MOBSF

ANDROID STATIC ANALYSIS REPORT

healow (7.3.0)

File Name:	com.ecw.healow_20240828.apk
Package Name:	com.ecw.healow
Scan Date:	Aug. 29, 2025, 9:59 p.m.
App Security Score:	49/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	16	2	2	1

FILE INFORMATION

File Name: com.ecw.healow_20240828.apk
Size: 95.98MB
MD5: 608346c9ac6a7146ffe3afa419d6c0bc
SHA1: 042c94cdb38050f249029a1c99f9a2f8843f6106
SHA256: ea0408dfd68d6aef0277049ccecd706381e9b90408a027855c9099ab1704711a

APP INFORMATION

App Name: healow
Package Name: com.ecw.healow
Main Activity: com.ecw.healow.MainActivity
Target SDK: 33
Min SDK: 21
Max SDK:
Android Version Name: 7.3.0
Android Version Code: 20240828

APP COMPONENTS

Activities: 148
Services: 16
Receivers: 15
Providers: 3
Exported Activities: 0
Exported Services: 4
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=01, ST=MA, L=Westborough, O=eClinicalWorks, OU=Healow, CN=Hemraj Gharia
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-03-07 07:07:24+00:00
Valid To: 2040-07-23 07:07:24+00:00
Issuer: C=01, ST=MA, L=Westborough, O=eClinicalWorks, OU=Healow, CN=Hemraj Gharia
Serial Number: 0x51383cac
Hash Algorithm: sha1
md5: acecbe03de67bdbd37b65156b2c27044
sha1: 0da3e0b2565634bc86323a9d34b54e8defb860af
sha256: d6a7bc922fb2e7139915e934ebbadf3683c525cbc44f9def115a70faa5770287
sha512: fe647839beeebf387705dc79df139ceb43d8c4b24e2711e07a3ee55a567d5e47ed0226ce38f7de50b8745721d9acf96f54ee06030bdbb42b8933b097bef15eb0
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 7ac48864a104eb29b5c73ce401f083e8c25470c76d3fc7ee7592f36ae082e54a
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.READ_CALENDAR	dangerous	read calendar events	Allows an application to read all of the calendar events stored on your phone. Malicious applications can use this to send your calendar events to other people.
android.permission.WRITE_CALENDAR	dangerous	add or modify calendar events and send emails to guests	Allows an application to add or change the events on your calendar, which may send emails to guests. Malicious applications can use this to erase or modify your calendar events or to send emails to guests.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

PERMISSION	STATUS	INFO	DESCRIPTION
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.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
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.DISABLE_KEYGUARD	normal	disable keyguard	Allows applications to disable the keyguard if it is not secure.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.USE_FULL_SCREEN_INTENT	normal	required for full screen intents in notifications.	Required for apps targeting Build.VERSION_CODES.Q that want to use notification full screen intents.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.SCHEDULE_EXACT_ALARM	normal	permits exact alarm scheduling for background work.	Allows an app to use exact alarm scheduling APIs to perform timing sensitive background work.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

APKID ANALYSIS

FILE	DETAILS
classes3.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check Build.BOARD check possible VM check FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)
classes2.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check Build.TAGS check FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)
classes4.dex	FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.ecw.healow.MainActivity	Schemes: @string/app_url_scheme://, https://, Hosts: msg.fm, msgtests.com, healow.co, cqaurl.ecwlab.com, Path Prefixes: /hpc,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 2 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 6 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Service (com.ecw.healow.utilities.FcmMessageService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
3	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.
4	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Service (com.google.android.play.core.assetpacks.AssetPackExtractionService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	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.
7	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.

