MOBSF

ANDROID STATIC ANALYSIS REPORT

NetGuard (2.330)

File Name:	eu.faircode.netguard_2024090101.apk
Package Name:	eu.faircode.netguard
Scan Date:	July 31, 2025, 11:37 p.m.
App Security Score:	46/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	22	2	1	1

FILE INFORMATION

File Name: eu.faircode.netguard_2024090101.apk
Size: 2.66MB
MD5: 9b389f94c16026ecd7cf3ce2a11ce983
SHA1: 68ec952d8cea3173bf2768e24bed322413481dd8
SHA256: 258172f5242e94469e973436b4a55ece6371dbdd49e6714a45ca58bc216a7788

APP INFORMATION

App Name: NetGuard
Package Name: eu.faircode.netguard
Main Activity: eu.faircode.netguard.ActivityMain
Target SDK: 34
Min SDK: 22
Max SDK:
Android Version Name: 2.330
Android Version Code: 2024090101

APP COMPONENTS

Activities: 7
Services: 6
Receivers: 5
Providers: 1
Exported Activities: 2
Exported Services: 6
Exported Receivers: 4
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: 2015-10-30 10:09:09+00:00
Valid To: 2043-03-17 10:09:09+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x124a21f6
Hash Algorithm: sha256
md5: 90d8cc508872be94e5a47224533cfcda
sha1: 3af2ad9c80b34528e1fa12e541209baebe128b81
sha256: cd775f59ee5aebba18d9f20aa5d69c7b6952958224b7c93f597e174b57b4dd8f
sha512: 52d9fa6b6ec97f0fd377ddbe758889f61f78b8cc0614804e0f4718c7dd7743f1f56d922d37b909eb099486f84070a5f4a913b055b641d8852d5b2b73e2aea19b
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: aff3dc69e023fa8673b409a102def0986f5ab054da48a39ca497cf14b2e93bec
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.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.
eu.faircode.netguard.permission.ADMIN	unknown	Unknown permission	Unknown permission from android reference
eu.faircode.netguard.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MANUFACTURER check possible Build.SERIAL check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</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: 13 | 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	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.
4	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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	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.
6	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.
7	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.
8	Service (eu.faircode.netguard.ServiceTileGraph) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
9	Service (eu.faircode.netguard.ServiceTileFilter) 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	Service (eu.faircode.netguard.ServiceTileLockdown) 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.
11	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.
12	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.
13	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.
14	Broadcast Receiver (eu.faircode.netguard.WidgetLockdown) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
15	Broadcast Receiver (eu.faircode.netguard.WidgetAdmin) is Protected by a permission. Permission: eu.faircode.netguard.permission.ADMIN protectionLevel: signature [android:exported=true]	info	A Broadcast Receiver is found to be exported, but is protected by permission.
16	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
				B/b.java F/g.java G/d.java G/e.java I/d.java I/f.java J/l.java J/m.java K/h.java K/n.java L/d.java M/C0008d.java M/C0012h.java M/C0016l.java M/C0018n.java M/K.java O/c.java P/B.java P/C0024b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
	The App logs information. Sensitive		CWE: CWE-532: Insertion of Sensitive Information into Log	P/C0027e.java P/C0030h.java P/j.java P/k.java P/p.java P/r.java P/v.java T/b.java T/f.java T/o.java V/d.java X/g.java X/h.java b0/c.java com/bumptech/glide/GeneratedAppGlideModuleImpl.java com/bumptech/glide/d.java com/bumptech/glide/load/data/b.java com/bumptech/glide/load/data/m.java com/bumptech/glide/load/data/o.java com/bumptech/glide/load/engine/K.java com/bumptech/glide/load/engine/RunnableC0211q.java com/bumptech/glide/load/engine/W.java com/bumptech/glide/load/engine/r.java com/bumptech/glide/load/engine/z.java com/bumptech/glide/manager/A.java com/bumptech/glide/manager/B.java com/bumptech/glide/manager/D.java com/bumptech/glide/manager/f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	[The app logs information. Sensitive information should never be logged.]	info	File OWASP MASVS: MSTG-STORAGE-3	com/bumptech/glide/manager/o.java com/bumptech/glide/manager/q.java com/bumptech/glide/manager/s.java com/bumptech/glide/manager/y.java com/bumptech/glide/request/i.java eu/faircode/netguard/ActivityDns.java eu/faircode/netguard/ActivityForwardApproval.java eu/faircode/netguard/ActivityLog.java eu/faircode/netguard/ActivityMain.java eu/faircode/netguard/ActivityPro.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/IAB.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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				eu/faircode/netguard/ServiceSinkhole.java eu/faircode/netguard/ServiceTileFilter.java eu/faircode/netguard/ServiceTileGraph.java eu/faircode/netguard/ServiceTileLockdown.java eu/faircode/netguard/ServiceTileMain.java eu/faircode/netguard/Util.java eu/faircode/netguard/WidgetAdmin.java eu/faircode/netguard/WidgetLockdown.java eu/faircode/netguard/WidgetMain.java m/C0246d.java t/C0281d.java
2	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
3	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	eu/faircode/netguard/Util.java
4	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	H/l.java com/bumptech/glide/load/engine/C0202h.java com/bumptech/glide/load/engine/I.java com/bumptech/glide/load/engine/S.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	n0/a.java n0/b.java n0/c.java o0/a.java
6	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
7	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/ActivityPro.java eu/faircode/netguard/AdapterRule.java
8	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

