MobSF

ANDROID STATIC ANALYSIS REPORT

app_icon

CoughMonitor (acmc1.8.0(5))

File Name:	172242680.apk
Package Name:	com.hyfe.coughmonitorcompanion
Scan Date:	Aug. 29, 2024, 7:39 a.m.
App Security Score:	57/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	17	2	2	1

FILE INFORMATION

File Name: 172242680.apk
Size: 6.73MB
MD5: 0639c1ed0bda5c39d0dba8e522c5b046
SHA1: aa5ca5cde37e3cc918bc65f8067aea8180c4bb56
SHA256: 37a7ff72a71ef7be7489c375617f9b6e576804eae66370ae72369491fcbc0724

APP INFORMATION

App Name: CoughMonitor
Package Name: com.hyfe.coughmonitorcompanion
Main Activity: com.hyfe.coughmonitorcompanion.MainActivity
Target SDK: 34
Min SDK: 31
Max SDK:
Android Version Name: acmc1.8.0(5)
Android Version Code: 172242680

APP COMPONENTS

Activities: 6
Services: 16
Receivers: 14
Providers: 2
Exported Activities: 2
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: 2024-02-01 09:34:17+00:00
Valid To: 2054-02-01 09:34:17+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xaaec3c6a41fa8e57df9e7a9ba344e1be669d8a51
Hash Algorithm: sha256
md5: db7a36bfe7342bd37314f1df9ab8d4c7
sha1: b9f80f7ec1bfd6ffc210bb40a33bdef7af77c989
sha256: 97e58e9ad70c305cba167b79ada746d0d41cac6a0891f8cb17123efc18440fee
sha512: b704c489f2f1f89cabce4a7e612447a3f3ad8fcc8e348c0bf4452f9b96fbd35658ef8e4a206fc427e064a80c0c7a6574c9c6f1f6dd683f6a4d581e50fc62f789
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 3afea7845f54335f5bf5d76fda2d1626700d83fbddf06e2410f73e7fcf8c084a
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.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.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
no.nordicsemi.android.LOG	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
com.hyfe.coughmonitorcompanion.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<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>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.BRAND check
Build.DEVICE check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
SIM operator check
network operator name check
device ID check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

NETWORK SECURITY

HIGH: **0** | WARNING: **1** | INFO: **0** | SECURE: **0**

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	warning	Base config is configured to trust system certificates.

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: **8** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Activity (com.google.firebase.auth.internal.GenericIdpActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity (com.google.firebase.auth.internal.RecaptchaActivity) 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 (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.

