



ANDROID STATIC ANALYSIS REPORT



 SaferVPN (1.0)

File Name: 5d3ff202f20af915863eee45916412a271bae1ea3a0e20988309c16723ce4da5.apk

Package Name: com.example.vpnner

Scan Date: April 26, 2025, 9:04 p.m.

App Security Score:

39/100 (HIGH RISK)

Grade:



 FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
5	11	2	1	1

 FILE INFORMATION

File Name: 5d3ff202f20af915863eee45916412a271bae1ea3a0e20988309c16723ce4da5.apk
Size: 11.75MB
MD5: 8a847b0f466b3174741aac734989aa73
SHA1: 03eadb4ab93a1a0232cb40b7d2ef179a1cd0174d
SHA256: 5d3ff202f20af915863eee45916412a271bae1ea3a0e20988309c16723ce4da5

APP INFORMATION

App Name: SaferVPN
Package Name: com.example.vpnner
Main Activity: com.example.vpnner.MainActivity
Target SDK: 25
Min SDK: 16
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 15
Services: 3
Receivers: 2
Providers: 0
Exported Activities: 0
Exported Services: 2
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2008-04-15 22:40:50+00:00
Valid To: 2035-09-01 22:40:50+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
Serial Number: 0xb3998086d056cffa
Hash Algorithm: md5
md5: 8ddb342f2da5408402d7568af21e29f9
sha1: 27196e386b875e76adf700e7ea84e4c6eee33dfa
sha256: c8a2e9bccf597c2fb6dc66bee293fc13f2fc47ec77bc6b2b0d52c11f51192ab8

sha512: 5d802f24d6ac76c708a8e7afe28fd97e038f888cef6665fb9b4a92234c311d6ff42127ccb2eb5a898f4e7e4e553f6ef602d43d1a2ebae9f002a6598e72fd2d83
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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
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.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_BACKGROUND_LOCATION	dangerous	access location in background	Allows an app to access location in the background.
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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
android.permission.CALL_PHONE	dangerous	directly call phone numbers	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.READ_CALL_LOG	dangerous	grants read access to the user's call log.	Allows an application to read the user's call log.
android.permission.READ_LOGS	unknown	Unknown permission	Unknown permission from android reference
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.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.
oppo.permission.OPPO_COMPONENT_SAFE	signature	permission specific to OPPO devices	It is used to grant apps the ability to access certain system-level features or components that are otherwise restricted for security reasons. This permission ensures that only trusted applications can interact with sensitive parts of the OPPO system.
com.huawei.permission.external_app_settings.USE_COMPONENT	signature	permission specific to Huawei devices	It is used to grant apps the ability to access certain system-level features or components that are otherwise restricted for security reasons. This permission ensures that only trusted applications can interact with sensitive parts of the Huawei system.

APKID ANALYSIS

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check Build.BRAND check Build.BOARD check possible Build.SERIAL check
	Compiler	r8

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

CERTIFICATE ANALYSIS

HIGH: 2 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	high	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Certificate algorithm vulnerable to hash collision	high	Application is signed with MD5. MD5 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 4.1-4.1.2, [minSdk=16]	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	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
3	App is direct-boot aware [android:directBootAware=true]	info	This app can run before the user unlocks the device. If you're using a custom subclass of Application, and if any component inside your application is direct - boot aware, then your entire custom application is considered to be direct - boot aware. During Direct Boot, your application can only access the data that is stored in device protected storage.
4	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
5	TaskAffinity is set for activity (de.blinkt.openvpn.DisconnectVPNActivity)	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.
6	Broadcast Receiver (com.example.vpnner.StartActivityOnBootReceiver) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
7	Broadcast Receiver (com.example.vpnner.NotificationReceiver) 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.
8	Service (de.blinkt.openvpn.core.OpenVPNService) 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.
9	Service (com.example.vpnner.MyJobIntentService) 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.

