MOBSF

ANDROID STATIC ANALYSIS REPORT

OpenVPN for Android (0.7.61)

File Name: de.blinkt.openvpn_216.apk

Package Name:	de.blinkt.openvpn
Scan Date:	Aug. 1, 2025, 12:10 a.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	32	2	2	1

FILE INFORMATION

File Name: de.blinkt.openvpn_216.apk
Size: 43.83MB
MD5: 96e4efe775f30ca4eeddb5a827adf7e7
SHA1: 3ad81699e928ca63a75c8ecd1c1a846f23ddbb7b
SHA256: 78c1413e86c8a4b776ff6bb195a39cdbda6860cc96c28d1dc7fcdc44d97bb19c

APP INFORMATION

App Name: OpenVPN for Android
Package Name: de.blinkt.openvpn
Main Activity: de.blinkt.openvpn.activities.MainActivity
Target SDK: 35
Min SDK: 21
Max SDK:
Android Version Name: 0.7.61
Android Version Code: 216

APP COMPONENTS

Activities: 14
Services: 5
Receivers: 2
Providers: 2
Exported Activities: 10
Exported Services: 4
Exported Receivers: 2
Exported Providers: 1

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: 2012-09-03 17:30:00+00:00
Valid To: 2040-01-20 17:30:00+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x5044e918
Hash Algorithm: sha1
md5: a9c9d6217921adace3956e867241f949
sha1: a46fd6d27ba0c44fe5e131670bcabce511027968
sha256: 4cd330fe6593e2e64b1e1fa383f0c6d73892184fc1cd1a909e71d558d862e212
sha512: a6f51a158da840b6f602b329c13783fa3d70043d0add6f86567fbf43664de72623f1dc60c2ff074b5474afde2b13dc5f78093e53376621af59861a21c458183f
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 34ce06c8195716f6330c87c5b9ca1b496d44812698daafdd548366598d2ce6eb
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.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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
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_SPECIAL_USE	normal	enables special-use foreground services.	Allows a regular application to use Service.startForeground with the type "specialUse".
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.
de.blinkt.openvpn.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.BOARD check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
de.blinkt.openvpn.activities.MainActivity	Schemes: openvpn://, Hosts: import-profile,
de.blinkt.openvpn.activities.ConfigConverter	Schemes: content://, Hosts: *, Mime Types: application/x-openvpn-profile, application/ovpn, */*, Path Patterns: .*..*..*..*..*.ovpn, .*..*..*..*.ovpn, .*..*..*.ovpn, .*..*.ovpn, .*.ovpn,

ACTIVITY	INTENT
de.blinkt.openvpn.activities.ConfigConverterFile	Schemes: file://, Hosts: *, Mime Types: */*, Path Patterns: .*..*..*..*..*.ovpn, .*..*..*..*.ovpn, .*..*..*.ovpn, .*..*.ovpn, .*.ovpn,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 2 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 24 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 5.0-5.0.2, [minSdk=21]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	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.
3	Service (de.blinkt.openvpn.OpenVPNTileService) 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.
4	TaskAffinity is set for activity (de.blinkt.openvpn.activities.ConfigConverter)	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.
5	Activity (de.blinkt.openvpn.activities.ConfigConverter) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Activity-Alias (de.blinkt.openvpn.activities.ConfigConverterFile) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	TaskAffinity is set for activity (de.blinkt.openvpn.activities.CreateShortcuts)	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.

