ANDROID STATIC ANALYSIS REPORT

Mihon (0.17.1)

File Name:	Mihon_0.17.1_APKPure.apk
Package Name:	app.mihon
Scan Date:	Feb. 6, 2025, 2:25 a.m.

App Security Score:	49/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	17	2	2	5

FILE INFORMATION

File Name: Mihon_0.17.1_APKPure.apk
Size: 23.88MB
MD5: b0c0af3241fd6e4bfbd2afb7452e7ad7
SHA1: 6ef0ce24e90d624474eec1119663593f479aef8c
SHA256: 6562cb4c25e5c06870271b093e32a9d488084b2c3f51245fdf57e082e27a4a71

APP INFORMATION

App Name: Mihon
Package Name: app.mihon
Main Activity: eu.kanade.tachiyomi.ui.main.MainActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 0.17.1
Android Version Code: 9

APP COMPONENTS

Activities: 11
Services: 14
Receivers: 17
Providers: 5
Exported Activities: 2
Exported Services: 2
Exported Receivers: 2
Exported Providers: 1

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: O=WorkshopOfAntsyLich, CN=AntsyLich
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-06-10 13:10:26+00:00
Valid To: 2047-06-04 13:10:26+00:00
Issuer: O=WorkshopOfAntsyLich, CN=AntsyLich
Serial Number: 0x4f6455b6

```
Hash Algorithm: sha256
md5: f677b11e0dbe6d6b106873e136d8c39b
sha1: 76b61d8e8bf66f61077c780182f8fec20f75bdda
sha256: 9add655a78e96c4ec7a53ef89dccb557cb5d767489fac5e785d671a5a75d4da2
sha512: bd6f5cf7b1bcc48254bc94f41e69d478417ec5f31640475bb9c27c8b67a18a01026c603e895923b17406ed9a3b47bd9b50cfa09d9250d637b9b03aefbc651929
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 7d002a3bc7651cba67a0f0dc5a3eef1c5f382bb89693afa0f6f2da2d4c6641ee
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.REQUEST_INSTALL_PACKAGES	dangerous	Allows an application to request installing packages.	Malicious applications can use this to try and trick users into installing additional malicious packages.
android.permission.REQUEST_DELETE_PACKAGES	normal	enables an app to request package deletions.	Allows an application to request deleting packages.
android.permission.UPDATE_PACKAGES_WITHOUT_USER_ACTION	normal	allows updating packages without requiring user action.	Allows an application to indicate via PackageInstaller.SessionParams.setRequireUserAction(int) that user action should not be required for an app update.
android.permission.QUERY_ALL_PACKAGES	normal	enables querying any normal app on the device.	Allows query of any normal app on the device, regardless of manifest declarations.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.READ_APP_SPECIFIC_LOCALES	unknown	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
android.permission.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.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.
app.mihon.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
moe.shizuku.manager.permission.API_V23	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>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
eu.kanade.tachiyomi.ui.main.MainActivity	Schemes: tachiyomi://, file://, content://, Hosts: add-repo, *, Mime Types: */*, Path Patterns: .*.tachibk, .*..*.tachibk, .*..*..*.tachibk, .*..*..*..*.tachibk, .*..*..*..*..*.tachibk, .*..*..*..*..*..*.tachibk, .*..*..*..*..*..*..*.tachibk,
eu.kanade.tachiyomi.ui.setting.track.TrackLoginActivity	Schemes: mihon://, Hosts: anilist-auth, bangumi-auth, myanimelist-auth, shikimori-auth,

NETWORK SECURITY

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

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.
3	*	high	Base config is configured to trust user installed 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: **9** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	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.
3	Activity (eu.kanade.tachiyomi.ui.deeplink.DeepLinkActivity) 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 (eu.kanade.tachiyomi.ui.setting.track.TrackLoginActivity) 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	Content Provider (rikka.shizuku.ShizukuProvider) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INTERACT_ACROSS_USERS_FULL [android:exported=true]	warning	A Content Provider 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.