</> CODE ANALYSIS

HIGH: 0 | WARNING: 4 | INFO: 2 | SECURE: 0 | SUPPRESSED: 0

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/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/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/ImageDecoderResourceDecoder.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/DefaultConnectivityMonitor.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/manager/RequestManagerFragment.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptechnology/glide/manager/RequestManagerRetriever.java com/bumptechnology/glide/manager/RequestTracker.java com/bumptechnology/glide/manager/SupportRequestManagerFragment.java com/bumptechnology/glide/module/ManifestParser.java com/bumptechnology/glide/request/SingleRequest.java com/bumptechnology/glide/request/target/CustomViewTarget.java com/bumptechnology/glide/request/target/ViewTarget.java com/bumptechnology/glide/signature/ApplicationVersionSignature.java com/bumptechnology/glide/util/ContentLengthInputStream.java com/bumptechnology/glide/util/pool/FactoryPools.java com/example/vpnner/CameraTakeActivity.java com/example/vpnner/Functions.java com/example/vpnner/MainActivity.java com/example/vpnner/MainService.java com/example/vpnner/NotificationService.java com/example/vpnner/RecorderService.java com/example/vpnner/ShotActivity.java com/example/vpnner/gpsutil.java de/blinkt/openvpn/FileProvider.java de/blinkt/openvpn/OpenVpnApi.java de/blinkt/openvpn/api/ConfirmDialog.java de/blinkt/openvpn/core/OpenVPNService.java de/blinkt/openvpn/core/OpenVPNThread.java de/blinkt/openvpn/core/OpenVpnManagementThread.java de/blinkt/openvpn/core/PRNGFixes.java de/blinkt/openvpn/core/StatusListener.java org.greenrobot.eventbus.Logger.java org.greenrobot.eventbus/util/AlertDialogConfig.java org.greenrobot.eventbus/util/AlertDialogManager.java
2	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	de/blinkt/openvpn/api/AppRestrictions.java de/blinkt/openvpn/core/LogItem.java de/blinkt/openvpn/core/PRNGFixes.java
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	de/blinkt/openvpn/VpnProfile.java de/blinkt/openvpn/core/ConfigParser.java de/blinkt/openvpn/core/OpenVPNService.java de/blinkt/openvpn/core/OpenVpnManagementThread.java de/blinkt/openvpn/core/OrbotHelper.java de/blinkt/openvpn/core/X509Utils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/bumptechnology/load/Option.java com/bumptechnology/load/engine/DataCacheKey.java com/bumptechnology/load/engine/EngineResource.java com/bumptechnology/load/engine/ResourceCacheKey.java com/bumptechnology/manager/RequestManagerRetriever.java com/example/vpnner/NotificationReceiverKt.java de/blinkt/openvpn/LaunchVPN.java de/blinkt/openvpn/api/ExternalAppDatabase.java de/blinkt/openvpn/Utils/PropertiesService.java
5	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/example/vpnner/Constants.java com/example/vpnner/RecorderService.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	com/example/vpnner/Functions.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	arm64-v8a/libcrypto.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
2	arm64-v8a/libopenvpn.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: ['_FD_ISSET_chk', '_vsprintf_chk', '_memmove_chk', '_FD_CLR_chk', '_strchr_chk', '_strncpy_chk', '_strrchr_chk', '_umask_chk', '_memset_chk', '_fgets_chk', '_memcpy_chk', '_strcpy_chk', '_FD_SET_chk', '_vsnprintf_chk', '_strcat_chk', '_read_chk', '_strlen_chk']	True info Symbols are stripped.
3	arm64-v8a/libovpnexec.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Position Independent Executable (PIE) 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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
4	arm64-v8a/libopvpnutil.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: ['__strncpy_chk']	True info Symbols are stripped.
5	x86/libjbcrypto.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
6	x86/libopenvpn.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.
7	x86/libovpnexec.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Position Independent Executable (PIE) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86/libopvpnutil.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.
9	armeabi-v7a/libjbcrypto.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
10	armeabi-v7a/libopenvpn.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.
11	armeabi-v7a/libovpnexec.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Position Independent Executable (PIE) 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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
12	armeabi-v7a/libpvpnutil.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.
13	x86_64/libjbcrypto.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
14	x86_64/libopenvpn.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: ['_strchr_chk', '_memcpy_chk', '_memmove_chk', '_memset_chk', '_strchr_chk', '_strlen_chk', '_vsnprintf_chk', '_strcpy_chk', '_fgets_chk', '_strncpy_chk', '_FD_CLR_chk', '_FD_ISSET_chk', '_FD_SET_chk', '_strcat_chk', '_read_chk', '_umask_chk', '_vsprintf_chk']	True info Symbols are stripped.
15	x86_64/libovpnexec.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Position Independent Executable (PIE) 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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
16	x86_64/libopvpnutil.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: ['__strncpy_chk']	True info Symbols are stripped.
17	arm64-v8a/libjbcrypto.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
18	arm64-v8a/libopenvpn.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: ['_FD_ISSET_chk', '_vsprintf_chk', '_memmove_chk', '_FD_CLR_chk', '_strchr_chk', '_strncpy_chk', '_strrchr_chk', '_umask_chk', '_memset_chk', '_fgets_chk', '_memcpy_chk', '_strcpy_chk', '_FD_SET_chk', '_vsnprintf_chk', '_strcat_chk', '_read_chk', '_strlen_chk']	True info Symbols are stripped.
19	arm64-v8a/libovpnexec.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Position Independent Executable (PIE) 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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	arm64-v8a/libopvpnutil.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: ['__strncpy_chk']	True info Symbols are stripped.
21	x86/libjbcrypto.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
22	x86/libopenvpn.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.
23	x86/libovpnexec.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Position Independent Executable (PIE) 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
24	x86/libopvpnutil.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.
25	armeabi-v7a/libjbcrypto.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
26	armeabi-v7a/libopenvpn.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.
27	armeabi-v7a/libovpnexec.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Position Independent Executable (PIE) 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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
28	armeabi-v7a/libpvpnutil.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.
29	x86_64/libjbcrypto.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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
30	x86_64/libopenvpn.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: ['_strchr_chk', '_memcpy_chk', '_memmove_chk', '_memset_chk', '_strchr_chk', '_strlen_chk', '_vsnprintf_chk', '_strcpy_chk', '_fgets_chk', '_strncpy_chk', '_FD_CLR_chk', '_FD_ISSET_chk', '_FD_SET_chk', '_strcat_chk', '_read_chk', '_umask_chk', '_vsprintf_chk']	True info Symbols are stripped.
31	x86_64/libovpnexec.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Position Independent Executable (PIE) 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.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries. Not applicable for Dart/Flutter libraries unless Dart FFI is used.	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
32	x86_64/libopvpnutil.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: ['__strncpy_chk']	True info Symbols are stripped.

 NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

 BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/bumptechnology/glide/disklru/DiskLruCache.java com/bumptechnology/glide/load/model/FileLoader.java de/blinkt/openvpn/FileProvider.java de/blinkt/openvpn/core/LogFileHandler.java de/blinkt/openvpn/core/PRNGFixes.java de/blinkt/openvpn/core/X509Utils.java okio/Okio.java
00208	Capture the contents of the device screen	collection screen	com/example/vpnner/ShotActivity.java
00209	Get pixels from the latest rendered image	collection	com/example/vpnner/ShotActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00210	Copy pixels from the latest rendered image into a Bitmap	collection	com/example/vpnner/ShotActivity.java
00022	Open a file from given absolute path of the file	file	com/example/vpnner/Functions.java com/example/vpnner/RecorderService.java de/blinkt/openvpn/VpnProfile.java de/blinkt/openvpn/core/OpenVpnManagementThread.java de/blinkt/openvpn/core/VPNLaunchHelper.java
00195	Set the output path of the recorded file	record file	com/example/vpnner/Functions.java com/example/vpnner/RecorderService.java
00199	Stop recording and release recording resources	record	com/example/vpnner/Functions.java com/example/vpnner/RecorderService.java
00198	Initialize the recorder and start recording	record	com/example/vpnner/Functions.java com/example/vpnner/RecorderService.java
00194	Set the audio source (MIC) and recorded file format	record	com/example/vpnner/Functions.java com/example/vpnner/RecorderService.java
00197	Set the audio encoder and initialize the recorder	record	com/example/vpnner/Functions.java com/example/vpnner/RecorderService.java
00007	Use absolute path of directory for the output media file path	file	com/example/vpnner/Functions.java com/example/vpnner/RecorderService.java
00196	Set the recorded file format and output path	record file	com/example/vpnner/Functions.java com/example/vpnner/RecorderService.java
00002	Open the camera and take picture	camera	com/example/vpnner/CameraTakeActivity.java com/example/vpnner/Functions.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptechnology/load/data/mediastore/ThumbFetcher.java com/example/vpnner/Functions.java
00189	Get the content of a SMS message	sms	com/example/vpnner/Functions.java
00202	Make a phone call	control	com/example/vpnner/Functions.java
00193	Send a SMS message	sms	com/example/vpnner/Functions.java