</> CODE ANALYSIS

HIGH: **2** | WARNING: **6** | INFO: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/Glide.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/load/data/AssetPathFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/engine/GlideException.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/engine/prefill/BitmapPreFillRunner.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/model/StreamEncoder.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	com/bumptech/glide/load/resource/DefaultOnHeaderDecodedListener.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/manager/RequestManagerRetriever.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/manager/SingletonConnectivityReceiver.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/module/ManifestParser.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/request/target/CustomViewTarget.java com/bumptech/glide/request/target/ViewTarget.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				et.java com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/ecw/healow/HealowApplication.java com/ecw/healow/MainActivity.java com/ecw/healow/UpdateScript600.java com/ecw/healow/authentication/AuthenticationServerLogger.java com/ecw/healow/crypto/PRNGFixes.java com/ecw/healow/modules/h2h/CallDetailsActivity.java com/ecw/healow/modules/h2h/CustomAudioDevice.java com/ecw/healow/modules/h2h/GLTextureView.java com/ecw/healow/modules/h2h/H2HLogs.java com/ecw/healow/modules/plus/data/PubNubChat.java com/ecw/healow/modules/records/MyRecordsActivityNew2.java com/ecw/healow/modules/televisit/QuestionnaireActivity.java com/ecw/healow/modules/televisit/TelevisitCallActivity.java com/ecw/healow/modules/televisit/fragment/ChatFragment.java com/ecw/healow/modules/televisit/fragment/PublisherControlFragment.java com/ecw/healow/network/core/AppApiLogger.java com/ecw/healow/network/core/H2HApiLogger.java com/ecw/healow/utilities/CommonUtilities.java com/ecw/healow/utilities/LocationHelper.java com/ecw/healow/utilities/sqlitedb/HealowDB.java com/opentok/android/BaseVideoCapturer.java com/opentok/android/OtLog.java com/opentok/android/PublisherKit.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/openTok/android/PublisherKit.java com/readystatesoftware/sqliteasset/SQLiteAssetHelper.java com/readystatesoftware/sqliteasset/Utils.java com/readystatesoftware/sqliteasset/VersionComparator.java com/vonage/mltransformers/CameraXVideoCapturer.java com/vonage/mltransformers/MediapipeVideoFrameProcessor.java eu/janmuller/android/simplecropimage/BitmapManager.java eu/janmuller/android/simplecropimage/CropImage.java org/joda/time/tz/DateTimeZoneBuilder.java org/joda/time/tz/ZoneInfoCompiler.java org/mozilla/classfile/TypeInfo.java org/mozilla/javascript/Interpreter.java org/mozilla/javascript/ScriptRuntime.java org/mozilla/javascript/tools/debugger/Dim.java org/mozilla/javascript/tools/idswitch/Main.java org/mozilla/javascript/tools/jsc/Main.java org/slf4j/helpers/Util.java
2	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/ecw/healow/utils/AndroidUtils.java eu/janmuller/android/simplecropimage/CropImage.java
3	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/ecw/healow/utilities/HealowPreferences.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	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	com/opentok/android/DefaultAudioDevice.java org/jsoup/helper/W3CDom.java org/jsoup/nodes/DocumentType.java org/mozilla/javascript/ClassCache.java org/mozilla/javascript/NativeError.java org/mozilla/javascript/NativeJavaObject.java org/mozilla/javascript/ScriptRuntime.java org/mozilla/javascript/xmlimpl/XmlNode.java
5	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	com/readystatesoftware/sqliteasset/SQLiteAssetHelper.java org/mozilla/javascript/tools/shell/Main.java
6	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	org/mozilla/javascript/tools/debugger/Dim.java
7	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/ecw/healow/network/core/VerifyCertificateUseCase.java
8	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	com/ecw/healow/authentication/PatientActivity.java com/ecw/healow/utilities/CommonUtilities.java com/pubnub/api/vendor/Crypto.java org/jsoup/helper/DataUtil.java
9	Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	com/ecw/healow/utilities/WebViewHealowClient.java com/ecw/healow/utilities/WebViewHealowClientForVendor.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	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	com/ecw/healow/utilities/sqlitedb/HealowDB.java com/readystatesoftware/sqliteasset/SQLiteAssetHelper.java