6	TaskAffinity is set for activity (androidx.glance.appwidget.action.InvisibleActionTrampolineActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
7	Service (androidx.glance.appwidget.GlanceRemoteViewsService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_REMOTEVIEWS [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	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.
9	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
10	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

HIGH: **1** | WARNING: **5** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	eu/kanade/tachiyomi/network/NetworkHelper.java org/conscrypt/CertificatePriorityComparator.java org/conscrypt/ChainStrengthAnalyzer.java org/conscrypt/EvpMdRef.java org/conscrypt/OAEPParameters.java org/conscrypt/OidData.java org/conscrypt/OpenSSLCipherRSA.java org/conscrypt/OpenSSLECGroupContext.java org/conscrypt/OpenSSLProvider.java org/conscrypt/OpenSSLSignature.java org/conscrypt/TrustManagerImpl.java org/conscrypt/ct/CTConstants.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	coil/request/CachePolicy$EnumUnboxingLocalUtility.java coil3/network/NetworkHeaders.java com/davemorrissey/labs/subscaleview/SubsamplingScaleImageView.java com/davemorrissey/labs/subscaleview/decoder/Decoder.java curtains/Curtains$rootViewsSpy$2.java curtains/internal/WindowManagerSpy$mViewsField$2.java eu/kanade/domain/ui/model/ThemeModeKt.java eu/kanade/tachiyomi/data/cache/ChapterCache.java io/requery/android/database/DefaultDatabaseErrorHandler.java io/requery/android/database/sqlite/CloseGuard.java io/requery/android/database/sqlite/SQLiteConnection.java io/requery/android/database/sqlite/SQLiteConnectionPool.java io/requery/android/database/sqlite/SQLiteDatabase.java io/requery/android/database/sqlite/SQLiteDebug.java io/requery/android/database/sqlite/SQLiteOpenHelper.java io/requery/android/database/sqlite/SQLiteQuery.java logcat/LogcatKt.java logcat/LogcatLogger.java me/saket/swipe/SwipeRippleState.java org/brotli/dec/IntReader.java org/commonmark/internal/util/AsciiMatcher.java org/conscrypt/Platform.java org/conscrypt/ct/CTVerifier.java org/nibor/autolink/LinkExtractor.java org/nibor/autolink/internal/EmailScanner.java rikka/shizuku/Shizuku.java rikka/shizuku/ShizukuProvider.java rikka/shizuku/ShizukuRemoteProcess$$ExternalSyntheticLambda0.java rikka/shizuku/SystemServiceHelper.java rx/plugins/RxJavaHooks.java tachiyomi/data/SourcesQueries$$ExternalSyntheticLambda0.java tachiyomi/source/local/LocalSource$$ExternalSyntheticLambda6.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	coil/memory/MemoryCache$Key.java coil3/memory/MemoryCache$Key.java coil3/request/Options.java coil3/transform/Transformation.java eu/kanade/domain/track/service/TrackPreferences.java eu/kanade/presentation/util/Screen.java eu/kanade/tachiyomi/data/backup/models/BackupPreference.java eu/kanade/tachiyomi/data/backup/models/BackupSourcePreferences.java eu/kanade/tachiyomi/data/track/kitsu/dto/KitsuSearchResultData.java org/conscrypt/OpenSSLECKeyFactory.java org/conscrypt/OpenSSLRSAKeyFactory.java org/jsoup/internal/SharedConstants.java org/jsoup/nodes/DocumentType.java org/jsoup/nodes/Element.java tachiyomi/view/LibraryViewQueries$$ExternalSyntheticLambda0.java uy/kohesive/injekt/registry/p000default/DefaultRegistrar.java
4	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	eu/kanade/tachiyomi/data/cache/CoverCache.java eu/kanade/tachiyomi/data/saver/Location.java tachiyomi/core/common/storage/AndroidStorageFolderProvider.java
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	org/conscrypt/Conscrypt.java org/conscrypt/DefaultSSLContextImpl.java org/conscrypt/SSLParametersImpl.java
6	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	io/requery/android/database/sqlite/SQLiteDatabase.java
7	Insecure Implementation of SSL. Trusting all the certificates or accepting self signed certificates is a critical Security Hole. 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	org/conscrypt/Conscrypt.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	org/jsoup/helper/DataUtil.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	eu/kanade/tachiyomi/util/system/ContextExtensionsKt.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libarchive-jni.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: ['__strcat_chk', '__read_chk', '__strchr_chk', '__memcpy_chk', '__memmove_chk', '__strlen_chk']	True info Symbols are stripped.
