MOBSF

ANDROID STATIC ANALYSIS REPORT

TrackerControl (2024.12.15-fdroid)

File Name:	net.kollnig.missioncontrol.fdroid_2024121503.apk
Package Name:	net.kollnig.missioncontrol.fdroid
Scan Date:	July 31, 2025, 11:50 p.m.

App Security Score: 43/100 (MEDIUM RISK)

Grade: B

Trackers Detection: 1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	22	2	0	1

FILE INFORMATION

File Name: net.kollnig.missioncontrol.fdroid_2024121503.apk

Size: 13.66MB
MD5: f179bde1e92ff4116b8b29f97d468dd3
SHA1: 1f4526d4768cdff3322c091ecbf2b3eefabcce78
SHA256: b6500ba63721d7a0c22279e229335f6d6563ea635c55e92d34817b626a84aca7

APP INFORMATION

App Name: TrackerControl
Package Name: net.kollnig.missioncontrol.fdroid
Main Activity: eu.faircode.netguard.ActivityMain
Target SDK: 34
Min SDK: 22
Max SDK:
Android Version Name: 2024.12.15-fdroid
Android Version Code: 2024121503

APP COMPONENTS

Activities: 8
Services: 5
Receivers: 5
Providers: 3
Exported Activities: 3
Exported Services: 3
Exported Receivers: 5
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-05-04 09:47:34+00:00
Valid To: 2047-09-20 09:47:34+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0xa3a4548
Hash Algorithm: sha256
md5: 76296e41132821cf09f36b9afdaa2106
sha1: 14501672c570afe9ac6b2191e6460878f7b83a9a
sha256: d54de792e8b68cb22d3dad7b5c9f37316489724ce6fb21572463ee5d4e074f01
sha512: 061ef2205037111d52375a43f42a2cce6461fae43968f6d30c54b8d0bc1946e05bb1c59d255edf02e90860324613fe78af2f0a2d4e31887913aecca4c8e4bc79
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: bdf11d59bfcd13c32cdab624726d6b94fdec0b1fadf12cb20a0e3ed7775e0862
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.
net.kollnig.missioncontrol.fdroid.permission.ADMIN	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.
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.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.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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
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.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.
net.kollnig.missioncontrol.fdroid.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER 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 Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Anti-VM Code</td><td>possible Build.SERIAL check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

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: 1 | 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.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 12 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.1-5.1.1, [minSdk=22]	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	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	Broadcast Receiver (eu.faircode.netguard.WidgetAdmin) is Protected by a permission, but the protection level of the permission should be checked. Permission: net.kollnig.missioncontrol.fdroid.permission.ADMIN [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
4	Activity (eu.faircode.netguard.ActivitySettings) 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	Activity (eu.faircode.netguard.ActivityForwardApproval) 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.
6	Activity (net.kollnig.missioncontrol.DetailsActivity) 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.
7	Service (eu.faircode.netguard.ServiceSinkhole) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_VPN_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.

NO	ISSUE	SEVERITY	DESCRIPTION
8	Service (eu.faircode.netguard.ServiceExternal) 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.
9	Service (eu.faircode.netguard.ServiceTileMain) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_QUICK_SETTINGS_TILE [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.
10	Broadcast Receiver (eu.faircode.netguard.ReceiverAutostart) is not Protected. [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.
11	Broadcast Receiver (eu.faircode.netguard.ReceiverPackageRemoved) is not Protected. [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.
12	Broadcast Receiver (eu.faircode.netguard.WidgetMain) is not Protected. [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.
13	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.
14	High Intent Priority (999) - {1} Hit(s) [android:priority]	warning	By setting an intent priority higher than another intent, the app effectively overrides other requests.

</> CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/Glide.java com/bumptech/glide/disklrucache/DiskLruCache.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java 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/ThumbnailStreamOpen