NO	ISSUE	SEVERITY	DESCRIPTION
6	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.
7	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [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.
8	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
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: **0** | WARNING: **6** | INFO: **2** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	d/i.java g8/c4.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	b/b.java b6/e.java g8/f4.java g8/h0.java g8/j.java g8/w3.java h0/f.java h6/n.java ha/f0.java ha/l0.java ha/m0.java ha/o0.java n5/b.java no/nordicsemi/android/log/localprovider/LocalLogDatabaseHelper.java o9/m1.java o9/r0.java r/d0.java r/e.java r/x1.java w6/c.java w6/h.java w6/i.java x6/n.java
				a/m.java a0/f.java a5/b.java a5/d.java a6/f.java ab/e0.java ab/k0.java ab/m0.java ab/n.java ab/o.java ab/q0.java ab/r0.java ab/s0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ab/t0.java ab/y.java b/b.java b0/b.java b5/a.java b6/c.java b6/e.java b6/n.java b7/a.java b7/b.java b9/a.java c3/w.java c5/o.java c5/r.java c6/g.java c6/m.java cb/d.java cb/e.java cb/f.java cb/j.java com/hyfe/coughmonitorcompanion/services/NotificationsService.java d/f.java db/b.java db/d.java e9/c0.java e9/g0.java e9/h0.java e9/l0.java e9/z.java ea/d.java eb/a.java f1/a0.java f9/a0.java f9/f0.java f9/l.java f9/m.java f9/r.java f9/s.java fa/p.java g/c.java g/c0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				g/d0.java g/f.java g/h0.java g/s.java g8/b0.java g8/c4.java g8/j0.java g8/n2.java g9/e.java g9/i.java h/a.java h0/f.java h0/k.java h0/r.java h5/d.java h6/b.java h6/e.java h6/j.java h6/n.java h6/o.java h6/p.java h6/r.java h7/j.java h8/a.java i/h.java i/i.java i1/f2.java i5/c.java i5/c0.java i5/d0.java i5/s.java i5/v.java i5/w.java i5/x.java i9/a.java i9/c.java il/b.java j/o.java j0/a.java j8/a.java j9/b.java j9/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/k.java k/l0.java k/q2.java k/r0.java k/x.java k8/a.java kh/c0.java l8/d.java l8/u.java l9/b.java m7/b.java m7/c.java m7/f.java m7/g.java m7/k.java m7/l.java m7/m.java m7/o.java m7/p.java m9/h.java m9/j.java m9/l.java m9/o.java m9/q.java m9/r.java m9/s.java m9/t.java m9/v.java m9/x.java mf/a.java n4/h.java n4/y.java n5/e.java n7/e.java n7/f.java n7/j.java n7/k.java n7/m.java n7/p.java n7/t.java n7/w.java n9/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				n9/g.java n9/m.java no/nordicsemi/android/ble/BleManagerHandler$4.java no/nordicsemi/android/ble/c0.java no/nordicsemi/android/ble/e0.java no/nordicsemi/android/ble/f.java no/nordicsemi/android/ble/n.java no/nordicsemi/android/ble/y.java no/nordicsemi/android/log/LocalLogSession.java o3/h.java o3/j0.java o5/a.java o9/d0.java o9/m1.java o9/r0.java p3/f.java p3/h.java p4/b.java pl/l.java q2/i0.java q2/p0.java q2/x.java q3/n.java q7/a.java q9/a.java q9/b.java qa/c.java qd/d.java ql/e.java r/f1.java r/q.java r/w.java r/y.java r4/a.java r4/a0.java r4/c0.java r4/e.java r4/g0.java r4/h.java r4/j0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				r4/l.java r4/m0.java r4/p.java r4/s0.java r4/u0.java r4/v.java r4/x.java r9/c.java ra/b.java s4/c.java s5/h.java s5/r.java s9/b.java sa/c.java t5/i0.java t5/l0.java t5/q.java t7/a.java u7/f.java uc/a.java v1/e.java v3/a.java v3/b.java v8/b.java v8/f.java v8/h.java w/c.java w6/c.java w6/i.java w6/k.java w7/a.java wa/a0.java wa/b0.java wa/e.java wa/e0.java wa/g0.java wa/h.java wa/j.java wa/m.java wa/n.java wa/t.java wa/u.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				wa/v.java wa/w.java wa/z.java x/o0.java x/x0.java x5/g.java xl/e.java y/n.java y7/d.java y7/f.java z3/c.java z3/f0.java z3/w0.java z3/y.java zd/l0.java
4	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/e.java db/e.java g8/c4.java hh/a.java hh/b.java ih/a.java ke/k.java nf/d1.java nf/e4.java nf/f1.java nf/v2.java of/n.java q2/i0.java uf/v.java v3/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	b3/p0.java b6/d.java da/h.java ga/a.java i1/i1.java ia/m.java ja/h.java la/f0.java n9/b.java no/nordicsemi/android/log/LogContract.java no/nordicsemi/android/log/localprovider/LocalLogDatabaseHelper.java o9/y0.java of/k.java tc/a1.java
6	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	l8/d.java m9/h.java
7	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	ed/d.java pl/d.java pl/g.java pl/k.java pl/l.java
8	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	m9/h.java q9/b.java ra/b.java u7/c.java
9	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	q2/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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	b6/e.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	x86_64/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	x86_64/libdatastore_shared_counter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	x86/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86/libdatastore_shared_counter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	armeabi-v7a/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	armeabi-v7a/libdatastore_shared_counter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	arm64-v8a/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	arm64-v8a/libdatastore_shared_counter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	x86_64/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	x86_64/libdatastore_shared_counter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	x86/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	x86/libdatastore_shared_counter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	armeabi-v7a/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	armeabi-v7a/libdatastore_shared_counter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	arm64-v8a/libimage_processing_util_jni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__memcpy_chk']	False warning Symbols are available.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	arm64-v8a/libdatastore_shared_counter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	False warning Symbols are available.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	5/24	android.permission.INTERNET, android.permission.CAMERA, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	6/45	android.permission.CHANGE_NETWORK_STATE, com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE, android.permission.BLUETOOTH

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

DOMAIN	STATUS	GEOLOCATION
firebase.google.com	ok	**IP:** 216.58.208.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 216.58.215.66 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.googleadservices.com	ok	**IP:** 216.58.208.194 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
regionconfig.amplitude.com	ok	**IP:** 18.66.233.47 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 216.58.215.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gl	ok	**IP:** 172.217.16.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.eu.amplitude.com	ok	**IP:** 3.74.190.35 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
api2.amplitude.com	ok	**IP:** 54.201.179.200 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
google.com	ok	**IP:** 216.58.215.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.250.186.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
accounts.google.com	ok	**IP:** 64.233.166.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
www.hyfe.ai	ok	**IP:** 63.35.51.142 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.343990 **Longitude:** -6.267190 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
firebase-settings.crashlytics.com	ok	**IP:** 216.58.215.99 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app-measurement.com	ok	**IP:** 142.250.203.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
goo.gle	ok	**IP:** 67.199.248.13 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map
regionconfig.eu.amplitude.com	ok	**IP:** 18.244.146.76 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.google.com	ok	**IP:** 172.217.16.4 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
v2.api.hyfe.ai	ok	**IP:** 18.244.146.84 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.slf4j.org	ok	**IP:** 195.15.222.169 **Country:** Switzerland **Region:** Basel-Stadt **City:** Basel **Latitude:** 47.558399 **Longitude:** 7.573270 **View:** Google Map
firebasestorage.googleapis.com	ok	**IP:** 142.250.186.202 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
hyfe-cmc-gateway-7d4xro8y.uc.gateway.dev	ok	**IP:** 216.239.36.56 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