NO	ISSUE	SEVERITY	DESCRIPTION
8	Activity (de.blinkt.openvpn.activities.CreateShortcuts) 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.
9	Content Provider (de.blinkt.openvpn.FileProvider) is not Protected. [android:exported=true]	warning	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	TaskAffinity is set for activity (de.blinkt.openvpn.activities.DisconnectVPN)	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.
11	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.
12	Service (de.blinkt.openvpn.api.ExternalOpenVPNService) 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.
13	Activity (de.blinkt.openvpn.api.GrantPermissionsActivity) 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.
14	Activity (de.blinkt.openvpn.api.ConfirmDialog) 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
15	Broadcast Receiver (de.blinkt.openvpn.OnBootReceiver) 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.
16	Service (de.blinkt.openvpn.core.keepVPNAlive) 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.
17	TaskAffinity is set for activity (de.blinkt.openvpn.LaunchVPN)	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.
18	Activity (de.blinkt.openvpn.LaunchVPN) 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.
19	TaskAffinity is set for activity (de.blinkt.openvpn.api.RemoteAction)	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.
20	Activity-Alias (de.blinkt.openvpn.api.ResumeVPN) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
21	Activity-Alias (de.blinkt.openvpn.api.PauseVPN) is not Protected. [android:exported=true]	warning	An Activity-Alias 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
22	Activity-Alias (de.blinkt.openvpn.api.DisconnectVPN) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
23	Activity-Alias (de.blinkt.openvpn.api.ConnectVPN) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
24	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
25	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: **5** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/OpenVPNThreadv3.java de/blinkt/openvpn/core/OpenVpnManagementThread.java de/blinkt/openvpn/core/OrbotHelper.java de/blinkt/openvpn/core/X509Utils.java de/blinkt/openvpn/fragments/DNSSummaryProvider.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/github/mikephil/charting/charts/BarChart.java com/github/mikephil/charting/charts/BarLineChartBase.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/charts/CombinedChart.java com/github/mikephil/charting/charts/HorizontalBarChart.java com/github/mikephil/charting/charts/PieRadarChartBase.java com/github/mikephil/charting/components/AxisBase.java com/github/mikephil/charting/data/ChartData.java com/github/mikephil/charting/data/CombinedData.java com/github/mikephil/charting/data/LineDataSet.java com/github/mikephil/charting/data/PieEntry.java com/github/mikephil/charting/listener/BarLineChartTouchListener.java com/github/mikephil/charting/renderer/CombinedChartRenderer.java com/github/mikephil/charting/renderer/ScatterChartRenderer.java com/github/mikephil/charting/utils/FileUtils.java com/github/mikephil/charting/utils/Utils.java de/blinkt/openvpn/FileProvider.java de/blinkt/openvpn/VpnProfile.java de/blinkt/openvpn/activities/InternalWebView.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/StatusListener.java de/blinkt/openvpn/fragments/ImportRemoteConfig$doAsImport$2.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	de/blinkt/openvpn/LaunchVPN.java de/blinkt/openvpn/api/ExternalAppDatabase.java de/blinkt/openvpn/api/ExternalOpenVPNService.java de/blinkt/openvpn/fragments/FileSelectionFragment.java
4	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/utils/FileUtils.java de/blinkt/openvpn/activities/ConfigConverter.java de/blinkt/openvpn/activities/FileSelect.java de/blinkt/openvpn/fragments/FileSelectionFragment.java
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	de/blinkt/openvpn/fragments/ImportRemoteConfig.java
6	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
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	de/blinkt/openvpn/fragments/LogFragment.java
8	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	de/blinkt/openvpn/activities/InternalWebView.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	x86_64/libovpnutil.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	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
3	x86_64/libosslspeedtest.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__read_chk', '__memcpy_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86_64/libovpn3.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: ['__vsprintf_chk', '__memcpy_chk', '__read_chk', '__strlen_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	x86_64/libosslutil.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__read_chk', '__memcpy_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	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', '__strncpy_chk', '__vsnprintf_chk', '__strlen_chk', '__strcat_chk', '__FD_SET_chk', '__umask_chk', '__read_chk', '__strncat_chk', '__memset_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	x86/libovpnutil.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
8	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.	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
9	x86/libosslspeedtest.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__read_chk', '__memcpy_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	x86/libovpn3.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: ['__vsprintf_chk', '__memcpy_chk', '__read_chk', '__strlen_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	x86/libosslutil.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__read_chk', '__memcpy_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	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.	True info The binary has the following fortified functions: ['__strchr_chk', '__memcpy_chk', '__strncpy_chk', '__vsnprintf_chk', '__strlen_chk', '__strcat_chk', '__FD_SET_chk', '__umask_chk', '__read_chk', '__strncat_chk', '__memset_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	armeabi-v7a/libovpnutil.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	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
15	armeabi-v7a/libosslspeedtest.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__read_chk', '__memcpy_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	armeabi-v7a/libovpn3.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: ['__vsprintf_chk', '__memcpy_chk', '__read_chk', '__vsnprintf_chk', '__strlen_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	armeabi-v7a/libosslutil.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__read_chk', '__memcpy_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	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.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strchr_chk', '__memcpy_chk', '__strncpy_chk', '__strlen_chk', '__strcat_chk', '__FD_SET_chk', '__umask_chk', '__read_chk', '__strncat_chk', '__memset_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	arm64-v8a/libovpnutil.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