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/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 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 com/bumptech/glide/signature/ApplicationVersionSignature.java com/bumptech/glide/util/ContentLengthInputStream.java com/bumptech/glide/util/pool/FactoryPools.java com/caverock/androidsvg/CSSParser.java com/caverock/androidsvg/SVG.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/caverock/androidsvg/SVG.java com/caverock/androidsvg/SVGAndroidRenderer.java com/caverock/androidsvg/SVGImageView.java com/caverock/androidsvg/SVGParser.java com/caverock/androidsvg/SimpleAssetResolver.java eu/faircode/netguard/ActivityDns.java eu/faircode/netguard/ActivityForwardApproval.java eu/faircode/netguard/ActivityLog.java eu/faircode/netguard/ActivityMain.java eu/faircode/netguard/ActivitySettings.java eu/faircode/netguard/AdapterLog.java eu/faircode/netguard/AdapterRule.java eu/faircode/netguard/ApplicationEx.java eu/faircode/netguard/DatabaseHelper.java eu/faircode/netguard/DownloadTask.java eu/faircode/netguard/IPUtil.java eu/faircode/netguard/ReceiverAutostart.java eu/faircode/netguard/ReceiverPackageRemoved.java eu/faircode/netguard/Rule.java eu/faircode/netguard/ServiceExternal.java eu/faircode/netguard/ServiceSinkhole.java eu/faircode/netguard/ServiceTileMain.java eu/faircode/netguard/Util.java eu/faircode/netguard/WidgetAdmin.java eu/faircode/netguard/WidgetMain.java net/kollnig/missioncontrol/DetailsActivity.java net/kollnig/missioncontrol/data/TrackerList.java org/acra/ACRA.java org/acra/collector/LogCatCollector.java org/acra/log/AndroidLogDelegate.java org/acra/reporter/ErrorReporterImpl.java org/jf/dexlib2/dexbacked/DexBackedMethodImplementation.java org/jf/dexlib2/dexbacked/raw/StringIdItem.java org/jf/dexlib2/dexbacked/raw/util/DexAnnotator.java
2	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/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/engine/EngineResource.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/manager/RequestManagerRetriever.java com/maxmind/geoip2/WebServiceClient.java net/kollnig/missioncontrol/data/InternetBlocklist.java net/kollnig/missioncontrol/data/TrackerBlocklist.java
3	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	org/acra/file/Directory.java
4	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	org/jf/dexlib2/writer/io/FileDeferredOutputStream.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	eu/faircode/netguard/DatabaseHelper.java
6	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/faircode/netguard/ActivityLog.java eu/faircode/netguard/AdapterRule.java
7	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	eu/faircode/netguard/Util.java
8	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	eu/faircode/netguard/ActivityForwardApproval.java eu/faircode/netguard/ActivityLog.java eu/faircode/netguard/ActivitySettings.java eu/faircode/netguard/AdapterLog.java eu/faircode/netguard/ServiceSinkhole.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	x86_64/libnetguard.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: ['__strcpy_chk', '__vsprintf_chk', '__strlen_chk', '__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	x86/libnetguard.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: ['__strcpy_chk', '__vsprintf_chk', '__strlen_chk', '__memcpy_chk']	True info Symbols are stripped.
3	armeabi-v7a/libnetguard.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: ['__strcpy_chk', '__vsprintf_chk', '__strlen_chk', '__memcpy_chk']	True info Symbols are stripped.
4	arm64-v8a/libnetguard.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: ['__strcpy_chk', '__vsprintf_chk', '__strlen_chk', '__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	x86_64/libnetguard.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: ['__strcpy_chk', '__vsprintf_chk', '__strlen_chk', '__memcpy_chk']	True info Symbols are stripped.
6	x86/libnetguard.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: ['__strcpy_chk', '__vsprintf_chk', '__strlen_chk', '__memcpy_chk']	True info Symbols are stripped.
7	armeabi-v7a/libnetguard.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: ['__strcpy_chk', '__vsprintf_chk', '__strlen_chk', '__memcpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	arm64-v8a/libnetguard.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: ['__strcpy_chk', '__vsprintf_chk', '__strlen_chk', '__memcpy_chk']	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/fasterxml/jackson/databind/ser/std/FileSerializer.java eu/faircode/netguard/ServiceSinkhole.java org/jf/dexlib2/DexFileFactory.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/fasterxml/jackson/core/JsonFactory.java com/fasterxml/jackson/core/TokenStreamFactory.java com/fasterxml/jackson/databind/ObjectReader.java eu/faircode/netguard/ActivityLog.java eu/faircode/netguard/ActivitySettings.java org/acra/util/StreamReader.java org/jf/dexlib2/DexFileFactory.java org/jf/dexlib2/writer/io/FileDeferredOutputStream.java
00012	Read data and put it into a buffer stream	file	org/jf/dexlib2/DexFileFactory.java