✉ EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	n7/r.java
support@coughmonitor.com	Android String Resource

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

HARDCODED SECRETS

POSSIBLE SECRETS
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Salasana"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Hasło"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "□□"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Wagwoordsleutel"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Sandi"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Jelszó"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Contrasinal"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Fjalëkalimi"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Pääsuvõti"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "□□□□"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Пароль"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Kod"

POSSIBLE SECRETS
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "□□□"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■ □□■■■■ □■ □■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Лозинка"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Contraseña"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Անցաբառ"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Heslo"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Pasahitza"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Klucz"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Sarbide-gakoa"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Zaporka"

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "گذرواژه"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "گذرکلید"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Գաղտնաբառ"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Wagwoord"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Parole"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Parol"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Парола"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■■■■■■"
"google_api_key" : "AIzaSyCIyT9aNDW7tpTzP15mLEbZWob8nV8FOt0"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "□□□□"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Aðgangsorð"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Slaptažodis"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■"
"com.google.firebase.crashlytics.mapping_file_id" : "48024603a7a244268d27623a3359b26b"

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Toegangssleutel"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Сырсөз"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Iphasiwedi"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Şifre"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Nyckel"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Geslo"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Parolă"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Nenosiri"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "ກະແຈຜ່ານ"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "□□□□□"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Senha"
"google_crash_reporting_api_key" : "AIzaSyCIyT9aNDW7tpTzP15mLEbZWob8nV8FOt0"

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Adgangskode"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Avainkoodi"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Aðgangslykill"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "□□"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Lozinka"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Wachtwoord"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■-■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Parool"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Adgangsnøgle"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "პაროლი"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Tilgangsnøkkel"

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■□■□"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "□□□□"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "□□"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Contrasenya"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "ລະຫັດຜ່ານ"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Azonosítókulcs"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Palavra-passe"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Lösenord"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Passord"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "סיסמה"

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Passwort"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "□□□□"
45b6543cc5f88cc0b236806d8ffc30fd
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
00000006-07ce-44b0-9a00-efba512356e5
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
8D53DC1D-1DB7-4CD3-868B-8A527460AA84
00000009-07ce-44b0-9a00-efba512356e5
DA2E7828-FBCE-4E01-AE9E-261174997C48
115792089210356248762697446949407573530086143415290314195533631308867097853951
6d23b8b05b1094b79aa40a2eb08bab6e
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
af60eb711bd85bc1e4d3e0a462e074eea428a8
0000000a-07ce-44b0-9a00-efba512356e5

POSSIBLE SECRETS
7d73d21f1bd82c9e5268b6dcf9fde2cb
470fa2b4ae81cd56ecbcda9735803434cec591fa
9ae097851d8a3c5ece8898a1d54e6ab0
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
0000000b-07ce-44b0-9a00-efba512356e5
00000002-07CE-44B0-9A00-EFBA512356E5
39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
39402006196394479212279040100143613805079739270465446667948293404245721771496870329047266088258938001861606973112319
a0784d7a4716f3feb4f64e7f4b39bf04
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
3071c8717539de5d5353f4c8cd59a032

POSSIBLE SECRETS
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
00000003-07ce-44b0-9a00-efba512356e5
36864200e0eaf5284d884a0e77d31646
808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
00000008-07ce-44b0-9a00-efba512356e5
115792089210356248762697446949407573529996955224135760342422259061068512044369
00000001-07CE-44B0-9A00-EFBA512356e5
bae8e37fc83441b16034566b

PLAYSTORE INFORMATION

Title: CoughMonitor Companion

Score: 0 **Installs:** 50+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.hyfe.coughmonitorcompanion

Developer Details: Hyfe, 9063262839836886650, 1209 Orange Street Wilmington, Delaware 19801, None, support@coughmonitor.com,

Release Date: Feb 4, 2024 **Privacy Policy:** Privacy link

Description:

The CoughMonitor Companion app pairs seamlessly with a variety of compatible wearables, providing you with continuous and precise cough monitoring. Key Features: - Simple Pairing: Experience hassle-free connectivity with our straightforward pairing process. The app is designed to effortlessly connect with compatible wearable devices, ensuring a smooth and quick setup to start monitoring your cough immediately. - Data Synchronization: Benefit from automatic data synchronization between your wearable and the app. This feature ensures that all your cough data is up-to-date and accurately recorded. - Privacy First: We prioritize your privacy. All data is encrypted and securely stored, ensuring your personal health information remains confidential.