RULE ID	BEHAVIOUR	LABEL	FILES
00203	Put a phone number into an intent	control	com/example/vpnner/Functions.java
00096	Connect to a URL and set request method	command network	com/example/vpnner/Functions.java com/example/vpnner/MainActivity.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/example/vpnner/Functions.java
00188	Get the address of a SMS message	sms	com/example/vpnner/Functions.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	com/example/vpnner/Functions.java
00176	Send sms to a contact of contact list	sms	com/example/vpnner/Functions.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/example/vpnner/Functions.java
00089	Connect to a URL and receive input stream from the server	command network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/example/vpnner/Functions.java com/example/vpnner/MainActivity.java
00158	Connect to a URL and send sensitive data got from resolver	privacy connection	com/example/vpnner/Functions.java
00030	Connect to the remote server through the given URL	network	com/bumptech/glide/load/data/HttpUrlFetcher.java com/example/vpnner/Functions.java com/example/vpnner/MainActivity.java
00175	Get notification manager and cancel notifications	notification	com/example/vpnner/Functions.java com/example/vpnner/UtilsKt.java
00006	Scheduling recording task	record	com/example/vpnner/Functions.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/example/vpnner/Functions.java
00191	Get messages in the SMS inbox	sms	com/example/vpnner/Functions.java
00200	Query data from the contact list	collection contact	com/example/vpnner/Functions.java
00187	Query a URI and check the result	collection sms calllog calendar	com/example/vpnner/Functions.java

RULE ID	BEHAVIOUR	LABEL	FILES
00152	Get data from HTTP and send SMS	command sms	com/example/vpnner/Functions.java
00041	Save recorded audio/video to file	record	com/example/vpnner/Functions.java
00201	Query data from the call log	collection callog	com/example/vpnner/Functions.java
00036	Get resource file from res/raw directory	reflection	com/example/vpnner/Functions.java
00012	Read data and put it into a buffer stream	file	de/blinkt/openvpn/core/LogFileHandler.java
00109	Connect to a URL and get the response code	network command	com/bumptechnology/load/data/HttpUrlFetcher.java com/example/vpnner/MainActivity.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	17/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_WIFI_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.READ_CONTACTS, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.READ_SMS, android.permission.SEND_SMS, android.permission.READ_CALL_LOG, android.permission.REQUEST_INSTALL_PACKAGES, android.permission.WAKE_LOCK
Other Common Permissions	4/44	android.permission.FOREGROUND_SERVICE, android.permission.ACCESS_BACKGROUND_LOCATION, android.permission.CALL_PHONE, 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
--------	----------------

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
cdsa.xyz	malware URL: cdsa.xyz IP: N/A Description: Malicious Domain tagged by Maltrail	IP: 13.248.169.48 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
openvpn.net	ok	IP: 104.19.191.106 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
repo.xposed.info	ok	IP: 45.55.233.97 Country: United States of America Region: New Jersey City: Clifton Latitude: 40.858429 Longitude: -74.163757 View: Google Map
natmchugh.blogspot.de	ok	IP: 142.250.179.225 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
android.googlesource.com	ok	IP: 74.125.133.82 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 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
sites.inka.de	ok	IP: 193.197.184.17 Country: Germany Region: Baden-Wurttemberg City: Stuttgart Latitude: 48.782318 Longitude: 9.177020 View: Google Map
crowdin.net	ok	IP: 3.91.254.30 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
xposed.info	ok	IP: 45.55.233.97 Country: United States of America Region: New Jersey City: Clifton Latitude: 40.858429 Longitude: -74.163757 View: Google Map
community.openvpn.net	ok	IP: 104.19.191.106 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.bouncycastle.org	ok	IP: 43.250.142.130 Country: Australia Region: Queensland City: Warren Latitude: -23.500000 Longitude: 150.283325 View: Google Map
google.com	ok	IP: 142.250.200.14 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
developer.android.com	ok	IP: 172.217.16.238 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