2	arm64-v8a/libandroidx.graphics.path.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
3	arm64-v8a/libsqlite3x.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', '__memcpy_chk', '__memset_chk', '__strchr_chk', '__memmove_chk']	True info Symbols are stripped.
4	arm64-v8a/libconscrypt_jni.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', '__strchr_chk', '__memset_chk', '__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	arm64-v8a/libimagedecoder.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: ['__memset_chk', '__memmove_chk', '__memcpy_chk', '__vsnprintf_chk', '__strlen_chk', '__strcat_chk', '__vsprintf_chk']	True info Symbols are stripped.
6	arm64-v8a/libquickjs.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', '__strchr_chk', '__vsprintf_chk', '__strcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	arm64-v8a/libarchive-jni.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: ['__strcat_chk', '__read_chk', '__strchr_chk', '__memcpy_chk', '__memmove_chk', '__strlen_chk']	True info Symbols are stripped.
8	arm64-v8a/libandroidx.graphics.path.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
9	arm64-v8a/libsqlite3x.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', '__memcpy_chk', '__memset_chk', '__strchr_chk', '__memmove_chk']	True info Symbols are stripped.
10	arm64-v8a/libconscrypt_jni.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', '__strchr_chk', '__memset_chk', '__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__strlen_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	arm64-v8a/libimagedecoder.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: ['__memset_chk', '__memmove_chk', '__memcpy_chk', '__vsnprintf_chk', '__strlen_chk', '__strcat_chk', '__vsprintf_chk']	True info Symbols are stripped.
12	arm64-v8a/libquickjs.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', '__strchr_chk', '__vsprintf_chk', '__strcpy_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	eu/kanade/presentation/more/onboarding/PermissionStep$$ExternalSyntheticLambda1.java eu/kanade/tachiyomi/data/notification/NotificationHandler.java eu/kanade/tachiyomi/extension/ExtensionManager.java eu/kanade/tachiyomi/extension/util/ExtensionInstallReceiver.java eu/kanade/tachiyomi/extension/util/ExtensionInstaller.java eu/kanade/tachiyomi/util/system/ContextExtensionsKt.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	eu/kanade/presentation/more/onboarding/PermissionStep$$ExternalSyntheticLambda1.java eu/kanade/tachiyomi/extension/util/ExtensionInstallReceiver.java eu/kanade/tachiyomi/util/system/ContextExtensionsKt.java
00036	Get resource file from res/raw directory	reflection	eu/kanade/presentation/more/onboarding/PermissionStep$$ExternalSyntheticLambda1.java eu/kanade/tachiyomi/extension/util/ExtensionInstallReceiver.java eu/kanade/tachiyomi/util/system/ContextExtensionsKt.java
00013	Read file and put it into a stream	file	com/jakewharton/disklrucache/StrictLineReader.java eu/kanade/tachiyomi/data/download/DownloadCache.java eu/kanade/tachiyomi/ui/browse/migration/search/MigrateDialogScreenModel.java eu/kanade/tachiyomi/util/storage/FileExtensionsKt.java okio/Okio__JvmOkioKt.java org/commonmark/internal/util/AsciiMatcher.java org/conscrypt/DefaultSSLContextImpl.java org/conscrypt/FileClientSessionCache.java org/conscrypt/KeyManagerFactoryImpl.java tachiyomi/source/local/LocalSource$$ExternalSyntheticLambda6.java