20	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
21	arm64-v8a/libosslspeedtest.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__read_chk', '__memcpy_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	arm64-v8a/libovpn3.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: ['__vsprintf_chk', '__memcpy_chk', '__read_chk', '__strlen_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	arm64-v8a/libosslutil.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__read_chk', '__memcpy_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	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: ['__strchr_chk', '__memcpy_chk', '__strncpy_chk', '__vsnprintf_chk', '__strlen_chk', '__strcat_chk', '__FD_SET_chk', '__umask_chk', '__read_chk', '__strncat_chk', '__memset_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
25	x86_64/libovpnutil.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
26	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
27	x86_64/libosslspeedtest.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__read_chk', '__memcpy_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
28	x86_64/libovpn3.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: ['__vsprintf_chk', '__memcpy_chk', '__read_chk', '__strlen_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	x86_64/libosslutil.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__read_chk', '__memcpy_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	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', '__strncpy_chk', '__vsnprintf_chk', '__strlen_chk', '__strcat_chk', '__FD_SET_chk', '__umask_chk', '__read_chk', '__strncat_chk', '__memset_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
31	x86/libovpnutil.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
32	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.	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
33	x86/libosslspeedtest.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__read_chk', '__memcpy_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
34	x86/libovpn3.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: ['__vsprintf_chk', '__memcpy_chk', '__read_chk', '__strlen_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
35	x86/libosslutil.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__read_chk', '__memcpy_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
36	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.	True info The binary has the following fortified functions: ['__strchr_chk', '__memcpy_chk', '__strncpy_chk', '__vsnprintf_chk', '__strlen_chk', '__strcat_chk', '__FD_SET_chk', '__umask_chk', '__read_chk', '__strncat_chk', '__memset_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
37	armeabi-v7a/libovpnutil.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
38	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
39	armeabi-v7a/libosslspeedtest.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__read_chk', '__memcpy_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
40	armeabi-v7a/libovpn3.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: ['__vsprintf_chk', '__memcpy_chk', '__read_chk', '__vsnprintf_chk', '__strlen_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
41	armeabi-v7a/libosslutil.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__read_chk', '__memcpy_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
42	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.	True info The binary has the following fortified functions: ['__vsnprintf_chk', '__strchr_chk', '__memcpy_chk', '__strncpy_chk', '__strlen_chk', '__strcat_chk', '__FD_SET_chk', '__umask_chk', '__read_chk', '__strncat_chk', '__memset_chk', '__memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
43	arm64-v8a/libovpnutil.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
44	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
45	arm64-v8a/libosslspeedtest.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__read_chk', '__memcpy_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
46	arm64-v8a/libovpn3.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: ['__vsprintf_chk', '__memcpy_chk', '__read_chk', '__strlen_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
47	arm64-v8a/libosslutil.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlen_chk', '__read_chk', '__memcpy_chk', '__memset_chk', '__memmove_chk', '__strchr_chk', '__strncpy_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
48	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: ['__strchr_chk', '__memcpy_chk', '__strncpy_chk', '__vsnprintf_chk', '__strlen_chk', '__strcat_chk', '__FD_SET_chk', '__umask_chk', '__read_chk', '__strncat_chk', '__memset_chk', '__memmove_chk']	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	com/github/mikephil/charting/charts/Chart.java de/blinkt/openvpn/VpnProfile.java de/blinkt/openvpn/activities/ConfigConverter.java de/blinkt/openvpn/core/OpenVpnManagementThread.java de/blinkt/openvpn/fragments/FileSelectionFragment.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	de/blinkt/openvpn/core/OpenVPNService.java de/blinkt/openvpn/fragments/SendDumpFragment.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	de/blinkt/openvpn/core/OpenVPNService.java
00091	Retrieve data from broadcast	collection	de/blinkt/openvpn/core/PasswordDialogFragment.java de/blinkt/openvpn/fragments/VPNProfileList.java
00013	Read file and put it into a stream	file	de/blinkt/openvpn/FileProvider.java de/blinkt/openvpn/activities/ConfigConverter.java de/blinkt/openvpn/activities/FileSelect.java de/blinkt/openvpn/core/LogFileHandler.java de/blinkt/openvpn/core/ProfileEncryption.java de/blinkt/openvpn/core/ProfileManager.java de/blinkt/openvpn/core/X509Utils.java okio/Okio__JvmOkioKt.java
00036	Get resource file from res/raw directory	reflection	de/blinkt/openvpn/fragments/SendDumpFragment.java
00012	Read data and put it into a buffer stream	file	de/blinkt/openvpn/core/LogFileHandler.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	4/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.READ_EXTERNAL_STORAGE
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
developer.android.com	ok	**IP:** 142.250.117.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
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
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
crowdin.com	ok	**IP:** 3.216.48.26 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
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
code.google.com	ok	**IP:** 142.250.129.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **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:** 3.216.48.26 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.bouncycastle.org	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
community.openvpn.net	ok	**IP:** 104.19.190.106 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **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