EMAILS

EMAIL	FILE
arne@rfc2549.org eay@cryptsoft.com helbeierling@t-online.de sales@openvpn.net	Android String Resource
sales@openvpn.net	apktool_out/lib/arm64-v8a/libopenvpn.so
sales@openvpn.net	apktool_out/lib/x86/libopenvpn.so
sales@openvpn.net	apktool_out/lib/armeabi-v7a/libopenvpn.so
sales@openvpn.net	apktool_out/lib/x86_64/libopenvpn.so

EMAIL	FILE
sales@openvpn.net	lib/arm64-v8a/libopenvpn.so
sales@openvpn.net	lib/x86/libopenvpn.so
sales@openvpn.net	lib/armeabi-v7a/libopenvpn.so
sales@openvpn.net	lib/x86_64/libopenvpn.so

HARDCODED SECRETS

POSSIBLE SECRETS
"auth_username" : "Username"
"password" : "Password"
"settings_auth" : "Authentication/Encryption"
"state_auth" : "Authenticating"
258EAFa5-E914-47DA-95CA-C5AB0DC85B11

SCAN LOGS

Timestamp	Event	Error
2025-04-26 21:04:44	Generating Hashes	OK
2025-04-26 21:04:44	Extracting APK	OK
2025-04-26 21:04:44	Unzipping	OK

2025-04-26 21:04:44	Parsing APK with androguard	OK
2025-04-26 21:04:44	Extracting APK features using aapt/aapt2	OK
2025-04-26 21:04:45	Getting Hardcoded Certificates/Keystores	OK
2025-04-26 21:04:46	Parsing AndroidManifest.xml	OK
2025-04-26 21:04:46	Extracting Manifest Data	OK
2025-04-26 21:04:46	Manifest Analysis Started	OK
2025-04-26 21:04:46	Performing Static Analysis on: SaferVPN (com.example.vpnner)	OK
2025-04-26 21:04:46	Fetching Details from Play Store: com.example.vpnner	OK
2025-04-26 21:04:47	Checking for Malware Permissions	OK
2025-04-26 21:04:47	Fetching icon path	OK
2025-04-26 21:04:47	Library Binary Analysis Started	OK
2025-04-26 21:04:47	Analyzing apktool_out/lib/arm64-v8a/libbcrypt.so	OK
2025-04-26 21:04:47	Analyzing apktool_out/lib/arm64-v8a/libopenvpn.so	OK
2025-04-26 21:04:47	Analyzing apktool_out/lib/arm64-v8a/libovpnexec.so	OK

2025-04-26 21:04:47	Analyzing apktool_out/lib/arm64-v8a/libbopvpnutil.so	OK
2025-04-26 21:04:47	Analyzing apktool_out/lib/x86/libjbcrypto.so	OK
2025-04-26 21:04:47	Analyzing apktool_out/lib/x86/libbopenvpn.so	OK
2025-04-26 21:04:47	Analyzing apktool_out/lib/x86/libbopvpnextec.so	OK
2025-04-26 21:04:47	Analyzing apktool_out/lib/x86/libbopvpnutil.so	OK
2025-04-26 21:04:47	Analyzing apktool_out/lib/armeabi-v7a/libjbcrypto.so	OK
2025-04-26 21:04:47	Analyzing apktool_out/lib/armeabi-v7a/libbopenvpn.so	OK
2025-04-26 21:04:47	Analyzing apktool_out/lib/armeabi-v7a/libbopvpnextec.so	OK
2025-04-26 21:04:47	Analyzing apktool_out/lib/armeabi-v7a/libbopvpnutil.so	OK
2025-04-26 21:04:47	Analyzing apktool_out/lib/x86_64/libjbcrypto.so	OK
2025-04-26 21:04:47	Analyzing apktool_out/lib/x86_64/libbopenvpn.so	OK
2025-04-26 21:04:47	Analyzing apktool_out/lib/x86_64/libbopvpnextec.so	OK
2025-04-26 21:04:47	Analyzing apktool_out/lib/x86_64/libbopvpnutil.so	OK
2025-04-26 21:04:47	Analyzing lib/arm64-v8a/libjbcrypto.so	OK