00012	Read data and put it into a buffer stream	file	org/conscrypt/DefaultSSLContextImpl.java
00022	Open a file from given absolute path of the file	file	coil/disk/DiskCache.java coil3/disk/UtilsKt$$ExternalSyntheticLambda0.java eu/kanade/tachiyomi/extension/util/ExtensionLoader$$ExternalSyntheticLambda14.java eu/kanade/tachiyomi/extension/util/ExtensionLoader.java org/jsoup/Jsoup.java tachiyomi/core/common/storage/AndroidStorageFolderProvider.java
00163	Create new Socket and connecting to it	socket	org/conscrypt/AbstractConscryptSocket.java org/conscrypt/KitKatPlatformOpenSSLSocketImplAdapter.java org/conscrypt/PreKitKatPlatformOpenSSLSocketImplAdapter.java
00192	Get messages in the SMS inbox	sms	eu/kanade/tachiyomi/extension/util/ExtensionInstaller.java
00035	Query the list of the installed packages	reflection	eu/kanade/tachiyomi/extension/util/ExtensionLoader.java
00096	Connect to a URL and set request method	command network	org/jsoup/helper/HttpConnection.java

RULE ID	BEHAVIOUR	LABEL	FILES
00089	Connect to a URL and receive input stream from the server	command network	org/jsoup/helper/HttpConnection.java
00030	Connect to the remote server through the given URL	network	org/jsoup/helper/HttpConnection.java
00109	Connect to a URL and get the response code	network command	org/jsoup/helper/HttpConnection.java
00094	Connect to a URL and read data from it	command network	org/jsoup/helper/HttpConnection.java
00108	Read the input stream from given URL	network command	org/jsoup/helper/HttpConnection.java
00162	Create InetSocketAddress object and connecting to it	socket	org/conscrypt/AbstractConscryptSocket.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/82031285239/namespaces/firebase:fetch?key=AIzaSyDTvOxBQnuXADx5isKxoynPG0nlAO8bQbk. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.REQUEST_INSTALL_PACKAGES, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	2/44	android.permission.FOREGROUND_SERVICE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS

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
dns.alidns.com	IP: 223.5.5.5 Country: China Region: Zhejiang City: Hangzhou
dns-unfiltered.adguard.com	IP: 94.140.14.140 Country: Cyprus Region: Lemesos City: Limassol
doh.pub	IP: 162.14.21.178 Country: China Region: Beijing City: Beijing
doh.360.cn	IP: 101.198.193.29 Country: China Region: Beijing City: Beijing

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
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

DOMAIN	STATUS	GEOLOCATION
dns.alidns.com	ok	**IP:** 223.5.5.5 **Country:** China **Region:** Zhejiang **City:** Hangzhou **Latitude:** 30.293650 **Longitude:** 120.161423 **View:** Google Map
free.shecan.ir	ok	**IP:** 178.22.122.100 **Country:** Iran (Islamic Republic of) **Region:** Tehran **City:** Tehran **Latitude:** 35.694389 **Longitude:** 51.421509 **View:** Google Map
dns.quad9.net	ok	**IP:** 149.112.112.112 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.796986 **Longitude:** -122.462738 **View:** Google Map
mihon.app	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
dns.google	ok	**IP:** 8.8.8.8 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dns.njal.la	ok	**IP:** 95.215.19.53 **Country:** Sweden **Region:** Skane lan **City:** Malmoe **Latitude:** 55.605869 **Longitude:** 13.000730 **View:** Google Map
www.interpretation	ok	No Geolocation information available.