EMAILS

EMAIL	FILE
arne@rfc2549.org	de/blinkt/openvpn/fragments/SendDumpFragment.java

EMAIL	FILE
alyaksandr.koshal@gmail.com luis449bp+openvpn@gmail.com sales@openvpn.net helbeierling@t-online.de dannybaumann@web.de volkangezer@gmail.com eay@cryptsoft.com ktdann@gmail.com tobiaschannel11@gmail.com sergi@koolpi.com arne@rfc2549.org baier.jan@gmail.com tools@artin.nu horonitel@gmail.com tojidotakarin@gmail.com	Android String Resource
appro@openssl.org	apktool_out/lib/x86_64/libosslspeedtest.so
appro@openssl.org	apktool_out/lib/x86_64/libovpn3.so
appro@openssl.org	apktool_out/lib/x86_64/libosslutil.so
appro@openssl.org sales@openvpn.net	apktool_out/lib/x86_64/libopenvpn.so
sales@openvpn.net	apktool_out/lib/x86/libopenvpn.so
sales@openvpn.net	apktool_out/lib/armeabi-v7a/libopenvpn.so
appro@openssl.org	apktool_out/lib/arm64-v8a/libosslspeedtest.so
appro@openssl.org	apktool_out/lib/arm64-v8a/libovpn3.so
appro@openssl.org	apktool_out/lib/arm64-v8a/libosslutil.so

EMAIL	FILE
appro@openssl.org sales@openvpn.net	apktool_out/lib/arm64-v8a/libopenvpn.so
appro@openssl.org	lib/x86_64/libosslspeedtest.so
appro@openssl.org	lib/x86_64/libovpn3.so
appro@openssl.org	lib/x86_64/libosslutil.so
appro@openssl.org sales@openvpn.net	lib/x86_64/libopenvpn.so
sales@openvpn.net	lib/x86/libopenvpn.so
sales@openvpn.net	lib/armeabi-v7a/libopenvpn.so
appro@openssl.org	lib/arm64-v8a/libosslspeedtest.so
appro@openssl.org	lib/arm64-v8a/libovpn3.so
appro@openssl.org	lib/arm64-v8a/libosslutil.so
appro@openssl.org sales@openvpn.net	lib/arm64-v8a/libopenvpn.so

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"state_auth" : "Authenticating"