SHARED LIBRARY BINARY ANALYSIS

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libhealow.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	arm64-v8a/libopentok.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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', '__strlen_chk', '__memset_chk', '__vsnprintf_chk', '__memmove_chk', '__strncpy_chk', '__read_chk', '__memchr_chk', '__strchr_chk', '__strrchr_chk', '__strcpy_chk', '__strcat_chk', '__strncat_chk', '__fgets_chk', '__vsprintf_chk', '__pread_chk', '__readlink_chk', '__poll_chk', '__umask_chk', '__FD_SET_chk', '__FD_ISSET_chk', '__FD_CLR_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	arm64-v8a/libiyhsarlxvqkf.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86_64/libhealow.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__memmove_chk', '__strlen_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	x86_64/libopentok.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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', '__strlen_chk', '__memset_chk', '__vsnprintf_chk', '__memmove_chk', '__strncpy_chk', '__read_chk', '__memchr_chk', '__strchr_chk', '__strrchr_chk', '__strcpy_chk', '__strcat_chk', '__strncat_chk', '__fgets_chk', '__vsprintf_chk', '__pread_chk', '__readlink_chk', '__poll_chk', '__umask_chk', '__FD_SET_chk', '__FD_ISSET_chk', '__FD_CLR_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	x86_64/libiyhsarlxvqkf.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	armeabi-v7a/libhealow.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	armeabi-v7a/libopentok.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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', '__strlen_chk', '__memset_chk', '__vsnprintf_chk', '__memmove_chk', '__strncpy_chk', '__read_chk', '__memchr_chk', '__strchr_chk', '__strrchr_chk', '__strcpy_chk', '__strcat_chk', '__strncat_chk', '__fgets_chk', '__vsprintf_chk', '__readlink_chk', '__poll_chk', '__umask_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	armeabi-v7a/libiyhsarlxvqkf.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__strlen_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	x86/libhealow.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	x86/libopentok.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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', '__strlen_chk', '__memset_chk', '__vsnprintf_chk', '__memmove_chk', '__strncpy_chk', '__read_chk', '__memchr_chk', '__strchr_chk', '__strrchr_chk', '__strcpy_chk', '__strcat_chk', '__strncat_chk', '__fgets_chk', '__vsprintf_chk', '__readlink_chk', '__poll_chk', '__umask_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	x86/libiyhsarlxvqkf.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	arm64-v8a/libhealow.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__vsnprintf_chk', '__strlen_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	arm64-v8a/libopentok.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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', '__strlen_chk', '__memset_chk', '__vsnprintf_chk', '__memmove_chk', '__strncpy_chk', '__read_chk', '__memchr_chk', '__strchr_chk', '__strrchr_chk', '__strcpy_chk', '__strcat_chk', '__strncat_chk', '__fgets_chk', '__vsprintf_chk', '__pread_chk', '__readlink_chk', '__poll_chk', '__umask_chk', '__FD_SET_chk', '__FD_ISSET_chk', '__FD_CLR_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	arm64-v8a/libiyhsarlxvqkf.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	x86_64/libhealow.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__memmove_chk', '__strlen_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	x86_64/libopentok.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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', '__strlen_chk', '__memset_chk', '__vsnprintf_chk', '__memmove_chk', '__strncpy_chk', '__read_chk', '__memchr_chk', '__strchr_chk', '__strrchr_chk', '__strcpy_chk', '__strcat_chk', '__strncat_chk', '__fgets_chk', '__vsprintf_chk', '__pread_chk', '__readlink_chk', '__poll_chk', '__umask_chk', '__FD_SET_chk', '__FD_ISSET_chk', '__FD_CLR_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	x86_64/libiyhsarlxvqkf.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	armeabi-v7a/libhealow.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	armeabi-v7a/libopentok.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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', '__strlen_chk', '__memset_chk', '__vsnprintf_chk', '__memmove_chk', '__strncpy_chk', '__read_chk', '__memchr_chk', '__strchr_chk', '__strrchr_chk', '__strcpy_chk', '__strcat_chk', '__strncat_chk', '__fgets_chk', '__vsprintf_chk', '__readlink_chk', '__poll_chk', '__umask_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	armeabi-v7a/libiyhsarlxvqkf.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__strlen_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	x86/libhealow.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	x86/libopentok.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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', '__strlen_chk', '__memset_chk', '__vsnprintf_chk', '__memmove_chk', '__strncpy_chk', '__read_chk', '__memchr_chk', '__strchr_chk', '__strrchr_chk', '__strcpy_chk', '__strcat_chk', '__strncat_chk', '__fgets_chk', '__vsprintf_chk', '__readlink_chk', '__poll_chk', '__umask_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	x86/libiyhsarlxvqkf.