2025-04-26 21:04:47	Analyzing lib/arm64-v8a/libopenvpn.so	OK
2025-04-26 21:04:47	Analyzing lib/arm64-v8a/libovpnexec.so	OK
2025-04-26 21:04:47	Analyzing lib/arm64-v8a/libovpnutil.so	OK
2025-04-26 21:04:47	Analyzing lib/x86/libcrypto.so	OK
2025-04-26 21:04:47	Analyzing lib/x86/libopenvpn.so	OK
2025-04-26 21:04:47	Analyzing lib/x86/libovpnexec.so	OK
2025-04-26 21:04:47	Analyzing lib/x86/libovpnutil.so	OK
2025-04-26 21:04:47	Analyzing lib/armeabi-v7a/libcrypto.so	OK
2025-04-26 21:04:47	Analyzing lib/armeabi-v7a/libopenvpn.so	OK
2025-04-26 21:04:47	Analyzing lib/armeabi-v7a/libovpnexec.so	OK
2025-04-26 21:04:47	Analyzing lib/armeabi-v7a/libovpnutil.so	OK
2025-04-26 21:04:47	Analyzing lib/x86_64/libcrypto.so	OK
2025-04-26 21:04:47	Analyzing lib/x86_64/libopenvpn.so	OK
2025-04-26 21:04:47	Analyzing lib/x86_64/libovpnexec.so	OK

2025-04-26 21:04:47	Analyzing lib/x86_64/libopvpnutil.so	OK
2025-04-26 21:04:47	Reading Code Signing Certificate	OK
2025-04-26 21:04:48	Running APKiD 2.1.5	OK
2025-04-26 21:04:49	Detecting Trackers	OK
2025-04-26 21:04:50	Decompiling APK to Java with JADX	OK
2025-04-26 21:04:56	Converting DEX to Smali	OK
2025-04-26 21:04:56	Code Analysis Started on - java_source	OK
2025-04-26 21:04:57	Android SBOM Analysis Completed	OK
2025-04-26 21:04:58	Android SAST Completed	OK
2025-04-26 21:04:58	Android API Analysis Started	OK
2025-04-26 21:04:58	Android API Analysis Completed	OK
2025-04-26 21:04:58	Android Permission Mapping Started	OK
2025-04-26 21:04:59	Android Permission Mapping Completed	OK
2025-04-26 21:04:59	Android Behaviour Analysis Started	OK

2025-04-26 21:05:00	Android Behaviour Analysis Completed	OK
2025-04-26 21:05:00	Extracting Emails and URLs from Source Code	OK
2025-04-26 21:05:00	Email and URL Extraction Completed	OK
2025-04-26 21:05:00	Extracting String data from APK	OK
2025-04-26 21:05:00	Extracting String data from SO	OK
2025-04-26 21:05:00	Extracting String data from Code	OK
2025-04-26 21:05:00	Extracting String values and entropies from Code	OK
2025-04-26 21:05:01	Performing Malware check on extracted domains	OK
2025-04-26 21:05:04	Saving to Database	OK
2025-04-26 21:10:52	Performing Malware check on extracted domains	OK
2025-04-26 21:10:54	Detecting Trackers from Domains	OK
2025-04-26 21:14:09	Performing Malware check on extracted domains	OK
2025-04-26 21:14:10	Detecting Trackers from Domains	OK

Report Generated by - MobSF v4.3.2

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.

© 2025 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).