POSSIBLE SECRETS
"faq_remote_api_title" : "□□□□API"
"pkcs12_file_encryption_key" : "PKCS12-Verschlüsselungs-Passwort"
"password" : "Passord"
"settings_auth" : "Autenticação/encriptação"
"pkcs12_file_encryption_key" : "PKCS12□□□□□□□□□□□□"
"password" : "סיסמה"
"state_auth" : "Uwierzytelnianie"
"save_password" : "□□□□"
"state_auth_pending" : "□□□□□□□□□"
"state_auth" : "Hitelesítés"
"auth_username" : "□□□□□□□□□□□□□□□□□"
"client_key_title" : "Clientzertifikatsschlüssel"
"settings_auth" : "Overitev/Šifriranje"
"settings_auth" : "Autentimine/Krüpteerimine"
"state_auth_pending" : "□□□□□□□"
"packet_auth" : "Paket-Authentifizierung"

POSSIBLE SECRETS
"state_auth_failed" : "□□□□"
"settings_auth" : "Overenia/šifrovania"
"settings_auth" : "Πιστοποίηση/Κρυπτογράφηση"
"external_authenticator" : "□□□□"
"private_key_password" : "□□□□"
"settings_auth" : "□□/□□"
"tls_authentication" : "TLS□□/□□□"
"settings_auth" : "Autentizace/Šifrování"
"password" : "Лозинка"
"show_password" : "□□□□"
"state_auth" : "Πιστοποίηση"
"packet_auth" : "□□□□□"
"state_auth" : "Authentifiziere"
"password" : "□□"
"client_key_title" : "□□□□□□□"
"password" : "Passwort"

POSSIBLE SECRETS
"state_auth" : "Overjanje"
"password" : "■■■■■■"
"settings_auth" : "Аутентификация/шифрование"
"settings_auth" : "Autentificare/criptare"
"faq_remote_api_title" : "Remote-API"
"state_auth" : "Autenticando"
"state_auth" : "Аутентификация"
"settings_auth" : "Authenticatie/Encryptie"
"state_auth" : "Godkender"
"settings_auth" : "Uwierzytelnianie/Szyfrowanie"
"state_auth" : "Autentisering"
"password" : "Salasõna"
"auth_username" : "□□□□(□□□□□□□□□□□)"
"tls_authentication" : "TLS□□/□□"
"state_auth" : "□□□"
"proxy_auth_username" : "Username"

POSSIBLE SECRETS
"tls_authentication" : "TLS-autentisering/kryptering"
"private_key_password" : "□□□□□□□□□□"
"auth_username" : "Hassan"
"state_auth" : "Autentificare"
"state_auth" : "Autentiserar"
"password" : "Lösenord"
"state_auth_failed" : "□□□□□□□"
"state_auth" : "מאמת"
"settings_auth" : "אימות/הצפנה"
"password" : "Пароль"
"faq_remote_api" : "Ok"
"settings_auth" : "Authentifizierung/Verschlüsselung"
"password" : "Geslo"
"state_auth" : "Authenticeren"
"state_auth_pending" : "□□□□□"
"tls_authentication" : "TLS-autentificering/kryptering"

POSSIBLE SECRETS
"session_ipv4string" : "%1$s-%2$s"
"password" : "Senha"
"vpn_allow_bypass" : "□□□□□□VPN"
"password" : "□□□□□"
"state_auth" : "Autentimine"
"password" : "Password"
"password" : "Wachtwoord"
"external_authenticator" : "□□□□□□□□"
"password" : "□□"
"state_auth" : "Аутентифікація"
"settings_auth" : "Autentisering/kryptering"
"client_key_title" : "Klientcertifikatnøgle"
"session_ipv4string" : "%1$s□%2$s"
"packet_auth" : "Pakkegodkendelse"
"password" : "Adgangskode"
"save_password" : "□□□□"