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	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: ['__strlen_chk', '__memmove_chk', '__vsnprintf_chk']	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/ecw/healow/MainActivity.java com/ecw/healow/authentication/fragments/PracticeSearchMapActivity.java com/ecw/healow/modules/appointments/MapHelper.java com/ecw/healow/modules/appointments/MyAppointmentsMapActivity.java com/ecw/healow/modules/h2h/H2HCallActivity.java com/ecw/healow/modules/medication/MedicationsEditActivity.java com/ecw/healow/modules/messages/MessageDetailActivity.java com/ecw/healow/modules/messages/MessageReplyActivity.java com/ecw/healow/modules/messages/NewMessageActivity.java com/ecw/healow/modules/plus/chatdetail/ChatDetailActivity.java com/ecw/healow/modules/plus/chatdetail/adapter/AbstractHtmlMessageRecyclerViewViewHolder.java com/ecw/healow/utilities/CommonUtilities.java com/ecw/healow/utilities/PermissionUtils.java com/ecw/healow/utilities/WebViewHealowClient.java com/ecw/healow/utilities/WebViewHealowClientForVendor.java com/ecw/healow/utilities/superactivities/MapActivityWithCustomTitle.java com/ecw/healow/utils/AndroidUtils.java com/ecw/healow/utils/CustomInfoWindowForMap.java com/ecw/healow/utils/IntentUtils.java com/ecw/healow/views/SimpleWebViewActivity.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/ecw/healow/utilities/CommonUtilities.java com/ecw/healow/utilities/WebViewHealowClient.java com/ecw/healow/utilities/WebViewHealowClientForVendor.java com/ecw/healow/utils/AndroidUtils.java com/ecw/healow/utils/IntentUtils.java
00036	Get resource file from res/raw directory	reflection	com/ecw/healow/modules/h2h/H2HCallActivity.java com/ecw/healow/utilities/CommonUtilities.java com/ecw/healow/utils/AndroidUtils.java com/ecw/healow/utils/IntentUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/ecw/healow/MainActivity.java com/ecw/healow/authentication/InitialSetupWizard.java com/ecw/healow/authentication/PINActivity.java com/ecw/healow/modules/appointments/AppointmentPastActivity.java com/ecw/healow/modules/appointments/AppointmentUpcomingActivity.java com/ecw/healow/modules/appointments/CancelAppointmentActivity.java com/ecw/healow/modules/appointments/MyAppointmentDetail.java com/ecw/healow/modules/appointments/MyAppointmentsMapActivity.java com/ecw/healow/modules/medication/MedicationsAddNewActivity.java com/ecw/healow/modules/openaccess/OaPhoneNoVerificationActvity.java com/ecw/healow/modules/televisit/QuestionnaireActivity.java eu/janmuller/android/simplecropimage/CropImage.java
00112	Get the date of the calendar event	collection calendar	com/ecw/healow/modules/openaccess/OaAppointmentBookRequestActivity.java com/ecw/healow/trackers/activity/EditActivityDialogFragment.java com/ecw/healow/trackers/bloodpressure/EditBloodPressureDialogFragment.java com/ecw/healow/trackers/bloodsugar/EditBloodSugarDialogFragment.java com/ecw/healow/trackers/bmi/EditBmiDialogFragment.java com/ecw/healow/trackers/calories/EditCalorieDialogFragment.java com/ecw/healow/trackers/distance/EditDistanceDialogFragment.java com/ecw/healow/trackers/floors/EditFloorDialogFragment.java com/ecw/healow/trackers/heartrate/EditHeartRateDialogFragment.java com/ecw/healow/trackers/sleep/EditSleepDialogFragment.java com/ecw/healow/trackers/spo2/EditSpO2DialogFragment.java com/ecw/healow/trackers/steps/EditStepDialogFragment.java com/ecw/healow/trackers/temperature/EditTemperatureDialogFragment.java com/ecw/healow/utilities/DateHelper.java com/ecw/healow/utilities/ProviderProfileRecycleAdapter.java com/ecw/healow/utilities/sqlitedb/HealowDB.java com/ecw/healow/utils/CalendarUtils.java com/fasterxml/jackson/databind/ser/std/StdKeySerializers.java com/fasterxml/jackson/databind/util/StdDateFormat.java
00121	Create a directory	file command	com/ecw/healow/utils/AndroidUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00125	Check if the given file path exist	file	com/ecw/healow/utils/AndroidUtils.java com/ecw/healow/views/SimpleWebViewActivity.java
00191	Get messages in the SMS inbox	sms	com/ecw/healow/utils/AndroidUtils.java com/ecw/healow/utils/ContentResolverUtils.java
00104	Check if the given path is directory	file	com/ecw/healow/utils/AndroidUtils.java
00013	Read file and put it into a stream	file	com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/load/ImageHeaderParserUtils.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/resource/bitmap/ImageReader.java com/ecw/healow/crypto/PRNGFixes.java com/ecw/healow/modules/h2h/SettingH2HApiLogDetail.java com/ecw/healow/network/core/HttpUrlConnectionHelper.java com/fasterxml/jackson/core/JsonFactory.java com/fasterxml/jackson/core/TokenStreamFactory.java com/fasterxml/jackson/databind/ObjectReader.java com/fasterxml/jackson/dataformat/cbor/CBORFactory.java okio/Okio.java org/joda/time/tz/ZoneInfoCompiler.java org/joda/time/tz/ZoneInfoProvider.java org/jsoup/helper/DataUtil.java org/mozilla/javascript/tools/SourceReader.java org/mozilla/javascript/tools/debugger/Dim.java org/mozilla/javascript/tools/idswitch/Main.java org/mozilla/javascript/tools/shell/Global.java
00056	Modify voice volume	control	com/vonage/webrtc/audio/WebRtcAudioTrack.java com/vonage/webrtc/voiceengine/WebRtcAudioTrack.java com/vonage/webrtc/voiceengine61/WebRtcAudioTrack.java