freedns.controld.com	ok	**IP:** 76.76.2.11 **Country:** Canada **Region:** Ontario **City:** Richmond Hill **Latitude:** 43.853016 **Longitude:** -79.432884 **View:** Google Map
dns-unfiltered.adguard.com	ok	**IP:** 94.140.14.140 **Country:** Cyprus **Region:** Lemesos **City:** Limassol **Latitude:** 34.674999 **Longitude:** 33.033329 **View:** Google Map
myanimelist.net	ok	**IP:** 3.168.122.79 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.text-decoration	ok	No Geolocation information available.
dns.twnic.tw	ok	**IP:** 101.101.101.101 **Country:** Taiwan (Province of China) **Region:** Taipei **City:** Taipei **Latitude:** 25.047760 **Longitude:** 121.531853 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.c	ok	No Geolocation information available.
doh.pub	ok	**IP:** 162.14.21.178 **Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map
www.recent	ok	No Geolocation information available.
www.style	ok	**IP:** 99.83.155.228 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
www.language	ok	No Geolocation information available.
kitsu.app	ok	**IP:** 104.26.9.99 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
.css	ok	No Geolocation information available.
shikimori.one	ok	**IP:** 172.67.157.46 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dontkillmyapp.com	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.hortcut	ok	No Geolocation information available.
www.world	ok	**IP:** 75.2.38.108 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
www.risktabsprev10pxrise25pxblueding300ballfordearnwildbox.fairlackverspairjunetechifpickevil	ok	No Geolocation information available.
www.a	ok	No Geolocation information available.
www.in	ok	No Geolocation information available.
doh.360.cn	ok	**IP:** 101.198.193.29 **Country:** China **Region:** Beijing **City:** Beijing **Latitude:** 39.907501 **Longitude:** 116.397232 **View:** Google Map
www.icon	ok	No Geolocation information available.
jsoup.org	ok	**IP:** 104.21.64.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.years	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
.jpg	ok	No Geolocation information available.
api.myanimelist.net	ok	**IP:** 18.238.80.96 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.css	ok	No Geolocation information available.
www.googleorganizationautocompleterequirementsconservative	ok	No Geolocation information available.
api.github.com	ok	**IP:** 140.82.113.5 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
example.com	ok	**IP:** 23.192.228.80 **Country:** United States of America **Region:** California **City:** San Jose **Latitude:** 37.339390 **Longitude:** -121.894958 **View:** Google Map
www.manifestations	ok	No Geolocation information available.
dns.mullvad.net	ok	**IP:** 194.242.2.2 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.mangaupdates.com	ok	**IP:** 24.199.74.221 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.714272 **Longitude:** -74.005966 **View:** Google Map
www.wencodeuricomponent	ok	No Geolocation information available.
cloudflare-dns.com	ok	**IP:** 104.16.248.249 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
github.com	ok	**IP:** 140.82.114.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
bgm.tv	ok	**IP:** 172.67.73.67 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

✉ EMAILS

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

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

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