POSSIBLE SECRETS
"settings_auth" : "Autentificering/kryptering"
"password" : "Hasło"
"client_key_title" : "□□□□□□□□"
"save_password" : "□□□□□□□□□"
"state_auth" : "□□□□□□□"
"settings_auth" : "■■■■■■■■/■■■■■■■■■■■"
"settings_auth" : "Authentification/Chiffrement"
"state_auth" : "□□□"
"vpn_allow_bypass" : "□□□□VPN□□□□□□□□□□□□□□"
"client_key_title" : "□□□□□□□□□□□□□"
"show_password" : "□□□□□□□□□□□"
"settings_auth" : "Autenticazione/crittografia"
"settings_auth" : "Autenticación/Cifrado"
"settings_auth" : "Authentication/Encryption"
"packet_auth" : "Packet-authenticatie"
"packet_auth" : "□□□□□□□"

POSSIBLE SECRETS
"password" : "Contraseña"
"client_key_title" : "Klientcertifikatsnyckel"
"trigger_pending_auth_dialog" : "□□□□□□□□□□□□□□□□□□□□□□□□□□□□□"
"settings_auth" : "□□/□□□"
"password" : "Jelszó"
"password" : "Contrasenya"
"password" : "Heslo"
"faq_remote_api_title" : "Fjern-API"
"state_auth_failed" : "□□□□□□□□□"
"trigger_pending_auth_dialog" : "□□□□□□□□□□□□□□□□□□□□□"
"settings_auth" : "□□/□□□"
"state_auth" : "مصادقة"
"password" : "□□"
"external_authenticator" : "□□□□□"
"packet_auth" : "□□□□"
"settings_auth" : "Автентифікація/Шифрування"

POSSIBLE SECRETS
"state_auth" : "Autenticazione"
"settings_auth" : "Autentificació/Encriptació"
"settings_auth" : "Hitelesítés/Titkosítás"
"settings_auth" : "Otentikasi/Enkripsi"
"show_password" : "□□□□"
"password" : "Sandi"
"packet_auth" : "Paketautentisering"
"state_auth" : "Autenticant"
"session_ipv6string" : "%1$s□%3$s□%2$s"
"settings_auth" : "المصادقة/التشفير"
"state_auth" : "Authentification"
"faq_remote_api_title" : "□□API"
"settings_auth" : "Autenticação/Cifragem"
"private_key_password" : "□□□□□□"
"state_auth" : "Аутентификација"
"auth_username" : "□□□□□□□□□□□□□□□"

POSSIBLE SECRETS
"password" : "Parola"
"session_ipv6string" : "%1$s-%3$s,%2$s"
"faq_remote_api_title" : "Fjärr-API"
"settings_auth" : "□□/□□"
"state_auth" : "□□□"
"packet_auth" : "Pakkegodkjenning"
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
1157920892103562487626974469494075735299969552241357603424222590610685120443 69

POSSIBLE SECRETS
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
115792089210356248762697446949407573530086143415290314195533631308867097853951
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7

PLAYSTORE INFORMATION

Title: OpenVPN for Android

Score: 4.1897106 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** **Category:** Communication **Play Store URL:** de.blinkt.openvpn

Developer Details: Arne Schwabe, Arne+Schwabe, None, http://ics-openvpn.blinkt.de/, arne-openvpn@rfc2549.org,

Release Date: Apr 11, 2012 **Privacy Policy:** Privacy link

Description:

Openvpn for Android is an open source client based on the open source OpenVPN project. It uses the VPNService API of Android 4.0+ and requires neither Jailbreak nor root on your telephone. FAQ Can I get free Internet No, this app is for connecting to an OpenVPN server. How to connect OpenVPN is a client software to connect to an OpenVPN server. It is not an APP selling or provding any VPN services. It allows to your own/company/university/provider OpenVPN server or to the VPN service of many of the commercial VPN providers. What is the difference between all the OpenVPN apps? For more information about the different OpenVPN clients in the Playstore see this: http://ics-openvpn.blinkt.de/FAQ.html#faq_androids_clients_title Access to your photos/media (Android older than 6.0) This app implements a feature to import OpenVPN profiles from the SDCard/internal memory. Google categorizes this access "accessing your media and photos" TAP Mode Only tun mode support (Sorry no tap, with Android 4.0 only tun can be supported). Joining Beta The beta is open, you can the beta by using the join beta beta. Please note that often a beta is not available since I mostly use the beta function to pretest release candidates. Translate the app If you want to help to translate OpenVPN into your native language look at the homepage of this project. Bug reports Please report bug/suggestions via email or at the code Google Code project. But please read the FAQ before writing me. Security OpenSSL Heartbleed: OpenVPN for Android uses its own non vulnerable OpenSSL version. For more details about OpenVPN and Heartbleed see: https://community.openvpn.net/openvpn/wiki/heartbleed