RULE ID	BEHAVIOUR	LABEL	FILES
00054	Install other APKs from file	reflection	com/ecw/healow/modules/messages/MessageThreadListAdapter.java com/ecw/healow/modules/myrecords/adpater/DocumentsAdapter.java com/ecw/healow/modules/plus/chatdetail/adapter/AbstractPDFAttachmentRecyclerView ViewHolder.java
00009	Put data in cursor to JSON object	file	com/ecw/healow/MainActivity.java com/ecw/healow/pojo/rating/RatingsPayload.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/ecw/healow/network/core/HttpUrlConnectionHelper.java com/pubnub/api/endpoints/vendor/AppEngineFactory.java kd/C0116kI.java org/jsoup/helper/HttpConnection.java org/mozilla/javascript/commonjs/module/provider/UrlModuleSourceProvider.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/ecw/healow/MainActivity.java com/pubnub/api/endpoints/vendor/AppEngineFactory.java org/jsoup/helper/HttpConnection.java org/mozilla/javascript/commonjs/module/provider/UrlModuleSourceProvider.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java com/ecw/healow/MainActivity.java com/ecw/healow/authentication/AddOREditEnvActivity.java com/ecw/healow/network/core/HttpUrlConnectionHelper.java com/pubnub/api/endpoints/vendor/AppEngineFactory.java kd/C0116kI.java org/jsoup/helper/HttpConnection.java org/mozilla/javascript/commonjs/module/provider/UrlModuleSourceProvider.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/ecw/healow/modules/medication/MedicationsEditActivity.java com/ecw/healow/modules/medication/MedicationsListAdapter.java com/ecw/healow/settings/ProfileImageUpdateDialogFragment.java com/ecw/healow/utilities/CommonUtilities.java com/fasterxml/jackson/databind/ser/std/FileSerializer.java kd/BH.java kd/VH.java kd/ZI.java org/jsoup/Jsoup.java org/mozilla/javascript/tools/jsc/Main.java
00015	Put buffer stream (data) to JSON object	file	kd/C0116kI.java
00096	Connect to a URL and set request method	command network	com/ecw/healow/network/core/HttpUrlConnectionHelper.java com/pubnub/api/endpoints/vendor/AppEngineFactory.java kd/C0116kI.java org/jsoup/helper/HttpConnection.java
00094	Connect to a URL and read data from it	command network	com/ecw/healow/network/core/HttpUrlConnectionHelper.java kd/C0116kI.java org/mozilla/javascript/tools/shell/Global.java
00108	Read the input stream from given URL	network command	com/ecw/healow/network/core/HttpUrlConnectionHelper.java kd/C0116kI.java
00183	Get current camera parameters and change the setting.	camera	com/vonage/webrtc/Camera1Session.java
00004	Get filename and put it to JSON object	file collection	com/ecw/healow/views/SimpleWebViewActivity.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/ecw/healow/utils/ContentResolverUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00028	Read file from assets directory	file	com/ecw/healow/modules/h2h/CountryCodeSelectionActivity.java com/opentok/android/PublisherKit.java
00102	Set the phone speaker on	command	com/ecw/healow/modules/h2h/CustomAudioDevice.java com/ecw/healow/modules/h2h/H2HAudioManager.java com/opentok/android/DefaultAudioDevice.java
00189	Get the content of a SMS message	sms	com/ecw/healow/utils/ContentResolverUtils.java
00188	Get the address of a SMS message	sms	com/ecw/healow/utils/ContentResolverUtils.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	com/ecw/healow/utils/ContentResolverUtils.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/ecw/healow/utils/ContentResolverUtils.java
00200	Query data from the contact list	collection contact	com/ecw/healow/utils/ContentResolverUtils.java
00187	Query a URI and check the result	collection sms calllog calendar	com/ecw/healow/utils/ContentResolverUtils.java
00201	Query data from the call log	collection calllog	com/ecw/healow/utils/ContentResolverUtils.java
00208	Capture the contents of the device screen	collection screen	com/vonage/webrtc/ScreenCapturerAndroid.java
00012	Read data and put it into a buffer stream	file	com/ecw/healow/network/core/HttpUrlConnectionHelper.java
00153	Send binary data over HTTP	http	com/ecw/healow/network/core/HttpUrlConnectionHelper.java

