MOBSF

ANDROID STATIC ANALYSIS REPORT

No icon

MyZio (2.1.1-rc2)

File Name:	com.irhythm.myzio.android_1944.apk
Package Name:	com.irhythm.myzio.android
Scan Date:	Aug. 30, 2025, 10:14 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	16	2	3	1

FILE INFORMATION

File Name: com.irhythm.myzio.android_1944.apk
Size: 12.83MB
MD5: a0cfe2694d8d1a3ec6bf172efc67ca42
SHA1: 307e452baf752d723a31e837af070aa487e94fff
SHA256: 6d3d5d87b4edc79c4d4a11303f1a527e093d68e6b5a616a48430f548f6b0ba5b

APP INFORMATION

App Name: MyZio
Package Name: com.irhythm.myzio.android
Main Activity: com.irhythm.myzio.android.AppActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 2.1.1-rc2

Android Version Code: 1944

APP COMPONENTS

Activities: 8
Services: 9
Receivers: 4
Providers: 3
Exported Activities: 2
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: O=IRhythmTech, OU=IRhythmTech, CN=IRhythmTech
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-03-10 13:38:02+00:00
Valid To: 2042-03-04 13:38:02+00:00
Issuer: O=IRhythmTech, OU=IRhythmTech, CN=IRhythmTech
Serial Number: 0x75508147
Hash Algorithm: sha256
md5: d12ab0f8ec7bc7648cde00e834e01aaf
sha1: 9deb4e7664aa9c5afe4a5694af7262cf70242112
sha256: 3ff04b79b04620fbe3921561aff0d76d53d13866cad18c3ebfd2aa57df9f7561
sha512: 27641b6ce4c463cebd88acfbde5a322ffd260f034037ff33728165f96ba10ff0cabe0a0a0f3967f658b66dcdc23bae91e3ca5d54cd19b420c3f411feebe445cb
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 7767ad4e08f450d4e82e339e81ba35b62010bf289f9d443ab38080b09b32bd04
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.
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.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.irhythm.myzio.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>a0cfe2694d8d1a3ec6bf172efc67ca42.apk</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>possible VM check</td></tr></table></td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check
Build.BOARD check
SIM operator check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.irhythm.myzio.android.AppActivity	Schemes: https://, Hosts: @string/deeplink_host_uk, @string/deeplink_host_us, Path Prefixes: /main/MESSAGES, /reset,
sdk.pendo.io.activities.PendoGateActivity	Schemes: pendo-f6ba59ea://,

🔒 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: **5** | 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	Activity (sdk.pendo.io.activities.PendoGateActivity) 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.
3	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.
4	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.
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.