"password" : "□□□□"
"username" : "Uzantnomo"
"onboarding_guides_returning_user" : "■ □■ □■■ □■■■■■■ □■■■■ □■■■■ □■ □■■ □■■ □□■ □"
"password" : "□□□□□□"
"unknown_author" : "□□"
"username" : "■■■■■■■■"
"password" : "Pasvorto"
"password" : "Salasana"
"unknown_author" : "■■■■■■■■■■■"
"username" : "Brukernavn"
"password" : "סיסמה"

POSSIBLE SECRETS
"password" : "■■■■■■■■"
"password" : "Sandhi"
"username" : "Brukarnamn"
"password" : "□□"
"username" : "■■■■■■■■■■■"
"username" : "Felhasználónév"
"pref_firebase" : "□□□□□□□□□□"
"password" : "■■■■■■■"
"username" : "□□□□□□"
"pref_firebase" : "□□□□□□□□□□□"
"unknown_author" : "■■■■■■■■■■■■■■"
"password" : "Password"
"password" : "■■■■■■■■■"
"password" : "Contrasenya"
"password" : "პაროლი"
"password" : "Parola"
"username" : "Käyttäjätunnus"
"unknown_author" : "□□□□□"
"private_settings" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"password" : "Passord"

POSSIBLE SECRETS
"password" : "□□"
"unknown_author" : "□□□□"
"password" : "Parolă"
"password" : "Contrasinal"
"password" : "Hasło"
"username" : "□□□"
"firebase_summary" : "□□"
"password" : "Пароль"
"ext_installer_private" : "Private"
"pref_firebase" : "■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■"
"password" : "Лозинка"
"password" : "Lozinka"
"password" : "Jelszó"
"username" : "Username"
"username" : "Användarnamn"
"google_api_key" : "AIzaSyDTvOxBQnuXADx5isKxoynPG0nlAO8bQbk"
"username" : "□□□□"
"password" : "Slaptažodis"
"password" : "Passwort"
"password" : "Аһарык"

POSSIBLE SECRETS
"password" : "Palavra-passe"
"username" : "Benutzername"
"password" : "Heslo"
"password" : "■■■■■■■■"
"password" : "■■■■■■■■"
"password" : "Lösenord"
"onboarding_guides_returning_user" : "%s□□□□□□□□□□□□□□□"
"pref_firebase" : "□□□□□□□□□"
"password" : "Contraseña"
"google_crash_reporting_api_key" : "AIzaSyDTvOxBQnuXADx5isKxoynPG0nlAO8bQbk"
"password" : "Wachtwoord"
"password" : "Құпиясөз"
"username" : "Gebruikersnaam"
"username" : "□□□□□"
"private_settings" : "□□□□□□□□□□□□□□□□□□□□□"
"username" : "■■■■■■■■■■"
"password" : "Parole"
"username" : "Lietotājvārds"
"firebase_summary" : "□□"
"password" : "Pasahitza"

POSSIBLE SECRETS
"username" : "Erabiltzaile-izena"
"password" : "Парола"
"password" : "گذرواژه"
"com.google.firebase.crashlytics.mapping_file_id" : "2db4dca0731b4efd83039c1783ed1a5e"
"password" : "Fjalëkalimi"
"password" : "Senha"
"username" : "■■■■■■■"
43e5ce36b207de16e5d3cfd3e79118db
b4050a850c04b3abf54132565044b0b7d7bfd8ba270b39432355ffb4
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
bd376388b5f723fb4c22dfe6cd4375a05a07476444d5819985007e34
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
dd031b32d2f56c990b1425efe6c42ad847e7fe3ab46bf1299f05ecd856bdb7dd
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
b70e0cbd6bb4bf7f321390b94a03c1d356c21122343280d6115c1d21
c46c9e24640a64dad5be5ca7a1a53a0f
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
54d7307928f63414defd96399fc31ba847961ceaecef3a5fd93144e960c0e151

POSSIBLE SECRETS
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
51953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
258EAFA5-E914-47DA-95CA-C5AB0DC85B11

SCAN LOGS

Timestamp	Event	Error
2025-02-06 02:25:29	Generating Hashes	OK
2025-02-06 02:25:29	Extracting APK	OK
2025-02-06 02:25:29	Unzipping	OK
2025-02-06 02:25:30	Parsing APK with androguard	OK
2025-02-06 02:25:31	Extracting APK features using aapt/aapt2	OK