RULE ID	BEHAVIOUR	LABEL	FILES
00123	Save the response to JSON after connecting to the remote server	network command	com/ecw/healow/MainActivity.java
00147	Get the time of current location	collection location	com/ecw/healow/utilities/CommonUtilities.java
00024	Write file after Base64 decoding	reflection file	com/ecw/healow/utilities/CommonUtilities.java
00001	Initialize bitmap object and compress data (e.g. JPEG) into bitmap object	camera	com/ecw/healow/utilities/CommonUtilities.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://eternal-argon-838.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/1012690656550/namespaces/firebase:fetch?key=AIzaSyC2ZLwtnv5xXZdO1fdVUa7pjdJlhzwwBKc. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	11/25	android.permission.WAKE_LOCK, android.permission.INTERNET, android.permission.ACCESS_FINE_LOCATION, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.RECORD_AUDIO, android.permission.ACCESS_COARSE_LOCATION, android.permission.CAMERA, android.permission.READ_PHONE_STATE
Other Common Permissions	6/44	android.permission.READ_CALENDAR, android.permission.MODIFY_AUDIO_SETTINGS, android.permission.BLUETOOTH, com.google.android.c2dm.permission.RECEIVE, android.permission.FOREGROUND_SERVICE, 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

DOMAIN	STATUS	GEOLOCATION
api.opentok.com	ok	**IP:** 168.100.106.197 **Country:** United States of America **Region:** New Jersey **City:** Holmdel **Latitude:** 40.383961 **Longitude:** -74.170563 **View:** Google Map
yourp2pservername.com	ok	No Geolocation information available.
www.tensorflow.org	ok	**IP:** 64.233.176.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.tokbox.com	ok	**IP:** 168.100.113.249 **Country:** United States of America **Region:** New Jersey **City:** Holmdel **Latitude:** 40.383961 **Longitude:** -74.170563 **View:** Google Map
test.healow.com	ok	**IP:** 23.98.138.20 **Country:** United States of America **Region:** Texas **City:** San Antonio **Latitude:** 29.424120 **Longitude:** -98.493629 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
crbug.com	ok	**IP:** 216.239.32.29 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.112.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.ietf.org	ok	**IP:** 104.16.45.99 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
yourhealowchatservername.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
app.healow.com	ok	**IP:** 20.121.85.115 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
www.slf4j.org	ok	**IP:** 159.100.250.151 **Country:** Switzerland **Region:** Vaud **City:** Lausanne **Latitude:** 46.515999 **Longitude:** 6.632820 **View:** Google Map
myservername.healow.com	ok	No Geolocation information available.
127.0.0.1	ok	**IP:** 127.0.0.1 **Country:** - **Region:** - **City:** - **Latitude:** 0.000000 **Longitude:** 0.000000 **View:** Google Map
eternal-argon-838.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
config.opentok.com	ok	**IP:** 18.238.109.37 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
yourshealowservername.com	ok	No Geolocation information available.
www.webrtc.org	ok	**IP:** 64.233.176.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
chat.eclinicalworks.com	ok	No Geolocation information available.
config-enterprise.opentok.com	ok	**IP:** 168.100.106.108 **Country:** United States of America **Region:** New Jersey **City:** Holmdel **Latitude:** 40.383961 **Longitude:** -74.170563 **View:** Google Map
developers.google.com	ok	**IP:** 172.217.215.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
aomediacodec.github.io	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