RULE ID	BEHAVIOUR	LABEL	FILES
00112	Get the date of the calendar event	collection calendar	com/fasterxml/jackson/databind/ser/std/StdKeySerializers.java com/fasterxml/jackson/databind/util/StdDateFormat.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java eu/faircode/netguard/DownloadTask.java eu/faircode/netguard/ServiceExternal.java eu/faircode/netguard/Util.java net/kollnig/missioncontrol/Common.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java eu/faircode/netguard/DownloadTask.java eu/faircode/netguard/ServiceExternal.java eu/faircode/netguard/Util.java
00109	Connect to a URL and get the response code	network command	com/bumptech/glide/load/data/HttpUrlFetcher.java eu/faircode/netguard/DownloadTask.java eu/faircode/netguard/ServiceExternal.java
00009	Put data in cursor to JSON object	file	eu/faircode/netguard/ServiceSinkhole.java net/kollnig/missioncontrol/data/TrackerList.java
00072	Write HTTP input stream into a file	command network file	eu/faircode/netguard/DownloadTask.java eu/faircode/netguard/ServiceExternal.java
00094	Connect to a URL and read data from it	command network	eu/faircode/netguard/DownloadTask.java eu/faircode/netguard/ServiceExternal.java eu/faircode/netguard/Util.java
00108	Read the input stream from given URL	network command	eu/faircode/netguard/DownloadTask.java eu/faircode/netguard/ServiceExternal.java eu/faircode/netguard/Util.java
00023	Start another application from current application	reflection control	eu/faircode/netguard/AdapterRule.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	eu/faircode/netguard/ActivityLog.java eu/faircode/netguard/ActivityMain.java eu/faircode/netguard/ActivitySettings.java eu/faircode/netguard/AdapterRule.java eu/faircode/netguard/ServiceSinkhole.java net/kollnig/missioncontrol/Common.java net/kollnig/missioncontrol/DetailsActivity.java net/kollnig/missioncontrol/details/TrackersListAdapter.java org/acra/sender/EmailIntentSender.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	eu/faircode/netguard/ActivityLog.java eu/faircode/netguard/ActivityMain.java eu/faircode/netguard/ActivitySettings.java eu/faircode/netguard/AdapterLog.java eu/faircode/netguard/AdapterRule.java eu/faircode/netguard/ServiceSinkhole.java
00192	Get messages in the SMS inbox	sms	net/kollnig/missioncontrol/DetailsActivity.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	eu/faircode/netguard/ActivityLog.java eu/faircode/netguard/ActivityMain.java eu/faircode/netguard/ServiceSinkhole.java net/kollnig/missioncontrol/DetailsActivity.java org/acra/sender/EmailIntentSender.java
00078	Get the network operator name	collection telephony	eu/faircode/netguard/Util.java
00096	Connect to a URL and set request method	command network	eu/faircode/netguard/Util.java
00130	Get the current WIFI information	wifi collection	eu/faircode/netguard/Util.java
00091	Retrieve data from broadcast	collection	eu/faircode/netguard/Util.java
00065	Get the country code of the SIM card provider	collection	eu/faircode/netguard/Util.java
00125	Check if the given file path exist	file	eu/faircode/netguard/ActivityLog.java eu/faircode/netguard/ActivitySettings.java eu/faircode/netguard/Util.java
00132	Query The ISO country code	telephony collection	eu/faircode/netguard/Util.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java
00036	Get resource file from res/raw directory	reflection	eu/faircode/netguard/ActivityMain.java eu/faircode/netguard/ServiceSinkhole.java org/acra/sender/EmailIntentSender.java
00024	Write file after Base64 decoding	reflection file	org/acra/util/IOUtils.java
00028	Read file from assets directory	file	com/caverock/androidsvg/SimpleAssetResolver.java
00035	Query the list of the installed packages	reflection	eu/faircode/netguard/Rule.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	eu/faircode/netguard/ActivitySettings.java

RULE ID	BEHAVIOUR	LABEL	FILES
00005	Get absolute path of file and put it to JSON object	file	eu/faircode/netguard/ServiceSinkhole.java
00004	Get filename and put it to JSON object	file collection	eu/faircode/netguard/ServiceSinkhole.java
00162	Create InetSocketAddress object and connecting to it	socket	eu/faircode/netguard/ServiceSinkhole.java
00163	Create new Socket and connecting to it	socket	eu/faircode/netguard/ServiceSinkhole.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.ACCESS_NETWORK_STATE, android.permission.READ_PHONE_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.WAKE_LOCK, android.permission.INTERNET, android.permission.VIBRATE
Other Common Permissions	2/44	android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS, android.permission.FOREGROUND_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
edpb.europa.eu	ok	**IP:** 18.184.99.46 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
javax.xml.xmlconstants	ok	No Geolocation information available.
www.speedguide.net	ok	**IP:** 68.67.73.20 **Country:** United States of America **Region:** Florida **City:** Jacksonville **Latitude:** 30.324120 **Longitude:** -81.680908 **View:** Google Map
xmlpull.org	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.wikipedia.org	ok	**IP:** 185.15.59.224 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 20.26.156.215 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
play.google.com	ok	**IP:** 142.251.30.102 **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
www.f-droid.org	ok	**IP:** 37.218.243.72 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
xml.org	ok	**IP:** 104.239.142.8 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map
www.dnslytics.com	ok	**IP:** 104.21.48.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
ipinfo.io	ok	**IP:** 34.117.59.81 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
raw.githubusercontent.com	ok	**IP:** 185.199.110.133 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