CODE ANALYSIS

HIGH: **2** | WARNING: **9** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				a0/e.java a0/h.java ab/b.java b0/b.java b8/a.java bb/f.java bb/h.java bb/j.java bb/l.java bb/n.java bb/o.java bb/p.java bb/q.java bb/s.java bb/t.java bb/v.java c4/a1.java c4/j.java c4/t0.java c5/b.java c5/c.java c5/g.java c8/e.java cb/b.java cb/d.java cb/i.java cc/a.java cg/p.java d/d.java d3/y.java d4/f.java d8/a.java da/e.java da/g.java e1/k1.java e5/c.java ea/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ec/b.java ed/c.java ei/e.java external/sdk/pendo/io/com/appmattus/certificatetransparency/internal/loglist/model/v2/Log$$serializer.java external/sdk/pendo/io/glide/a.java external/sdk/pendo/io/glide/gifdecoder/StandardGifDecoder.java external/sdk/pendo/io/glide/gifdecoder/d.java external/sdk/pendo/io/glide/load/data/AssetPathFetcher.java external/sdk/pendo/io/glide/load/data/HttpUrlFetcher.java external/sdk/pendo/io/glide/load/data/LocalUriFetcher.java external/sdk/pendo/io/glide/load/data/mediastore/ThumbFetcher.java external/sdk/pendo/io/glide/load/data/mediastore/c.java external/sdk/pendo/io/glide/load/engine/Engine.java external/sdk/pendo/io/glide/load/engine/bitmap_recycle/LruArrayPool.java external/sdk/pendo/io/glide/load/engine/bitmap_recycle/LruBitmapPool.java external/sdk/pendo/io/glide/load/engine/cache/DiskLruCacheWrapper.java external/sdk/pendo/io/glide/load/engine/g.java external/sdk/pendo/io/glide/load/engine/h.java external/sdk/pendo/io/glide/load/engine/n.java external/sdk/pendo/io/glide/load/engine/u.java external/sdk/pendo/io/glide/load/model/ByteBufferEncoder.java external/sdk/pendo/io/glide/load/model/ByteBufferFileLoader.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				external/sdk/pendo/io/glide/load/model/FileLoader.java external/sdk/pendo/io/glide/load/model/ResourceLoader.java external/sdk/pendo/io/glide/load/model/StreamEncoder.java external/sdk/pendo/io/glide/load/resource/ImageDecoderResourceDecoder.java external/sdk/pendo/io/glide/load/resource/bitmap/BitmapEncoder.java external/sdk/pendo/io/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java external/sdk/pendo/io/glide/load/resource/bitmap/DefaultImageHeaderParser.java external/sdk/pendo/io/glide/load/resource/bitmap/VideoDecoder.java external/sdk/pendo/io/glide/load/resource/bitmap/b.java external/sdk/pendo/io/glide/load/resource/bitmap/c.java external/sdk/pendo/io/glide/load/resource/bitmap/d.java external/sdk/pendo/io/glide/load/resource/gif/ByteBufferGifDecoder.java external/sdk/pendo/io/glide/load/resource/gif/GifDrawableEncoder.java external/sdk/pendo/io/glide/load/resource/gif/StreamGifDecoder.java external/sdk/pendo/io/glide/manager/DefaultConnectivityMonitorFactory.java external/sdk/pendo/io/glide/manager/b.java external/sdk/pendo/io/glide/request/SingleRequest.java external/sdk/pendo/io/glide/request/target/CustomViewTarget.java external/sdk/pendo/io/glide/request/target/ViewTarget.java external/sdk/pendo/io/mozilla/javascript/ScriptRuntime.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				external/sdk/pendo/io/mozilla/javascript/tools/debugger/Dim.java external/sdk/pendo/io/mozilla/javascript/tools/idswitch/Main.java external/sdk/pendo/io/mozilla/javascript/tools/jsc/Main.java f/a0.java f/b0.java f/e.java f/f0.java f/o0.java f/s.java f4/m.java f4/q.java f8/e.java f8/g.java fb/a.java fb/b.java fd/y2.java g4/f.java g4/h.java g4/i.java gb/c.java h0/f.java h0/k.java h0/r.java h4/d.java ha/j.java hb/b.java hh/l.java i/i.java i/j.java ic/e.java ih/d.java j/i.java j/o.java j0/a.java j1/y.java k/e1.java k/g2.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	k/g3.java k/i.java k/j.java k/k3.java k/l0.java k/l2.java k/z.java k/z3.java k4/o.java k8/r.java kc/a.java kc/c.java kc/d.java l4/a.java l5/o.java l5/r.java l5/t.java l8/a1.java l8/d8.java l8/m5.java l8/n5.java l8/p5.java la/a.java la/c.java la/d.java m1/q2.java m7/c.java m7/i.java n5/d.java n6/i.java n8/l6.java net/sqlcipher/AbstractCursor.java net/sqlcipher/BulkCursorToCursorAdaptor.java net/sqlcipher/DatabaseUtils.java net/sqlcipher/DefaultDatabaseErrorHandler.java net/sqlcipher/database/SQLiteCompiledSql.java net/sqlcipher/database/SQLiteContentHelper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				net/sqlcipher/database/SQLiteDatabase.java net/sqlcipher/database/SQLiteDebug.java net/sqlcipher/database/SQLiteOpenHelper.java net/sqlcipher/database/SQLiteProgram.java net/sqlcipher/database/SQLiteQuery.java net/sqlcipher/database/SQLiteQueryBuilder.java net/sqlcipher/database/SqliteWrapper.java p4/c1.java p4/c2.java p4/q0.java p4/x.java p4/x1.java p4/y1.java p5/d1.java p5/n0.java p5/x.java p5/y0.java pb/b.java q/a0.java q/b2.java q/g0.java q/h.java q/i1.java q/i2.java q/y.java q8/b6.java q8/d6.java q8/h6.java q8/i3.java q8/i6.java q8/m6.java qa/e.java qa/g.java r2/f.java r4/b.java r6/n.java r7/a.java r7/b.java r9/e.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				s0/t0.java s3/e.java s4/v.java s5/b.java s8/a.java s9/a.java sb/c.java sdk/pendo/io/PendoInternal.java sdk/pendo/io/activities/PendoGateActivity.java sdk/pendo/io/c0/j.java sdk/pendo/io/c0/k.java sdk/pendo/io/c0/m.java sdk/pendo/io/c0/n.java sdk/pendo/io/g3/c.java sdk/pendo/io/g9/a.java sdk/pendo/io/h0/a.java sdk/pendo/io/i8/e.java sdk/pendo/io/j0/a.java sdk/pendo/io/j7/g.java sdk/pendo/io/logging/PendoLogger.java sdk/pendo/io/logging/c.java sdk/pendo/io/p/a.java sdk/pendo/io/p8/a.java sdk/pendo/io/v/a.java sdk/pendo/io/w/a.java sdk/pendo/io/w/b.java sdk/pendo/io/y/b.java t3/a0.java t3/e0.java t3/h.java t3/j.java t3/j0.java t3/k0.java t3/n.java t3/s.java t3/y.java t4/c.java t5/e.java t8/a.java tb/b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				u5/a.java u7/b.java u7/c.java u7/d.java u7/g.java u7/h.java u7/i.java u7/k.java u7/l.java u7/m.java u9/h.java ub/c.java v1/l.java v3/f.java v6/c.java v7/d.java v7/e.java v7/h.java v7/i.java v7/j.java v7/n.java v7/r.java v7/u.java v9/c.java va/c.java va/d.java va/e.java va/i.java w/c.java w0/n0.java w4/e.java w8/e.java w9/g.java w9/i.java w9/k.java x/o0.java x/x0.java x7/e.java x7/n.java xa/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				xb/c0.java xb/e.java xb/e0.java xb/g.java xb/i.java xb/m.java xb/o.java xb/r.java xb/s.java xb/t.java xb/u.java xb/x.java xb/y.java xb/z.java y/l.java y1/f.java y3/a.java y3/c.java y3/f.java y3/h.java y3/l.java y3/r.java y3/s.java y7/e.java y7/h.java y7/h0.java y7/i0.java y7/k0.java y7/l.java y7/n0.java y7/s.java y7/v.java ya/b.java ya/c.java z9/h.java za/c.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	a0/f.java ag/a.java f4/m.java q8/h6.java ra/a.java sdk/pendo/io/j3/d.java sdk/pendo/io/j3/h.java sdk/pendo/io/j4/f.java sdk/pendo/io/v4/c.java sdk/pendo/io/v4/d.java sdk/pendo/io/w2/z.java zf/a.java zf/b.java
3	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	c3/j.java c3/n0.java dd/f2.java dd/w1.java ed/v0.java external/sdk/pendo/io/com/appmattus/certificatetransparency/internal/loglist/model/v2/Log.java external/sdk/pendo/io/glide/load/engine/c.java external/sdk/pendo/io/glide/load/engine/m.java external/sdk/pendo/io/glide/load/engine/s.java external/sdk/pendo/io/mozilla/javascript/ClassCache.java external/sdk/pendo/io/mozilla/javascript/NativeError.java external/sdk/pendo/io/mozilla/javascript/NativeJavaObject.java external/sdk/pendo/io/mozilla/javascript/ScriptRuntime.java external/sdk/pendo/io/mozilla/javascript/xmli