EMAILS

EMAIL	FILE
0@a5.39	com/ecw/healow/modules/plus/chatdetail/GroupDetailActivity.java
ce@bk6b.71	com/ecw/healow/network/helper/apihelper/OpenAccessApiHelper.java
7co@c.8402	com/ecw/healow/pojo/openaccess/AvailableAppointmentResponse.java
u001f@ne.qz	com/bumptech/glide/request/SingleRequest.java
n@e.bl2	com/vonage/webrtc/voiceengine/WebRtcAudioUtils.java
d@66.i4	com/fasterxml/jackson/databind/util/ISO8601Utils.java
u001a@8.i1	com/fasterxml/jackson/databind/type/SimpleType.java
abs@email.com abc@xyzmail.com	Android String Resource
appro@openssl.org	lib/arm64-v8a/libopentok.so

EMAIL	FILE
appro@openssl.org	apktool_out/lib/arm64-v8a/libopentok.so

TRACKERS

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

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://eternal-argon-838.firebaseio.com"
"user" : "User"
"google_crash_reporting_api_key" : "AIzaSyC2ZLwtnv5xXZdO1fdVUa7pjdJlhzwwBKc"
"map_api_key" : "AIzaSyBJ66jDB8pv29kCVdSLA5_8MgwaQm0Hi7E"
"user" : "Usuario"
"google_api_key" : "AIzaSyC2ZLwtnv5xXZdO1fdVUa7pjdJlhzwwBKc"
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
c103703e120ae8cc73c9248622f3cd1e

POSSIBLE SECRETS
49f946663a8deb7054212b8adda248c6
71f8cf7d83deae7b38191cd22946d47b54d59471

PLAYSTORE INFORMATION

Title: healow

Score: 4.6072445 **Installs:** 5,000,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.ecw.healow

Developer Details: eClinicalWorks LLC, 8033512383076013922, None, https://healow.com, help@healow.com,

Release Date: Mar 12, 2013 **Privacy Policy:** Privacy link

Description:

Healow App is a convenient mobile tool that helps patients access health information and communicate with their providers to stay engaged, motivated, and make healthy choices. With the healow app, patients can easily: Message the care team – Contact care team through quick, secure direct messages. View test results – Access labs and other test results as soon as they become available. Self-schedule appointments – Book appointments with the care team and view upcoming visits beyond regular office hours. Check in before the visit – Easily check in for appointments and save time by completing any necessary documentation before arrival. Attend virtual visits –Initiate and attend telehealth visits with members of the care team. View medications, set medication reminders, and request for refills without calling the doctor. View medical history including allergies, immunizations, vitals, visit summary, and other health information. Monitor vitals and meet health goals using weight management, activity, fitness, and sleeping tracking tools to track readings and watch for trend changes to share with the doctor. Manage and view multiple family member's health records under one account. Please note that patients must have an existing healow Patient Portal account with their doctor's office. Once downloaded and launched, the patient must log in using the username and password used to access the provider's healow Patient Portal website to begin using the app. It will ask the user to create a pin and enable Face ID or Touch ID. Enabling either of these features will save the user from having to enter their login information every time they want to use the app.

SCAN LOGS

Timestamp	Event	Error
2025-08-29 21:59:26	Generating Hashes	OK

2025-08-29 21:59:27	Extracting APK	OK
2025-08-29 21:59:27	Unzipping	OK
2025-08-29 21:59:29	Parsing APK with androguard	OK
2025-08-29 21:59:29	Extracting APK features using aapt/aapt2	OK
2025-08-29 21:59:30	Getting Hardcoded Certificates/Keystores	OK
2025-08-29 21:59:35	Parsing AndroidManifest.xml	OK
2025-08-29 21:59:35	Extracting Manifest Data	OK
2025-08-29 21:59:35	Manifest Analysis Started	OK
2025-08-29 21:59:35	Performing Static Analysis on: healow (com.ecw.healow)	OK
2025-08-29 21:59:36	Fetching Details from Play Store: com.ecw.healow	OK
2025-08-29 21:59:36	Checking for Malware Permissions	OK

