1237b.java o1/C2199b.java
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	b7/e0.java com/itamarmedical/watchpat/Watc hPATApp.java com/itamarmedical/watchpat/view model/MainViewModel.java d7/C1259j.java m7/C2119b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	<a href="#">This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.</a>	secure	OWASP MASVS: MSTG-NETWORK-4	E8/d.java E8/g.java E8/k.java E8/l.java
6	<a href="#">SHA-1 is a weak hash known to have hash collisions.</a>	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	Q5/b.java R5/c.java u5/AbstractC2608g.java z5/C3318b.java
7	<a href="#">This App may request root (Super User) privileges.</a>	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	p7/AbstractC2274a.java
8	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	s3/C2373l.java z3/C3298D.java
9	<a href="#">This App may have root detection capabilities.</a>	secure	OWASP MASVS: MSTG-RESILIENCE-1	M/A0.java u5/AbstractC2608g.java
10	<a href="#">The App uses an insecure Random Number Generator.</a>	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	P1/AbstractC0556h.java V7/a.java V7/b.java W1/L.java W7/a.java X1/z.java g2/f0.java i/RunnableC1641K.java s3/C2375n.java u0/C2533a0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	<a href="#">App can read/write to External Storage. Any App can read data written to External Storage.</a>	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	l6/f.java com/itamarmedical/watchpat/activities/WelcomeActivity.java l7/C.java l7/C1944i.java s3/AbstractC2367f.java y6/C3192a.java
12	<a href="#">Calling Cipher.getInstance("AES") will return AES ECB mode by default. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.</a>	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	Z6/c.java

## NIAP ANALYSIS v1.3

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

## BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00096	Connect to a URL and set request method	command network	U1/o.java a7/C0936a.java l7/H.java o1/C2199b.java



RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	R5/c.java U1/o.java l7/H.java o1/C2199b.java
00109	Connect to a URL and get the response code	network command	R5/c.java U1/o.java a7/C0936a.java g4/e.java l7/H.java o1/C2199b.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	C/C0047h.java N6/e.java U5/E.java X6/AbstractServiceConnectionC0835l.java g7/f.java i4/AbstractC1707e.java l/RunnableC1890g.java q4/AbstractC2290a.java s3/AbstractC2367f.java v/C2690a.java y5/C3188a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	A3/a.java I1/C0217e.java T3/i.java U5/E.java X6/DialogInterfaceOnClickListenerC0824c0.java com/itamarmedical/watchpat/WatchPATApp.java com/itamarmedical/watchpat/activities/ServiceActivity.java com/itamarmedical/watchpat/services/S3Service.java e3/C1315a.java I7/C.java I7/C1935A.java I7/C1944i.java I7/J.java s3/AbstractC2367f.java v5/g.java y6/C3192a.java z0/C3259b.java
00091	Retrieve data from broadcast	collection	U5/E.java U5/I.java com/itamarmedical/sleepath_sdk/presentation/activity/LoginActivity.java I7/C.java m3/C2108c.java
00125	Check if the given file path exist	file	U5/E.java I7/C.java
00036	Get resource file from res/raw directory	reflection	U1/s.java U5/E.java i4/AbstractC1707e.java m/ViewOnClickListenerC2038e1.java q4/AbstractC2290a.java s3/AbstractC2367f.java x3/C3023c.java y5/C3188a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	i4/AbstractC1707e.java y5/C3188a.java
00094	Connect to a URL and read data from it	command network	U1/o.java y5/C3188a.java
00013	Read file and put it into a stream	file	B5/c.java G1/g.java I1/C0217e.java J8/v.java U1/c.java U1/s.java U6/P.java V2/a.java V2/e.java V2/i.java X6/DialogInterfaceOnClickListenerC0824c0.java a7/C0936a.java d1/AbstractC1220c.java I5/AbstractC1921b.java I7/C.java I7/C1935A.java q4/AbstractC2290a.java s3/C2373l.java u5/AbstractC2608g.java u5/C2616o.java v5/g.java z5/C3317a.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	W1/C0778o.java
00012	Read data and put it into a buffer stream	file	G1/g.java I1/C0217e.java a7/C0936a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00009	Put data in cursor to JSON object	file	X3/a.java
00014	Read file into a stream and put it into a JSON object	file	B5/c.java s3/C2373l.java v5/g.java
00162	Create InetAddress object and connecting to it	socket	E8/c.java E8/l.java
00163	Create new Socket and connecting to it	socket	E8/c.java E8/l.java
00046	Method reflection	reflection	T6/B0.java
00075	Get location of the device	collection location	s3/C2381t.java
00137	Get last known location of the device	location collection	s3/C2381t.java
00114	Create a secure socket connection to the proxy address	network command	A8/l.java
00191	Get messages in the SMS inbox	sms	m/ViewOnClickListenerC2038e1.java
00005	Get absolute path of file and put it to JSON object	file	v5/g.java
00132	Query The ISO country code	telephony collection	k2/C1835f.java
00028	Read file from assets directory	file	U1/a.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	U1/o.java
00108	Read the input stream from given URL	network command	U1/o.java

## FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for <a href="https://firebaseremoteconfig.googleapis.com/v1/projects/802330651214/namespaces/firebase:fetch?key=AlzaSyBW19IE4h6WDGD3wHnFA5c-MjtAMazkPCw">https://firebaseremoteconfig.googleapis.com/v1/projects/802330651214/namespaces/firebase:fetch?key=AlzaSyBW19IE4h6WDGD3wHnFA5c-MjtAMazkPCw</a> . This is indicated by the response: {'state': 'NO_TEMPLATE'}

## ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION
Other Common Permissions	5/44	android.permission.FOREGROUND_SERVICE, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.ACCESS_BACKGROUND_LOCATION, 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
xml.org	ok	IP: 104.239.142.8 Country: United States of America Region: Texas City: Windcrest Latitude: 29.499678 Longitude: -98.399246 View: <a href="#">Google Map</a>
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: <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	<b>IP:</b> 142.250.188.238 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
default.url	ok	No Geolocation information available.
www.w3.org	ok	<b>IP:</b> 104.18.23.19 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Francisco <b>Latitude:</b> 37.775700 <b>Longitude:</b> -122.395203 <b>View:</b> <a href="#">Google Map</a>
firebase.google.com	ok	<b>IP:</b> 142.250.176.14 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
developer.android.com	ok	<b>IP:</b> 172.217.14.110 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
g.co	ok	<b>IP:</b> 142.250.72.174 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
accounts.google.com	ok	<b>IP:</b> 142.250.101.84 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
www.itamar-medical.com	ok	<b>IP:</b> 172.66.140.20 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> San Francisco <b>Latitude:</b> 37.775700 <b>Longitude:</b> -122.395203 <b>View:</b> <a href="#">Google Map</a>
firebaseinstallations.googleapis.com	ok	<b>IP:</b> 142.250.217.138 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>



DOMAIN	STATUS	GEOLOCATION
developer.apple.com	ok	<b>IP:</b> 17.253.83.145 <b>Country:</b> Singapore <b>Region:</b> Singapore <b>City:</b> Singapore <b>Latitude:</b> 1.289670 <b>Longitude:</b> 103.850067 <b>View:</b> <a href="#">Google Map</a>
ns.adobe.com	ok	No Geolocation information available.
schemas.microsoft.com	ok	<b>IP:</b> 13.107.246.71 <b>Country:</b> Netherlands <b>Region:</b> Noord-Holland <b>City:</b> Amsterdam <b>Latitude:</b> 52.374031 <b>Longitude:</b> 4.889690 <b>View:</b> <a href="#">Google Map</a>
firebase-settings.crashlytics.com	ok	<b>IP:</b> 142.250.176.3 <b>Country:</b> United States of America <b>Region:</b> California <b>City:</b> Mountain View <b>Latitude:</b> 37.405991 <b>Longitude:</b> -122.078514 <b>View:</b> <a href="#">Google Map</a>
schemas.android.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
eprovide.mapi-trust.org	ok	<b>IP:</b> 212.2.188.75 <b>Country:</b> Ireland <b>Region:</b> Dublin <b>City:</b> Dublin <b>Latitude:</b> 53.343990 <b>Longitude:</b> -6.267190 <b>View:</b> <a href="#">Google Map</a>
xmlpull.org	ok	<b>IP:</b> 185.199.110.153 <b>Country:</b> United States of America <b>Region:</b> Pennsylvania <b>City:</b> California <b>Latitude:</b> 40.065632 <b>Longitude:</b> -79.891708 <b>View:</b> <a href="#">Google Map</a>
dashif.org	ok	<b>IP:</b> 185.199.108.153 <b>Country:</b> United States of America <b>Region:</b> Pennsylvania <b>City:</b> California <b>Latitude:</b> 40.065632 <b>Longitude:</b> -79.891708 <b>View:</b> <a href="#">Google Map</a>
aomedia.org	ok	<b>IP:</b> 185.199.111.153 <b>Country:</b> United States of America <b>Region:</b> Pennsylvania <b>City:</b> California <b>Latitude:</b> 40.065632 <b>Longitude:</b> -79.891708 <b>View:</b> <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
goo.gle	ok	<b>IP:</b> 67.199.248.13 <b>Country:</b> United States of America <b>Region:</b> New York <b>City:</b> New York City <b>Latitude:</b> 40.739288 <b>Longitude:</b> -73.984955 <b>View:</b> <a href="#">Google Map</a>