NO	ISSUE	SEVERITY	STANDARDS	FILES
				mpl/XmlNode.java m1/h2.java m1/q1.java sdk/pendo/io/actions/ActivationManager.java sdk/pendo/io/actions/FloatingVisualGuide.java sdk/pendo/io/actions/ToolTipVisualGuide.java sdk/pendo/io/actions/handlers/PendoGlobalCommandHandler.java sdk/pendo/io/d1/e.java sdk/pendo/io/m/d.java sdk/pendo/io/models/GlobalEventPropertiesKt.java sdk/pendo/io/models/StepModel.java sdk/pendo/io/n/b.java sdk/pendo/io/q/g.java sdk/pendo/io/views/custom/videoplayer/PendoYoutubePlayer.java v6/d.java vg/t0.java
4	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	hh/d.java hh/g.java hh/k.java hh/l.java sdk/pendo/io/f3/c.java sdk/pendo/io/f3/d.java sdk/pendo/io/f3/g.java sdk/pendo/io/f3/h.java sdk/pendo/io/k/d.java sdk/pendo/io/t4/c.java sdk/pendo/io/t4/p0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	h0/f.java l8/u5.java m7/c.java m7/h.java m7/i.java n7/m.java net/sqlcipher/database/SQLiteDatabase.java q/b2.java q/f.java q/f0.java q/h.java q8/d3.java q8/d6.java q8/i.java q8/j3.java
6	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	bb/f.java fb/b.java sdk/pendo/io/g9/m.java tb/b.java ub/c.java
7	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	bb/f.java da/g.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	external/sdk/pendo/io/mozilla/javascript/tools/shell/Main.java q8/h6.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	external/sdk/pendo/io/mozilla/javascript/tools/debugger/Dim.java sdk/pendo/io/a4/b.java sdk/pendo/io/b4/b.java sdk/pendo/io/d4/b.java sdk/pendo/io/e4/d.java sdk/pendo/io/e4/f.java sdk/pendo/io/e4/k.java sdk/pendo/io/f4/h.java sdk/pendo/io/j/b.java sdk/pendo/io/j/j.java sdk/pendo/io/k/i.java sdk/pendo/io/n3/b.java sdk/pendo/io/o3/a.java sdk/pendo/io/r3/a.java sdk/pendo/io/s3/a.java sdk/pendo/io/v3/b.java sdk/pendo/io/x3/a.java sdk/pendo/io/y3/a.java sdk/pendo/io/z3/a.java
10	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	sdk/pendo/io/views/custom/videoplayer/PendoYoutubePlayer.java
11	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	sdk/pendo/io/PendoInternal.java sdk/pendo/io/r8/a.java
12	This App uses SQL Cipher. SQLCipher provides 256-bit AES encryption to sqlite database files.	info	OWASP MASVS: MSTG-CRYPTO-1	net/sqlcipher/database/SupportHelper.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
13	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	a0/h.java
14	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	external/sdk/pendo/io/daimajia/BuildConfig.java
15	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	q8/i6.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES

RULE ID	BEHAVIOUR	LABEL	FILES
00162	Create InetSocketAddress object and connecting to it	socket	hh/c.java hh/l.java sdk/pendo/io/f3/b.java sdk/pendo/io/f3/h.java sdk/pendo/io/t4/b1.java
00163	Create new Socket and connecting to it	socket	hh/c.java hh/l.java sdk/pendo/io/f3/b.java sdk/pendo/io/f3/h.java sdk/pendo/io/t4/b1.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	bb/f.java c5/g.java cb/d.java cg/p.java external/sdk/pendo/io/glide/load/a.java external/sdk/pendo/io/glide/load/model/FileLoader.java external/sdk/pendo/io/mozilla/javascript/tools/SourceReader.java external/sdk/pendo/io/mozilla/javascript/tools/debugger/Dim.java external/sdk/pendo/io/mozilla/javascript/tools/idswitch/Main.java external/sdk/pendo/io/mozilla/javascript/tools/shell/Global.java fb/a.java h4/d.java hb/b.java l8/p5.java mh/u.java n5/a.java n5/d.java n5/h.java n8/l6.java q8/i6.java sdk/pendo/io/g9/h.java sdk/pendo/io/p/a.java sdk/pendo/io/t4/m1.java sdk/pendo/io/t4/n0.java
00012	Read data and put it into a buffer stream	file	c5/g.java sdk/pendo/io/t4/m1.java sdk/pendo/io/t4/n0.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/irhythm/myzio/android/PushMessagingService.java ha/j.java j/g.java l5/p.java l5/q.java l5/r.java m5/m.java r0/a.java sdk/pendo/io/actions/handlers/PendoGlobalCommandHandler.java u7/f.java v7/e.java
00022	Open a file from given absolute path of the file	file	cb/d.java external/sdk/pendo/io/mozilla/javascript/tools/jsc/Main.java q6/a.java sdk/pendo/io/g9/h.java
00094	Connect to a URL and read data from it	command network	external/sdk/pendo/io/mozilla/javascript/tools/shell/Global.java ha/j.java j/g.java q8/l3.java
00109	Connect to a URL and get the response code	network command	external/sdk/pendo/io/glide/load/data/HttpUrlFetcher.java external/sdk/pendo/io/mozilla/javascript/commonjs/module/provider/UrlModuleSourceProvider.java j/g.java q/h.java q8/l3.java r7/b.java ub/c.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	cc/a.java external/sdk/pendo/io/glide/load/data/mediastore/ThumbFetcher.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	external/sdk/pendo/io/glide/load/data/HttpUrlFetcher.java external/sdk/pendo/io/mozilla/javascript/commonjs/module/provider/UrlModuleSourceProvider.java j/g.java q/h.java q8/l3.java ub/c.java
00030	Connect to the remote server through the given URL	network	external/sdk/pendo/io/glide/load/data/HttpUrlFetcher.java external/sdk/pendo/io/mozilla/javascript/commonjs/module/provider/UrlModuleSourceProvider.java q8/l3.java
00108	Read the input stream from given URL	network command	j/g.java q8/l3.java
00114	Create a secure socket connection to the proxy address	network command	dh/l.java sdk/pendo/io/b3/f.java
00096	Connect to a URL and set request method	command network	q/h.java
00125	Check if the given file path exist	file	q/h.java
00091	Retrieve data from broadcast	collection	l8/p5.java
00075	Get location of the device	collection location	f/e.java
00137	Get last known location of the device	location collection	f/e.java
00130	Get the current WIFI information	wifi collection	sdk/pendo/io/l8/d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00065	Get the country code of the SIM card provider	collection	sdk/pendo/io/l8/e.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	ha/j.java m5/m.java v7/e.java
00014	Read file into a stream and put it into a JSON object	file	cb/d.java hb/b.java q8/i6.java
00005	Get absolute path of file and put it to JSON object	file	cb/d.java
00047	Query the local IP address	network collection	sdk/pendo/io/t4/e1.java
00191	Get messages in the SMS inbox	sms	k/g3.java
00036	Get resource file from res/raw directory	reflection	ha/j.java k/g3.java n6/c.java v7/e.java
00004	Get filename and put it to JSON object	file collection	q8/i6.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/475193168757/namespaces/firebase:fetch?key=AIzaSyDaWpPJGbLq6QJFUCy3Q1M8P-3HhZNE2Kk. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.VIBRATE, android.permission.WAKE_LOCK
Other Common Permissions	3/44	com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, 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
www.googleadservices.com	ok	**IP:** 142.250.189.2 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gle	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.zetetic.net	ok	**IP:** 18.238.96.79 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
plus.google.com	ok	**IP:** 172.217.12.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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
data.eu.pendo.io	ok	**IP:** 34.110.214.126 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
www.irhythmtech.com	ok	**IP:** 151.101.67.10 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.113.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
videos.myzio.com	ok	**IP:** 18.238.96.35 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
developer.android.com	ok	**IP:** 172.217.14.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
help-dev.myzio.com	ok	**IP:** 18.238.109.83 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	**IP:** 31.97.181.89 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Bowness-on-Windermere **Latitude:** 54.363312 **Longitude:** -2.918590 **View:** Google Map
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
www.myzio.co.uk	ok	**IP:** 18.238.96.71 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.youtube.com	ok	**IP:** 142.250.72.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
data.jpn.pendo.io	ok	**IP:** 34.149.195.87 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
www.myzio.com	ok	**IP:** 18.238.109.51 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
127.0.0.1	ok	**IP:** 127.0.0.1 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
help.myzio.com	ok	**IP:** 18.155.173.12 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.gstatic.com	ok	**IP:** 142.251.40.35 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
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
ktor.io	ok	**IP:** 13.224.53.49 **Country:** United States of America **Region:** Arizona **City:** Phoenix **Latitude:** 33.448380 **Longitude:** -112.074043 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
schemas.android.com	ok	No Geolocation information available.
data.pendo.io	ok	**IP:** 34.107.204.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
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
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
us1.data.pendo.io	ok	**IP:** 34.110.177.118 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