2025-02-06 02:25:32	Getting Hardcoded Certificates/Keystores	OK
2025-02-06 02:25:37	Parsing AndroidManifest.xml	OK
2025-02-06 02:25:37	Extracting Manifest Data	OK

2025-02-06 02:25:37	Manifest Analysis Started	OK
2025-02-06 02:25:37	Reading Network Security config from network_security_config.xml	OK
2025-02-06 02:25:37	Parsing Network Security config	OK
2025-02-06 02:25:37	Performing Static Analysis on: Mihon (app.mihon)	OK
2025-02-06 02:25:37	Fetching Details from Play Store: app.mihon	OK
2025-02-06 02:25:37	Checking for Malware Permissions	OK
2025-02-06 02:25:37	Fetching icon path	OK
2025-02-06 02:25:38	Library Binary Analysis Started	OK
2025-02-06 02:25:38	Analyzing lib/arm64-v8a/libarchive-jni.so	OK
2025-02-06 02:25:38	Analyzing lib/arm64-v8a/libandroidx.graphics.path.so	OK
2025-02-06 02:25:38	Analyzing lib/arm64-v8a/libsqlite3x.so	OK
2025-02-06 02:25:38	Analyzing lib/arm64-v8a/libconscrypt_jni.so	OK
2025-02-06 02:25:38	Analyzing lib/arm64-v8a/libimagedecoder.so	OK
2025-02-06 02:25:38	Analyzing lib/arm64-v8a/libquickjs.so	OK

2025-02-06 02:25:38	Analyzing apktool_out/lib/arm64-v8a/libarchive-jni.so	OK
2025-02-06 02:25:38	Analyzing apktool_out/lib/arm64-v8a/libandroidx.graphics.path.so	OK
2025-02-06 02:25:38	Analyzing apktool_out/lib/arm64-v8a/libsqlite3x.so	OK
2025-02-06 02:25:38	Analyzing apktool_out/lib/arm64-v8a/libconscrypt_jni.so	OK
2025-02-06 02:25:38	Analyzing apktool_out/lib/arm64-v8a/libimagedecoder.so	OK
2025-02-06 02:25:38	Analyzing apktool_out/lib/arm64-v8a/libquickjs.so	OK
2025-02-06 02:25:39	Reading Code Signing Certificate	OK
2025-02-06 02:25:40	Running APKiD 2.1.5	OK
2025-02-06 02:25:44	Detecting Trackers	OK
2025-02-06 02:25:48	Decompiling APK to Java with JADX	OK
2025-02-06 02:28:00	Decompiling with JADX failed, attempting on all DEX files	OK
2025-02-06 02:28:00	Decompiling classes.dex with JADX	OK
2025-02-06 02:39:04	Decompiling with JADX failed for classes.dex	OK

2025-02-06 02:39:04	Decompiling classes2.dex with JADX	OK
2025-02-06 02:39:06	Decompiling classes3.dex with JADX	OK
2025-02-06 02:39:27	Decompiling classes.dex with JADX	OK
2025-02-06 02:58:11	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/b0c0af3241fd6e4bfbd2afb7452e7ad7/java_source', '-q', '-r', '--show-bad-code', '/home/mobsf/.MobSF/uploads/b0c0af3241fd6e4bfbd2afb7452e7ad7/apktool_out/classes.dex'], 999.9999764290001)
2025-02-06 02:58:11	Converting DEX to Smali	OK
2025-02-06 02:58:11	Code Analysis Started on - java_source	OK
2025-02-06 02:58:19	Android SBOM Analysis Completed	OK
2025-02-06 02:58:30	Android SAST Completed	OK
2025-02-06 02:58:30	Android API Analysis Started	OK
2025-02-06 02:58:34	Android API Analysis Completed	OK
2025-02-06 02:58:34	Android Permission Mapping Started	OK
2025-02-06 02:58:38	Android Permission Mapping Completed	OK
2025-02-06 02:58:39	Android Behaviour Analysis Started	OK

2025-02-06 02:58:43	Android Behaviour Analysis Completed	OK
2025-02-06 02:58:43	Extracting Emails and URLs from Source Code	OK
2025-02-06 02:58:47	Email and URL Extraction Completed	OK
2025-02-06 02:58:47	Extracting String data from APK	OK
2025-02-06 02:58:49	Extracting String data from SO	OK
2025-02-06 02:58:49	Extracting String data from Code	OK
2025-02-06 02:58:49	Extracting String values and entropies from Code	OK
2025-02-06 02:58:54	Performing Malware check on extracted domains	OK
2025-02-06 02:59:01	Saving to Database	OK

Report Generated by - MobSF v4.3.0

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.