## EMAILS

EMAIL	FILE
wp1@itamar-medical.com	l7/G.java
u0013android@android.com0 u0013android@android.com	i4/n.java

## TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	<a href="https://reports.exodus-privacy.eu.org trackers/27">https://reports.exodus-privacy.eu.org trackers/27</a>

## HARDCODED SECRETS

## POSSIBLE SECRETS

```
"com.google.firebase.crashlytics.mapping_file_id" : "054eafb412f744b6b2ced286e6bccd16"
```

```
"google_api_key": "AlzaSyBW19IE4h6WDGD3wHnFA5c-MjTAMazkPCw"
```

```
"google_crash_reporting_api_key": "AlzaSyBW19IE4h6WDGD3wHnFA5c-MjTAMazkPCw"
```

```
"password" : "Password:"
```

[illegible]

5181942b9ebc31ce68dacb56c16fd79f

16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a

ae2044fb577e65ee8bb576ca48a2f06e

edef8ba9-79d6-4ace-a3c8-27dcd51d21ed

470fa2b4ae81cd56ecbda9735803434cec591fa

9a04f079-9840-4286-ab92-e65be0885f95

6e400001-b5a3-f393-e0a9-e50e24dcca9e

6e400002-b5a3-f393-e0a9-e50e24dcca9e

6e400003-b5a3-f393-e0a9-e50e24dcca9e

e2719d58-a985-b3c9-781a-b030af78d30e

# PLAYSTORE INFORMATION

**Title:** WatchPAT

**Score:** 3.8921568 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** [com.itamarmedical.watchpat](https://play.google.com/store/apps/details?id=com.itamarmedical.watchpat)

**Developer Details:** Itamar Medical, Itamar+Medical, None, <https://www.itamar-medical.com/>, [itamar.medical.development@gmail.com](mailto:itamar.medical.development@gmail.com),

**Release Date:** Jul 29, 2019 **Privacy Policy:** [Privacy link](#)

**Description:**

Sleep patterns monitoring, analysis and detection of sleep related issues

## SCAN LOGS

Timestamp	Event	Error
2025-08-30 22:15:36	Generating Hashes	OK
2025-08-30 22:15:36	Extracting APK	OK
2025-08-30 22:15:36	Unzipping	OK
2025-08-30 22:15:36	Parsing APK with androguard	OK
2025-08-30 22:15:37	Extracting APK features using aapt/aapt2	OK

2025-08-30 22:15:37	Getting Hardcoded Certificates/Keystores	OK
2025-08-30 22:15:39	Parsing AndroidManifest.xml	OK
2025-08-30 22:15:40	Extracting Manifest Data	OK
2025-08-30 22:15:40	Manifest Analysis Started	OK
2025-08-30 22:15:40	Performing Static Analysis on: WatchPAT (com.itamarmedical.watchpat)	OK
2025-08-30 22:15:40	Fetching Details from Play Store: com.itamarmedical.watchpat	OK
2025-08-30 22:15:41	Checking for Malware Permissions	OK
2025-08-30 22:15:41	Fetching icon path	OK
2025-08-30 22:15:41	Library Binary Analysis Started	OK
2025-08-30 22:15:41	Reading Code Signing Certificate	OK
2025-08-30 22:15:41	Running APKiD 2.1.5	OK

2025-08-30 22:15:43	Detecting Trackers	OK
2025-08-30 22:15:43	Decompiling APK to Java with JADX	OK
2025-08-30 22:15:57	Converting DEX to Smali	OK
2025-08-30 22:15:57	Code Analysis Started on - java_source	OK
2025-08-30 22:15:59	Android SBOM Analysis Completed	OK
2025-08-30 22:16:09	Android SAST Completed	OK
2025-08-30 22:16:09	Android API Analysis Started	OK
2025-08-30 22:16:23	Android API Analysis Completed	OK
2025-08-30 22:16:23	Android Permission Mapping Started	OK
2025-08-30 22:16:32	Android Permission Mapping Completed	OK
2025-08-30 22:16:33	Android Behaviour Analysis Started	OK

2025-08-30 22:16:45	Android Behaviour Analysis Completed	OK
2025-08-30 22:16:45	Extracting Emails and URLs from Source Code	OK
2025-08-30 22:16:48	Email and URL Extraction Completed	OK
2025-08-30 22:16:48	Extracting String data from APK	OK
2025-08-30 22:16:49	Extracting String data from Code	OK
2025-08-30 22:16:49	Extracting String values and entropies from Code	OK
2025-08-30 22:16:50	Performing Malware check on extracted domains	OK
2025-08-30 22:16:55	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](#).