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.

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

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

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS 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
00072	Write HTTP input stream into a file	command network file	eu/faircode/netguard/DownloadTask.java eu/faircode/netguard/ServiceExternal.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/m.java eu/faircode/netguard/DownloadTask.java eu/faircode/netguard/ServiceExternal.java eu/faircode/netguard/Util.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/m.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/m.java 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
00108	Read the input stream from given URL	network command	eu/faircode/netguard/DownloadTask.java eu/faircode/netguard/ServiceExternal.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

RULE ID	BEHAVIOUR	LABEL	FILES
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
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/ActivityPro.java eu/faircode/netguard/ActivitySettings.java eu/faircode/netguard/AdapterRule.java eu/faircode/netguard/ServiceSinkhole.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/ActivityPro.java eu/faircode/netguard/AdapterRule.java
00036	Get resource file from res/raw directory	reflection	eu/faircode/netguard/ActivityMain.java eu/faircode/netguard/ServiceSinkhole.java
00013	Read file and put it into a stream	file	F/g.java F/i.java H/e.java M/C0018n.java eu/faircode/netguard/ActivityLog.java eu/faircode/netguard/ActivitySettings.java

RULE ID	BEHAVIOUR	LABEL	FILES
00191	Get messages in the SMS inbox	sms	eu/faircode/netguard/ActivityLog.java eu/faircode/netguard/ActivitySettings.java eu/faircode/netguard/AdapterLog.java eu/faircode/netguard/AdapterRule.java eu/faircode/netguard/ServiceSinkhole.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	eu/faircode/netguard/ActivitySettings.java
00023	Start another application from current application	reflection control	eu/faircode/netguard/AdapterRule.java
00022	Open a file from given absolute path of the file	file	eu/faircode/netguard/ServiceSinkhole.java
00005	Get absolute path of file and put it to JSON object	file	eu/faircode/netguard/ServiceSinkhole.java
00009	Put data in cursor to JSON object	file	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	1/44	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
api.github.com	ok	**IP:** 20.26.156.210 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
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
urlhaus.abuse.ch	ok	**IP:** 146.75.74.49 **Country:** Sweden **Region:** Vastra Gotalands lan **City:** Goeteborg **Latitude:** 57.707161 **Longitude:** 11.966790 **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:** 142.251.30.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 172.217.169.36 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.netguard.me	ok	**IP:** 18.172.153.114 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.dnslytics.com	ok	**IP:** 104.21.16.1 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
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
contact.faircode.eu	ok	**IP:** 18.172.153.108 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **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

HARDCODED SECRETS

POSSIBLE SECRETS
"setting_socks5_username" : "SOCKS5□□□□%s"
"menu_app_user" : "□□□□□□"
"setting_socks5_password" : "SOCKS5□□□%s"
"menu_app_user" : "□□□□□□□□□□"

PLAYSTORE INFORMATION

Title: NetGuard - no-root firewall

Score: 4.3690143 **Installs:** 5,000,000+ **Price:** 0 **Android Version Support:** **Category:** Tools **Play Store URL:** eu.faircode.netguard

Developer Details: Marcel Bokhorst, FairCode BV, 8420080860664580239, None, https://www.netguard.me/, marcel+help@faircode.eu,

Release Date: Nov 3, 2015 **Privacy Policy:** Privacy link

Description:

NetGuard is an internet security app, which offers simple and advanced ways to restrict apps' access to the internet. Applications and addresses can individually be allowed or denied access to your Wi-Fi and/or mobile connection. Root permissions are not required. Blocking access to the internet can help: • reduce your data usage • save your battery • increase your privacy Features: • Simple to use • No root required • 100% open source • No calling home • No tracking or analytics • No advertisements • Actively developed and supported • Android 5.1 and later supported • IPv4/IPv6 TCP/UDP supported • Tethering supported • Optionally allow when screen on • Optionally block when roaming • Optionally block system applications • Optionally notify when an application accesses the internet • Optionally record network usage per application per address • Material design theme with light and dark theme PRO features: • Log all outgoing traffic; search and filter access attempts; export PCAP files to analyze traffic • Allow/block individual addresses per application • New application notifications; configure NetGuard directly from the notification • Display network speed graph in a status bar notification • Select from five additional themes in both light and dark version There is no other no-root firewall offering all these features. If you like to test new features, you can participate in the test program: https://play.google.com/apps/testing/eu.faircode.netguard All required permissions are described here: https://github.com/M66B/NetGuard/blob/master/FAQ.md#user-content-faq42 NetGuard uses the Android VPNService to route traffic to itself, so it can be filtered on-device instead of on a server. Only one app can use this service at the same time, which is a limitation of Android. The full source code is available here:

https://github.com/M66B/NetGuard

SCAN LOGS

Timestamp	Event	Error
2025-07-31 23:37:48	Generating Hashes	OK
2025-07-31 23:37:48	Extracting APK	OK
2025-07-31 23:37:48	Unzipping	OK
2025-07-31 23:37:49	Parsing APK with androguard	OK
2025-07-31 23:37:51	Extracting APK features using aapt/aapt2	OK
2025-07-31 23:37:51	Getting Hardcoded Certificates/Keystores	OK
2025-07-31 23:38:04	Parsing AndroidManifest.xml	OK
2025-07-31 23:38:04	Extracting Manifest Data	OK

2025-07-31 23:38:04	Manifest Analysis Started	OK
2025-07-31 23:38:04	Reading Network Security config from network_security_config.xml	OK
2025-07-31 23:38:04	Parsing Network Security config	OK
2025-07-31 23:38:04	Performing Static Analysis on: NetGuard (eu.faircode.netguard)	OK
2025-07-31 23:38:06	Fetching Details from Play Store: eu.faircode.netguard	OK
2025-07-31 23:38:07	Checking for Malware Permissions	OK
2025-07-31 23:38:07	Fetching icon path	OK
2025-07-31 23:38:07	Library Binary Analysis Started	OK
2025-07-31 23:38:07	Analyzing apktool_out/lib/x86_64/libnetguard.so	OK
2025-07-31 23:38:07	Analyzing apktool_out/lib/x86/libnetguard.so	OK
2025-07-31 23:38:07	Analyzing apktool_out/lib/armeabi-v7a/libnetguard.so	OK

2025-07-31 23:38:07	Analyzing apktool_out/lib/arm64-v8a/libnetguard.so	OK
2025-07-31 23:38:07	Analyzing lib/x86_64/libnetguard.so	OK
2025-07-31 23:38:07	Analyzing lib/x86/libnetguard.so	OK
2025-07-31 23:38:07	Analyzing lib/armeabi-v7a/libnetguard.so	OK
2025-07-31 23:38:07	Analyzing lib/arm64-v8a/libnetguard.so	OK
2025-07-31 23:38:07	Reading Code Signing Certificate	OK
2025-07-31 23:38:09	Running APKiD 2.1.5	OK
2025-07-31 23:38:12	Updating Trackers Database....	OK
2025-07-31 23:38:12	Detecting Trackers	OK
2025-07-31 23:38:14	Decompiling APK to Java with JADX	OK
2025-07-31 23:38:59	Converting DEX to Smali	OK

2025-07-31 23:38:59	Code Analysis Started on - java_source	OK
2025-07-31 23:39:01	Android SBOM Analysis Completed	OK
2025-07-31 23:39:12	Android SAST Completed	OK
2025-07-31 23:39:12	Android API Analysis Started	OK
2025-07-31 23:39:15	Android API Analysis Completed	OK
2025-07-31 23:39:16	Android Permission Mapping Started	OK
2025-07-31 23:39:19	Android Permission Mapping Completed	OK
2025-07-31 23:39:19	Android Behaviour Analysis Started	OK
2025-07-31 23:39:23	Android Behaviour Analysis Completed	OK
2025-07-31 23:39:23	Extracting Emails and URLs from Source Code	OK
2025-07-31 23:39:23	Email and URL Extraction Completed	OK

2025-07-31 23:39:23	Extracting String data from APK	OK
2025-07-31 23:39:24	Extracting String data from SO	OK
2025-07-31 23:39:24	Extracting String data from Code	OK
2025-07-31 23:39:24	Extracting String values and entropies from Code	OK
2025-07-31 23:39:25	Performing Malware check on extracted domains	OK
2025-07-31 23:39:28	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.