2025-08-29 21:59:36	Fetching icon path	OK
2025-08-29 21:59:36	Library Binary Analysis Started	OK
2025-08-29 21:59:36	Analyzing lib/arm64-v8a/libhealow.so	OK
2025-08-29 21:59:36	Analyzing lib/arm64-v8a/libopentok.so	OK
2025-08-29 21:59:37	Analyzing lib/arm64-v8a/libiyhsarlxvqkf.so	OK
2025-08-29 21:59:37	Analyzing lib/x86_64/libhealow.so	OK
2025-08-29 21:59:37	Analyzing lib/x86_64/libopentok.so	OK
2025-08-29 21:59:37	Analyzing lib/x86_64/libiyhsarlxvqkf.so	OK
2025-08-29 21:59:37	Analyzing lib/armeabi-v7a/libhealow.so	OK
2025-08-29 21:59:37	Analyzing lib/armeabi-v7a/libopentok.so	OK
2025-08-29 21:59:38	Analyzing lib/armeabi-v7a/libiyhsarlxvqkf.so	OK

2025-08-29 21:59:38	Analyzing lib/x86/libhealow.so	OK
2025-08-29 21:59:38	Analyzing lib/x86/libopentok.so	OK
2025-08-29 21:59:38	Analyzing lib/x86/libiyhsarlxvqkf.so	OK
2025-08-29 21:59:38	Analyzing apktool_out/lib/arm64-v8a/libhealow.so	OK
2025-08-29 21:59:38	Analyzing apktool_out/lib/arm64-v8a/libopentok.so	OK
2025-08-29 21:59:38	Analyzing apktool_out/lib/arm64-v8a/libiyhsarlxvqkf.so	OK
2025-08-29 21:59:38	Analyzing apktool_out/lib/x86_64/libhealow.so	OK
2025-08-29 21:59:38	Analyzing apktool_out/lib/x86_64/libopentok.so	OK
2025-08-29 21:59:39	Analyzing apktool_out/lib/x86_64/libiyhsarlxvqkf.so	OK
2025-08-29 21:59:39	Analyzing apktool_out/lib/armeabi-v7a/libhealow.so	OK
2025-08-29 21:59:39	Analyzing apktool_out/lib/armeabi-v7a/libopentok.so	OK

2025-08-29 21:59:39	Analyzing apktool_out/lib/armeabi-v7a/libiyhsarlxvqkf.so	OK
2025-08-29 21:59:39	Analyzing apktool_out/lib/x86/libhealow.so	OK
2025-08-29 21:59:39	Analyzing apktool_out/lib/x86/libopentok.so	OK
2025-08-29 21:59:40	Analyzing apktool_out/lib/x86/libiyhsarlxvqkf.so	OK
2025-08-29 21:59:40	Reading Code Signing Certificate	OK
2025-08-29 21:59:42	Running APKiD 2.1.5	OK
2025-08-29 21:59:51	Detecting Trackers	OK
2025-08-29 21:59:55	Decompiling APK to Java with JADX	OK
2025-08-29 22:00:17	Converting DEX to Smali	OK
2025-08-29 22:00:17	Code Analysis Started on - java_source	OK
2025-08-29 22:00:20	Android SBOM Analysis Completed	OK

2025-08-29 22:00:29	Android SAST Completed	OK
2025-08-29 22:00:29	Android API Analysis Started	OK
2025-08-29 22:00:36	Android API Analysis Completed	OK
2025-08-29 22:00:37	Android Permission Mapping Started	OK
2025-08-29 22:00:46	Android Permission Mapping Completed	OK
2025-08-29 22:00:46	Android Behaviour Analysis Started	OK
2025-08-29 22:00:55	Android Behaviour Analysis Completed	OK
2025-08-29 22:00:55	Extracting Emails and URLs from Source Code	OK
2025-08-29 22:01:01	Email and URL Extraction Completed	OK
2025-08-29 22:01:01	Extracting String data from APK	OK
2025-08-29 22:01:02	Extracting String data from SO	OK

2025-08-29 22:01:04	Extracting String data from Code	OK
2025-08-29 22:01:04	Extracting String values and entropies from Code	OK
2025-08-29 22:01:08	Performing Malware check on extracted domains	OK
2025-08-29 22:01:10	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.