SCAN LOGS

Timestamp	Event	Error
2024-08-29 07:39:00	Generating Hashes	OK
2024-08-29 07:39:00	Extracting APK	OK
2024-08-29 07:39:00	Unzipping	OK
2024-08-29 07:39:01	Getting Hardcoded Certificates/Keystores	OK
2024-08-29 07:39:05	Parsing AndroidManifest.xml	OK
2024-08-29 07:39:05	Parsing APK with androguard	OK
2024-08-29 07:39:06	Extracting Manifest Data	OK
2024-08-29 07:39:06	Performing Static Analysis on: CoughMonitor (com.hyfe.coughmonitorcompanion)	OK

2024-08-29 07:39:06	Fetching Details from Play Store: com.hyfe.coughmonitorcompanion	OK
2024-08-29 07:39:06	Manifest Analysis Started	OK
2024-08-29 07:39:06	Reading Network Security config from network_security_config.xml	OK
2024-08-29 07:39:06	Parsing Network Security config	OK
2024-08-29 07:39:06	Checking for Malware Permissions	OK
2024-08-29 07:39:06	Fetching icon path	OK
2024-08-29 07:39:07	Library Binary Analysis Started	OK
2024-08-29 07:39:07	Analyzing lib/x86_64/libimage_processing_util_jni.so	OK
2024-08-29 07:39:07	Analyzing lib/x86_64/libdatastore_shared_counter.so	OK
2024-08-29 07:39:07	Analyzing lib/x86/libimage_processing_util_jni.so	OK
2024-08-29 07:39:07	Analyzing lib/x86/libdatastore_shared_counter.so	OK

2024-08-29 07:39:07	Analyzing lib/armeabi-v7a/libimage_processing_util_jni.so	OK
2024-08-29 07:39:08	Analyzing lib/armeabi-v7a/libdatastore_shared_counter.so	OK
2024-08-29 07:39:08	Analyzing lib/arm64-v8a/libimage_processing_util_jni.so	OK
2024-08-29 07:39:08	Analyzing lib/arm64-v8a/libdatastore_shared_counter.so	OK
2024-08-29 07:39:08	Analyzing apktool_out/lib/x86_64/libimage_processing_util_jni.so	OK
2024-08-29 07:39:08	Analyzing apktool_out/lib/x86_64/libdatastore_shared_counter.so	OK
2024-08-29 07:39:08	Analyzing apktool_out/lib/x86/libimage_processing_util_jni.so	OK
2024-08-29 07:39:08	Analyzing apktool_out/lib/x86/libdatastore_shared_counter.so	OK
2024-08-29 07:39:08	Analyzing apktool_out/lib/armeabi-v7a/libimage_processing_util_jni.so	OK
2024-08-29 07:39:08	Analyzing apktool_out/lib/armeabi-v7a/libdatastore_shared_counter.so	OK
2024-08-29 07:39:08	Analyzing apktool_out/lib/arm64-v8a/libimage_processing_util_jni.so	OK

2024-08-29 07:39:08	Analyzing apktool_out/lib/arm64-v8a/libdatastore_shared_counter.so	OK
2024-08-29 07:39:08	Reading Code Signing Certificate	OK
2024-08-29 07:39:08	Running APKiD 2.1.5	OK
2024-08-29 07:39:09	Updating Trackers Database....	OK
2024-08-29 07:39:09	Detecting Trackers	OK
2024-08-29 07:39:12	Decompiling APK to Java with jadx	OK
2024-08-29 07:39:59	Converting DEX to Smali	OK
2024-08-29 07:39:59	Code Analysis Started on - java_source	OK
2024-08-29 07:40:48	Android SAST Completed	OK
2024-08-29 07:40:49	Android API Analysis Started	OK
2024-08-29 07:41:31	Android Permission Mapping Started	OK

2024-08-29 07:41:54	Android Permission Mapping Completed	OK
2024-08-29 07:41:58	Finished Code Analysis, Email and URL Extraction	OK
2024-08-29 07:41:58	Extracting String data from APK	OK
2024-08-29 07:41:59	Extracting String data from SO	OK
2024-08-29 07:41:59	Extracting String data from Code	OK
2024-08-29 07:41:59	Extracting String values and entropies from Code	OK
2024-08-29 07:42:01	Performing Malware check on extracted domains	OK
2024-08-29 07:42:04	Saving to Database	OK

Report Generated by - MobSF v4.0.7

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.