✉ EMAILS

EMAIL	FILE
ck_received_xt_00004@myzio.com ck_finished_at_00003@myzio.com aring_shastaxt_00001@myzio.com ck_tracking_xt_00002@myzio.com ck_finished_xt_00003@myzio.com ock_wearing_at_00001@myzio.com ock_wearing_xt_00001@myzio.com ck_tracking_at_00002@myzio.com eived_shastaxt_00004@myzio.com ished_shastaxt_00003@myzio.com ck_received_at_00004@myzio.com cking_shastaxt_00002@myzio.com	ud/b.java
jfrey@irhythmtech.com	zc/e.java
u0013android@android.com0 u0013android@android.com	v7/p.java

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

TRACKER	CATEGORIES	URL
Pendo	Analytics	https://reports.exodus-privacy.eu.org/trackers/416

HARDCODED SECRETS

POSSIBLE SECRETS
"api_host_uk" : "api.myzio.co.uk"
"api_host_us" : "api.myzio.com"
"com.google.firebase.crashlytics.mapping_file_id" : "93209691026443d284fe334e76521d06"
"google_api_key" : "AIzaSyDaWpPJGbLq6QJFUCy3Q1M8P-3HhZNE2Kk"
"google_crash_reporting_api_key" : "AIzaSyDaWpPJGbLq6QJFUCy3Q1M8P-3HhZNE2Kk"
"library_android_database_sqlcipher_authorWebsite" : "https://www.zetetic.net/sqlcipher/"
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A93AD2CAFFFFFFFFFFFFFFFF
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1B6qsa2sbpc4CuFEjgRWez9nN

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DCC4024FFFFFFFFFFFFFFFF
41058363725152142129326129780047268409114441015993725554835256314039467401291
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B66C62E37FFFFFFFFFFFFFFFF
fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7
VTdL1VbC2tejvcI2BlMkEpk1BzBZI0KQB0GaDWFLN
Vd99BKh6pxt3mXSDJzHuVrCq52xBXAKVahbuFb6dqBc
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AACAA68FFFFFFFFFFFFFFFF

POSSIBLE SECRETS
32670510020758816978083085130507043184471273380659243275938904335757337482424
nvknbo5+6pBVWVZpCg5Rtpii3JUKMxOmJrccBCo7ICIqPIj/L9Nc5zmWMH2igKHLq
95475cf5d93e596c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bbdd84c9836be1f31c0777725aeb6c2fc38b85f48076fa76bcd8146cc89a6fb2f706dd719898c2083dc8d896f84062e2c9c94d137b054a8d8096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9eb60eee8b030376b236bc73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520086746175c8885925ebc64c6147906773496990cb714ec667304e261faee33b3cbdf008e0c3fa90650d97d3909c9275bf4ac86ffcb3d03e6dfc8ada5934242dd6d3bcca2a406cb0b
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B423861285C97FFFFFFFFFFFFFFFF
55066263022277343669578718895168534326250603453777594175500187360389116729240
sha256/CSQXOhdMIW0brwDlUwD3WVimKx9VYLdtqFVfMrngHLg=
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE65381FFFFFFFFFFFFFFFF

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C6272B045B3B71F9DC6B80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CCFF46AAA36AD004CF600C8381E425A31D951AE64FDB23FCEC9509D43687FEB69EDD1CC5E0B8CC3BDF64B10EF86B63142A3AB8829555B2F747C932665CB2C0F1CC01BD70229388839D2AF05E454504AC78B7582822846C0BA35C35F5C59160CC046FD8251541FC68C9C86B022BB7099876A460E7451A8A93109703FEE1C217E6C3826E52C51AA691E0E423CFC99E9E31650C1217B624816CDAD9A95F9D5B8019488D9C0A0A1FE3075A577E23183F81D4A3F2FA4571EFC8CE0BA8A4FE8B6855DFE72B0A66EDED2FBABFBE58A30FAFABE1C5D71A87E2F741EF8C1FE86FEA6BBFDE530677F0D97D11D49F7A8443D0822E506A9F4614E011E2A94838FF88CD68C8BB7C5C6424CFFFFFFFFFFFFFFFF
115792089237316195423570985008687907852837564279074904382605163141518161494337
099c76f4-a3f1-41ad-a0d2-46e790697f91
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
115792089210356248762697446949407573530086143415290314195533631308867097853951
26617408020502170632287687167233609607298591687569731477066713684188029449964278084915450806277719023520942412250655586621571135455709168141616373158959998466
68647976601306097149819007990813932172694353001433054093944634591855431833976553942450577463332171975329639963713633211138647686124403803403728088927070054449
sha256/DxH4tt40L+eduF6szpY6TONlxhZhBd+pJ9wbHlQ2fuw=