EMAILS

EMAIL	FILE
crash@trackercontrol.org	eu/faircode/netguard/ApplicationEx.java
hello@trackercontrol.org□□□□□□□□ □□□□□□□□□□□□□□□tc@kollnig.net□□□□□□□□ ד-tc@kollnig.net tc@kollnig.net ta-protection-office@google.com □□□tc@kollnig.net□□□□□□□□ hello@trackercontrol.org	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
ACRA	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/444

HARDCODED SECRETS

POSSIBLE SECRETS
"instructions_monitoring_private_dns" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□DNS□"
"menu_app_user" : "□□□□□□□"
"menu_app_user" : "□□□□□□□□□□"
"instructions_monitoring_private_dns" : "□□DNS□□□□□□□□□□□□□□□□□□"
013602400437880159360205O5
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a

SCAN LOGS

Timestamp	Event	Error
2025-07-31 23:50:13	Generating Hashes	OK
2025-07-31 23:50:13	Extracting APK	OK
2025-07-31 23:50:13	Unzipping	OK
2025-07-31 23:50:14	Parsing APK with androguard	OK
2025-07-31 23:50:16	Extracting APK features using aapt/aapt2	OK
2025-07-31 23:50:17	Getting Hardcoded Certificates/Keystores	OK
2025-07-31 23:50:34	Parsing AndroidManifest.xml	OK
2025-07-31 23:50:34	Extracting Manifest Data	OK

2025-07-31 23:50:34	Manifest Analysis Started	OK
2025-07-31 23:50:34	Reading Network Security config from network_security_config.xml	OK
2025-07-31 23:50:34	Parsing Network Security config	OK
2025-07-31 23:50:34	Performing Static Analysis on: TrackerControl (net.kollnig.missioncontrol.fdroid)	OK
2025-07-31 23:50:35	Fetching Details from Play Store: net.kollnig.missioncontrol.fdroid	OK
2025-07-31 23:50:35	Checking for Malware Permissions	OK
2025-07-31 23:50:35	Fetching icon path	OK
2025-07-31 23:50:35	Library Binary Analysis Started	OK
2025-07-31 23:50:35	Analyzing apktool_out/lib/x86_64/libnetguard.so	OK
2025-07-31 23:50:35	Analyzing apktool_out/lib/x86/libnetguard.so	OK
2025-07-31 23:50:35	Analyzing apktool_out/lib/armeabi-v7a/libnetguard.so	OK
2025-07-31 23:50:35	Analyzing apktool_out/lib/arm64-v8a/libnetguard.so	OK
2025-07-31 23:50:35	Analyzing lib/x86_64/libnetguard.so	OK
2025-07-31 23:50:35	Analyzing lib/x86/libnetguard.so	OK
2025-07-31 23:50:35	Analyzing lib/armeabi-v7a/libnetguard.so	OK

2025-07-31 23:50:35	Analyzing lib/arm64-v8a/libnetguard.so	OK
2025-07-31 23:50:35	Reading Code Signing Certificate	OK
2025-07-31 23:50:38	Running APKiD 2.1.5	OK
2025-07-31 23:50:45	Detecting Trackers	OK
2025-07-31 23:50:52	Decompiling APK to Java with JADX	OK
2025-07-31 23:54:14	Converting DEX to Smali	OK
2025-07-31 23:54:14	Code Analysis Started on - java_source	OK
2025-07-31 23:54:38	Android SBOM Analysis Completed	OK
2025-07-31 23:55:21	Android SAST Completed	OK
2025-07-31 23:55:21	Android API Analysis Started	OK
2025-07-31 23:55:27	Android API Analysis Completed	OK
2025-07-31 23:55:28	Android Permission Mapping Started	OK
2025-07-31 23:55:36	Android Permission Mapping Completed	OK
2025-07-31 23:55:37	Android Behaviour Analysis Started	OK
2025-07-31 23:55:49	Android Behaviour Analysis Completed	OK

2025-07-31 23:55:49	Extracting Emails and URLs from Source Code	OK
2025-07-31 23:55:54	Email and URL Extraction Completed	OK
2025-07-31 23:55:54	Extracting String data from APK	OK
2025-07-31 23:55:54	Extracting String data from SO	OK
2025-07-31 23:55:55	Extracting String data from Code	OK
2025-07-31 23:55:55	Extracting String values and entropies from Code	OK
2025-07-31 23:56:08	Performing Malware check on extracted domains	OK
2025-07-31 23:56:12	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.