SCAN LOGS

Timestamp	Event	Error
2025-08-01 00:10:43	Generating Hashes	OK
2025-08-01 00:10:44	Extracting APK	OK
2025-08-01 00:10:44	Unzipping	OK
2025-08-01 00:10:46	Parsing APK with androguard	OK
2025-08-01 00:10:48	Extracting APK features using aapt/aapt2	OK
2025-08-01 00:10:49	Getting Hardcoded Certificates/Keystores	OK
2025-08-01 00:10:59	Parsing AndroidManifest.xml	OK
2025-08-01 00:10:59	Extracting Manifest Data	OK
2025-08-01 00:10:59	Manifest Analysis Started	OK
2025-08-01 00:10:59	Performing Static Analysis on: OpenVPN for Android (de.blinkt.openvpn)	OK

2025-08-01 00:11:00	Fetching Details from Play Store: de.blinkt.openvpn	OK
2025-08-01 00:11:01	Checking for Malware Permissions	OK
2025-08-01 00:11:01	Fetching icon path	OK
2025-08-01 00:11:01	Library Binary Analysis Started	OK
2025-08-01 00:11:01	Analyzing apktool_out/lib/x86_64/libovpnutil.so	OK
2025-08-01 00:11:01	Analyzing apktool_out/lib/x86_64/libovpnexec.so	OK
2025-08-01 00:11:01	Analyzing apktool_out/lib/x86_64/libosslspeedtest.so	OK
2025-08-01 00:11:01	Analyzing apktool_out/lib/x86_64/libovpn3.so	OK
2025-08-01 00:11:02	Analyzing apktool_out/lib/x86_64/libosslutil.so	OK
2025-08-01 00:11:02	Analyzing apktool_out/lib/x86_64/libopenvpn.so	OK
2025-08-01 00:11:02	Analyzing apktool_out/lib/x86/libovpnutil.so	OK

2025-08-01 00:11:02	Analyzing apktool_out/lib/x86/libovpnexec.so	OK
2025-08-01 00:11:02	Analyzing apktool_out/lib/x86/libosslspeedtest.so	OK
2025-08-01 00:11:03	Analyzing apktool_out/lib/x86/libovpn3.so	OK
2025-08-01 00:11:03	Analyzing apktool_out/lib/x86/libosslutil.so	OK
2025-08-01 00:11:03	Analyzing apktool_out/lib/x86/libopenvpn.so	OK
2025-08-01 00:11:03	Analyzing apktool_out/lib/armeabi-v7a/libovpnutil.so	OK
2025-08-01 00:11:03	Analyzing apktool_out/lib/armeabi-v7a/libovpnexec.so	OK
2025-08-01 00:11:03	Analyzing apktool_out/lib/armeabi-v7a/libosslspeedtest.so	OK
2025-08-01 00:11:03	Analyzing apktool_out/lib/armeabi-v7a/libovpn3.so	OK
2025-08-01 00:11:04	Analyzing apktool_out/lib/armeabi-v7a/libosslutil.so	OK
2025-08-01 00:11:04	Analyzing apktool_out/lib/armeabi-v7a/libopenvpn.so	OK