POSSIBLE SECRETS
9cdbd84c9f1ac2f38d0f80f42ab952e7338bf511
83257109614890299855467512895201081792878530488613155947092059024805031998844192244386437603929473330780865116278 71
115792089210356248762697446949407573529996955224135760342422259061068512044369
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E0DD9020BFD64B645036C7A4E677D2C38532A3A23BA4442CAF53EA63BB454329B7624C8917BDD64B1C0FD4CB38E8C334C701C3ACDAD0657FCCFEC719B1F5C3E4E46041F388147FB4CFDB477A52471F7A9A96910B855322EDB6340D8A00EF092350511E30ABEC1FFF9E3A26E7FB29F8C183023C3587E38DA0077D9B4763E4E4B94B2BBC194C6651E77CAF992EEAAC0232A281BF6B3A739C1226116820AE8DB5847A67CBEF9C9091B462D538CD72B03746AE77F5E62292C311562A846505DC82DB854338AE49F5235C95B91178CCF2DD5CACEF403EC9D1810C6272B045B3B71F9DC6B80D63FDD4A8E9ADB1E6962A69526D43161C1A41D570D7938DAD4A40E329CD0E40E65FFFFFFFFFFFFFFFF
30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d2029d83c1c158547f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346d3f529252
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
AC6BDB41324A9A9BF166DE5E1389582FAF72B6651987EE07FC3192943DB56050A37329CBB4A099ED8193E0757767A13DD52312AB4B03310DCD7F48A9DA04FD50E8083969EDB767B0CF6095179A163AB3661A05FBD5FAAAE82918A9962F0B93B855F97993EC975EEAA80D740ADBF4FF747359D041D5C33EA71D281E446B14773BCA97B43A23FB801676BD207A436C6481F1D2B9078717461A5B9D32E688F87748544523B524B0D57D5EA77A2775D2ECFA032CFBDBF52FB3786160279004E57AE6AF874E7303CE53299CCC041C7BC308D82A5698F3A8D0C38271AE35F8E9DBFBB694B5C803D89F7AE435DE236D525F54759B65E372FCD68EF20FA7111F9E4AFF73
sha256/++MBgDH5WGvL9Bcn5Be30cRcL0f5O+NyoXuWtQdX1aI=

POSSIBLE SECRETS
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394 2643
10938490380737342745111123907668055699362075989516837489945863944959531161507350160137087375737596232485921322967063133094384525315910129121423274884789859 84
37571800257700204635455072244911836035944551347697624866945677796155444774405563166912344050129455395621444445372894285225856667291965808101243442775783767 84
033c76f4-a3f1-41ad-a0d2-46e790697f91
EEAF0AB9ADB38DD69C33F80AFA8FC5E86072618775FF3C0B9EA2314C9C256576D674DF7496EA81D3383B4813D692C6E0E0D5D8E250B98BE48E495C1D6089DAD15DC7D7B46154D6B6CE8EF4AD69B15D4982559B297BCF1885C529F566660E57EC68EDBC3C05726CC02FD4CBF4976EAA9AFD5138FE8376435B9FC61D2FC0EB06E3
f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a
962eddcc369cba8ebb260ee6b6a126d9346e38c5
FFFFFFFFFFFFFFFFADF85458A2BB4A9AAFDC5620273D3CF1D8B9C583CE2D3695A9E13641146433FBCC939DCE249B3EF97D2FE363630C75D8F681B202AEC4617AD3DF1ED5D5FD65612433F51F5F066ED0856365553DED1AF3B557135E7F57C935984F0C70E0E68B77E2A689DAF3EFE8721DF158A136ADE73530ACCA4F483A797ABC0AB182B324FB61D108A94BB2C8E3FBB96ADAB760D7F4681D4F42A3DE394DF4AE56EDE76372BB190B07A7C8EE0A6D709E02FCE1CDF7E2ECC03404CD28342F619172FE9CE98583FF8E4F1232EEF28183C3FE3B1B4C6FAD733BB5FCBC2EC22005C58EF1837D1683B2C6F34A26C1B2EFFA886B4238611FCFDCDE355B3B6519035BBC34F4DEF99C023861B46FC9D6E6C9077AD91D2691F7F7EE598CB0FAC186D91CAEFE130985139270B4130C93BC437944F4FD4452E2D74DD364F2E21E71F54BFF5CAE82AB9C9DF69EE86D2BC522363A0DABC521979B0DEADA1DBF9A42D5C4484E0ABCD06BFA53DDEF3C1B20EE3FD59D7C25E41D2B669E1EF16E6F52C3164DF4FB7930E9E4E58857B6AC7D5F42D69F6D187763CF1D5503400487F55BA57E31CC7A7135C886EFB4318AED6A1E012D9E6832A907600A918130C46DC778F971AD0038092999A333CB8B7A1A1DB93D7140003C2A4ECEA9F98D0ACC0A8291CDCEC97DCF8EC9B55A7F88A46B4DB5A851F44182E1C68A007E5E655F6AFFFFFFFFFFFFFFFF
115792089210356248762697446949407573530086143415290314195533631308867097853948
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA237327FFFFFFFFFFFFFFFF

POSSIBLE SECRETS
115792089237316195423570985008687907853269984665640564039457584007908834671663
fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17
27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575
470fa2b4ae81cd56ecbcda9735803434cec591fa
IWvsYcGISw67dizNL4POm20jfi9nRGlDLKbXBm8ds42riYe7JymtRpcNoRsuDy2OmMxk2ow
678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C934063199FFFFFFFFFFFFFFFF
b869c82b35d70e1b1ff91b28e37a62ecdc34409b
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
42debb9da5b3d88cc956e08787ec3f3a09bba5f48b889a74aaf53174aa0fbe7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76137e792f3f0db859d095e4a5b932024f079ecf2ef09c797452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94cccf1449ac43d586d0beee43251b0b2287349d68de0d144403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1b27d0639f695e347d8d1cf9ac819a26ca9b04cb0eb9b7b035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffbc97134025fe8ce04c4399ad96569be91a546f4978693c7a
1cf97e06-85b1-4a6d-87f1-d828e9daa0ba

POSSIBLE SECRETS
sXchDaQebHnPiGvyDOAT4saGEUetSyo9MKLOoWFsueri23bOdgWp4Dy1WlUzewbgBHod5pcM9H95GQRV3JDXboIRROSBigeC5yjU1hGzHHyXss8UDprecbAYxknTcQkhslANGRUZmdTOQ5qTRsLAt6BTYuyvVRdhS8exSZEy
FDB497E7C6F9D71A89D042B0FA5B7A4DEA5EE7938F08CFDA9F1FB58EBDF749E7
48439561293906451759052585252797914202762949526041747995844080717082404635286
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112316
b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae466748d9b5a536
0b9c76f4-a3f1-41ad-a0d2-46e790697f91
mTXGHffQH60PUAftuehx0SxdC4Q6QuG84twNvZjh34ot6RZfKBxJoGIYI3kFey1Rv8E
9760508f15230bccb292b982a2eb840bf0581cf5
e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf
36134250956749795798585127919587881956611106672985015071877198253568414405109
9DEF3CAFB939277AB1F12A8617A47BBBDBA51DF499AC4C80BEEEA9614B19CC4D5F4F5F556E27CBDE51C6A94BE4607A291558903BA0D0F84380B655BB9A22E8DCDF028A7CEC67F0D08134B1C8B97989149B609E0BE3BAB63D47548381DBC5B1FC764E3F4B53DD9DA1158BFD3E2B9C8CF56EDF019539349627DB2FD53D24B7C48665772E437D6C7F8CE442734AF7CCB7AE837C264AE3A9BEB87F8A2FE9B8B5292E5A021FFF5E91479E8CE7A28C2442C6F315180F93499A234DCF76E3FED135F9BB
eyJkYXRhY2VudGVyIjoidXMiLCJrZXkiOiI2OTJlZDRhMWMwYjdmMDM0YWYzMDhiNWMzYWUzNzE0YjBhZGU5NDI5NDQwZjg3ZWE2ZTUzZjRjODU4NTUxYTJiMjgzZGE1OWVjNTRlZGNmYmQwNjNhMTJmOGVmNzQ0NDhjMTk5MjNlN2ZjYTAyMmUzOGViNjkyY2I2OTk0OWQwODlmZTNlMDZlMGM5ZGI4Y2VlYmU0OTBiMmM1NDFlM2UyLjY5OWYyY2VlN2RmMjI4ZDhlMzQzYzVjZDNmYTliZDRhLjI5ZWNjNjFlNTQwM2NjYWExZjg2NmMzNTVhM2QwYzMyMTRlYzA0ZjIzNGE4M2Y3MDE0OGVlYTc3NTI0NTQxNWEifQ
77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399

POSSIBLE SECRETS
kKtp8EWjxLrSb9lMqKiG7W7V3UdL
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A63A3620FFFFFFFFFFFFFFFF
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCbelsiqvdpzGmRF3pex4Ar1HNI
f8183668ba5fc5bb06b5981e6d8b795d30b8978d43ca0ec572e37e09939a9773
Ct4eTlXHBIY2EaV7t7LjJaynVJCpkv4LKjTTAumiGUIuQhrNhZLuF
57896044618658097711785492504343953926634992332820282019728792003956564819949
8d5155894229d5e689ee01e6018a237e2cae64cd
sha256/18tkPyr2nckv4fgo0dhAkaUtJ2hu2831xlO2SKhq8dg=
726838724295606890549323807888004534353641360687318060281490199180612328166730772686396383698676545930088884461843637361053498018365439
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCv8IqRRwpH8s7EnWhLwuFqnbTA

POSSIBLE SECRETS
FFFFFFFFFFFFFFFFC90FDAA22168C234C4C6628B80DC1CD129024E088A67CC74020BBEA63B139B22514A08798E3404DDEF9519B3CD3A431B302B0A6DF25F14374FE1356D6D51C245E485B576625E7EC6F44C42E9A637ED6B0BFF5CB6F406B7EDEE386BFB5A899FA5AE9F24117C4B1FE649286651ECE45B3DC2007CB8A163BF0598DA48361C55D39A69163FA8FD24CF5F83655D23DCA3AD961C62F356208552BB9ED529077096966D670C354E4ABC9804F1746C08CA18217C32905E462E36CE3BE39E772C180E86039B2783A2EC07A28FB5C55DF06F4C52C9DE2BCBF6955817183995497CEA956AE515D2261898FA051015728E5A8AAAC42DAD33170D04507A33A85521ABDF1CBA64ECFB850458DBEF0A8AEA71575D060C7DB3970F85A6E1E4C7ABF5AE8CDB0933D71E8C94E04A25619DCEE3D2261AD2EE6BF12FFA06D98A0864D87602733EC86A64521F2B18177B200CBBE117577A615D6C770988C0BAD946E208E24FA074E5AB3143DB5BFCE0FD108E4B82D120A92108011A723C12A787E6D788719A10BDBA5B2699C327186AF4E23C1A946834B6150BDA2583E9CA2AD44CE8DBBBC2DB04DE8EF92E8EFC141FBECAA6287C59474E6BC05D99B2964FA090C3A2233BA186515BE7ED1F612970CEE2D7AFB81BDD762170481CD0069127D5B05AA993B4EA988D8FDDC186FFB7DC90A6C08F4DF435C93402849236C3FAB4D27C7026C1D4DCB2602646DEC9751E763DBA37BDF8FF9406AD9E530EE5DB382F413001AEB06A53ED9027D831179727B0865A8918DA3EDBEBCF9B14ED44CE6CBACED4BB1BDB7F1447E6CC254B332051512BD7AF426FB8F401378CD2BF5983CA01C64B92ECF032EA15D1721D03F482D7CE6E74FEF6D55E702F46980C82B5A84031900B1C9E59E7C97FBEC7E8F323A97A7E36CC88BE0F1D45B7FF585AC54BD407B22B4154AACC8F6D7EBF48E1D814CC5ED20F8037E0A79715EEF29BE32806A1D58BB7C5DA76F550AA3D8A1FBFF0EB19CCB1A313D55CDA56C9EC2EF29632387FE8D76E3C0468043E8F663F4860EE12BF2D5B0B7474D6E694F91E6DBE115974A3926F12FEE5E438777CB6A932DF8CD8BEC4D073B931BA3BC832B68D9DD300741FA7BF8AFC47ED2576F6936BA424663AAB639C5AE4F5683423B4742BF1C978238F16CBE39D652DE3FDB8BEFC848AD922222E04A4037C0713EB57A81A23F0C73473FC646CEA306B4BCBC8862F8385DDFA9D4B7FA2C087E879683303ED5BDD3A062B3CF5B3A278A66D2A13F83F44F82DDF310EE074AB6A364597E899A0255DC164F31CC50846851DF9AB48195DED7EA1B1D510BD7EE74D73FAF36BC31ECFA268359046F4EB879F924009438B481C6CD7889A002ED5EE382BC9190DA6FC026E479558E4475677E9AA9E3050E2765694DFC81F56E880B96E7160C980DD98EDD3DFFFFFFFFFFFFFFFF
26247035095799689268623156744566981891852923491109213387815615900925518854738050089022388053975719786650872476732087
nMcadFr9rwxGUMGOn8qIcjLE4vr9T1rxm6DekW9IBGNAwGOynuA+ebTfpfPMYY8nO