2025-08-01 00:11:04	Analyzing apktool_out/lib/arm64-v8a/libovpnutil.so	OK
2025-08-01 00:11:04	Analyzing apktool_out/lib/arm64-v8a/libovpnexec.so	OK
2025-08-01 00:11:04	Analyzing apktool_out/lib/arm64-v8a/libosslspeedtest.so	OK
2025-08-01 00:11:04	Analyzing apktool_out/lib/arm64-v8a/libovpn3.so	OK
2025-08-01 00:11:05	Analyzing apktool_out/lib/arm64-v8a/libosslutil.so	OK
2025-08-01 00:11:05	Analyzing apktool_out/lib/arm64-v8a/libopenvpn.so	OK
2025-08-01 00:11:05	Analyzing lib/x86_64/libovpnutil.so	OK
2025-08-01 00:11:05	Analyzing lib/x86_64/libovpnexec.so	OK
2025-08-01 00:11:05	Analyzing lib/x86_64/libosslspeedtest.so	OK
2025-08-01 00:11:05	Analyzing lib/x86_64/libovpn3.so	OK
2025-08-01 00:11:06	Analyzing lib/x86_64/libosslutil.so	OK

2025-08-01 00:11:06	Analyzing lib/x86_64/libopenvpn.so	OK
2025-08-01 00:11:06	Analyzing lib/x86/libovpnutil.so	OK
2025-08-01 00:11:06	Analyzing lib/x86/libovpnexec.so	OK
2025-08-01 00:11:06	Analyzing lib/x86/libosslspeedtest.so	OK
2025-08-01 00:11:06	Analyzing lib/x86/libovpn3.so	OK
2025-08-01 00:11:07	Analyzing lib/x86/libosslutil.so	OK
2025-08-01 00:11:07	Analyzing lib/x86/libopenvpn.so	OK
2025-08-01 00:11:07	Analyzing lib/armeabi-v7a/libovpnutil.so	OK
2025-08-01 00:11:07	Analyzing lib/armeabi-v7a/libovpnexec.so	OK
2025-08-01 00:11:07	Analyzing lib/armeabi-v7a/libosslspeedtest.so	OK
2025-08-01 00:11:07	Analyzing lib/armeabi-v7a/libovpn3.so	OK

2025-08-01 00:11:07	Analyzing lib/armeabi-v7a/libosslutil.so	OK
2025-08-01 00:11:08	Analyzing lib/armeabi-v7a/libopenvpn.so	OK
2025-08-01 00:11:08	Analyzing lib/arm64-v8a/libovpnutil.so	OK
2025-08-01 00:11:08	Analyzing lib/arm64-v8a/libovpnexec.so	OK
2025-08-01 00:11:08	Analyzing lib/arm64-v8a/libosslspeedtest.so	OK
2025-08-01 00:11:08	Analyzing lib/arm64-v8a/libovpn3.so	OK
2025-08-01 00:11:08	Analyzing lib/arm64-v8a/libosslutil.so	OK
2025-08-01 00:11:08	Analyzing lib/arm64-v8a/libopenvpn.so	OK
2025-08-01 00:11:09	Reading Code Signing Certificate	OK
2025-08-01 00:11:12	Running APKiD 2.1.5	OK
2025-08-01 00:11:21	Detecting Trackers	OK

2025-08-01 00:11:26	Decompiling APK to Java with JADX	OK
2025-08-01 00:13:47	Converting DEX to Smali	OK
2025-08-01 00:13:48	Code Analysis Started on - java_source	OK
2025-08-01 00:14:17	Android SBOM Analysis Completed	OK
2025-08-01 00:14:29	Android SAST Completed	OK
2025-08-01 00:14:29	Android API Analysis Started	OK
2025-08-01 00:14:32	Android API Analysis Completed	OK
2025-08-01 00:14:33	Android Permission Mapping Started	OK
2025-08-01 00:14:35	Android Permission Mapping Completed	OK
2025-08-01 00:14:35	Android Behaviour Analysis Started	OK
2025-08-01 00:14:38	Android Behaviour Analysis Completed	OK

2025-08-01 00:14:38	Extracting Emails and URLs from Source Code	OK
2025-08-01 00:14:39	Email and URL Extraction Completed	OK
2025-08-01 00:14:39	Extracting String data from APK	OK
2025-08-01 00:14:41	Extracting String data from SO	OK
2025-08-01 00:14:45	Extracting String data from Code	OK
2025-08-01 00:14:45	Extracting String values and entropies from Code	OK
2025-08-01 00:14:52	Performing Malware check on extracted domains	OK
2025-08-01 00:14:56	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.