PLAYSTORE INFORMATION

Title: MyZio

Score: 4.6048055 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.irhythm.myzio.android

Developer Details: iRhythm Technologies, Inc., iRhythm+Technologies,+Inc., None, http://www.irhythmtech.com/contact-us, support@irhythmtech.com,

Release Date: Jul 12, 2017 **Privacy Policy:** Privacy link

Description:

MyZio® is the perfect companion app to the Zio® ECG monitor. Use the app to track your monitors shipping status, enter your symptoms, and access helpful information while wearing your Zio ECG monitor. Key Features: ◦ Signup for a MyZio account anytime ◦ Track your monitor’s shipping status ◦ Seamlessly register your

Zio ECG monitor and start logging symptoms. ◦ Enter your symptoms. View and edit your symptoms as needed. ◦ Access information about the Zio service. Instructional videos are included to help you throughout your Zio experience. *Features vary by market and country

SCAN LOGS

Timestamp	Event	Error
2025-08-30 22:14:00	Generating Hashes	OK
2025-08-30 22:14:00	Extracting APK	OK
2025-08-30 22:14:00	Unzipping	OK
2025-08-30 22:14:00	Parsing APK with androguard	OK
2025-08-30 22:14:00	Extracting APK features using aapt/aapt2	OK
2025-08-30 22:14:00	Getting Hardcoded Certificates/Keystores	OK
2025-08-30 22:14:02	Parsing AndroidManifest.xml	OK
2025-08-30 22:14:02	Extracting Manifest Data	OK

2025-08-30 22:14:02	Manifest Analysis Started	OK
2025-08-30 22:14:02	Performing Static Analysis on: MyZio (com.irhythm.myzio.android)	OK
2025-08-30 22:14:02	Fetching Details from Play Store: com.irhythm.myzio.android	OK
2025-08-30 22:14:02	Checking for Malware Permissions	OK
2025-08-30 22:14:02	Fetching icon path	OK
2025-08-30 22:14:03	Library Binary Analysis Started	OK
2025-08-30 22:14:03	Reading Code Signing Certificate	OK
2025-08-30 22:14:03	Running APKiD 2.1.5	OK
2025-08-30 22:14:07	Detecting Trackers	OK
2025-08-30 22:14:09	Decompiling APK to Java with JADX	OK
2025-08-30 22:14:27	Converting DEX to Smali	OK

2025-08-30 22:14:27	Code Analysis Started on - java_source	OK
2025-08-30 22:14:32	Android SBOM Analysis Completed	OK
2025-08-30 22:14:46	Android SAST Completed	OK
2025-08-30 22:14:46	Android API Analysis Started	OK
2025-08-30 22:14:58	Android API Analysis Completed	OK
2025-08-30 22:14:59	Android Permission Mapping Started	OK
2025-08-30 22:15:09	Android Permission Mapping Completed	OK
2025-08-30 22:15:09	Android Behaviour Analysis Started	OK
2025-08-30 22:15:25	Android Behaviour Analysis Completed	OK
2025-08-30 22:15:25	Extracting Emails and URLs from Source Code	OK
2025-08-30 22:15:29	Email and URL Extraction Completed	OK

2025-08-30 22:15:29	Extracting String data from APK	OK
2025-08-30 22:15:29	Extracting String data from Code	OK
2025-08-30 22:15:29	Extracting String values and entropies from Code	OK
2025-08-30 22:15:31	Performing Malware check on extracted domains	OK
2025-08-30 22:15:34	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.