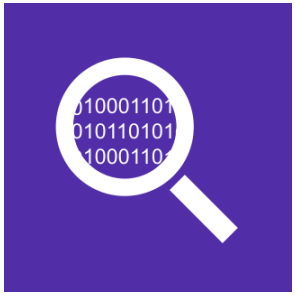
MOBSF

ANDROID STATIC ANALYSIS REPORT



PCAPdroid (1.8.6)

File Name:	com.emanuelef.remote_capture_86.apk
Package Name:	com.emanuelef.remote_capture
Scan Date:	Aug. 1, 2025, 12:58 a.m.
App Security Score:	51/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	11	2	1	1

FILE INFORMATION

File Name: com.emanuelef.remote_capture_86.apk
Size: 14.8MB
MD5: eeb6ca611b9dc520874ca2ea3272e8ca
SHA1: 1de3f5572c5cb59bcc1d55a8c0583064cee52bcf
SHA256: 6e4961d792357e1337ae92fc92ebeae77e1143fe360411da18301b3a24c1a137

APP INFORMATION

App Name: PCAPdroid
Package Name: com.emanuelef.remote_capture
Main Activity: com.emanuelef.remote_capture.activities.MainActivity
Target SDK: 35
Min SDK: 21
Max SDK:
Android Version Name: 1.8.6
Android Version Code: 86

APP COMPONENTS

Activities: 22
Services: 2
Receivers: 3
Providers: 2
Exported Activities: 1
Exported Services: 0
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-02-02 22:01:02+00:00
Valid To: 2048-06-20 22:01:02+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x1f8eec19969a2871
Hash Algorithm: sha256
md5: d5a2b3265c34a3ab19357c93ea3dd5fb
sha1: 72777d6939ef150099219bbb68c17220db28ea8e
sha256: 9fdd93b62bcc95e86ff681a401f81653e37626e83369a3e192e060f2a3ca147d
sha512: 36af4dbe2260bddfc55b3b596e1ce3570b3ef593d91cff4a14651817ed12668723c645bd9d0de2d61a52110a4ab7f7932459e809222cdad6cd6dafb0d52d13ac
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 62ed6719b849db049da83f72baabc7d8f63930bced2249c4c3c6d24c230219a6
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.WRITE_CLIPS	unknown	Unknown permission	Unknown permission from android reference
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
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.INTERACT_ACROSS_USERS	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
com.emanuelef.remote_capture.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
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.

APKID ANALYSIS

FILE	DETAILS

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

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 1

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

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 3 | 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	Activity (com.emanuelef.remote_capture.activities.CaptureCtrl) 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
4	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
				cat/ereza/customactivityoncrash/CustomActivityOnCrash.java cat/ereza/customactivityoncrash/provider/CaocInitProvider.java com/emanuelef/remote_capture/ActionReceiver.java com/emanuelef/remote_capture/AppsLoader.java com/emanuelef/remote_capture/AppsResolver.java com/emanuelef/remote_capture/Billing.java com/emanuelef/remote_capture/Blacklists.java com/emanuelef/remote_capture/BootReceiver.java com/emanuelef/remote_capture/CaptureHelper.java com/emanuelef/remote_capture/CaptureService.java com/emanuelef/remote_capture/Cidr.java com/emanuelef/remote_capture/ConnectionsRegister.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/emanuelef/remote_capture/Geolocation.java com/emanuelef/remote_capture/HTTPReassembly.java com/emanuelef/remote_capture/Log.java com/emanuelef/remote_capture/MitmAddon.java com/emanuelef/remote_capture/MitmReceiver.java com/emanuelef/remote_capture/PCAPdroid.java com/emanuelef/remote_capture/PersistableUriPermission.java com/emanuelef/remote_capture/Utils.java com/emanuelef/remote_capture/VpnReconnectService.java com/emanuelef/remote_capture/activities/AboutActivity.java com/emanuelef/remote_capture/activities/AppDetailsActivity.java com/emanuelef/remote_capture/activities/AppFilterActivity.java com/emanuelef/remote_capture/activities/CaptureCtrl.java com/emanuelef/remote_capture/activities/ConnectionDetailsActivity.java com/emanuelef/remote_capture/activities/EditListActivity.java com/emanuelef/remote_capture/activities/FirewallActivity.java com/emanuelef/remote_capture/activities/LogviewActivity.java com/emanuelef/remote_capture/activities/MainActivity.java com/emanuelef/remote_capture/activities/MalwareDetection.java com/emanuelef/remote_capture/activities/OnBoardingActivity.java com/emanuelef/remote_capture/activities/prefs/SettingsActivity.java com/emanuelef/remote_capture/activities/prefs/VpnExemptionsActivity.java com/emanuelef/remote_capture/adapters/AppsTogglesAdapter.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/emanuelef/remote_capture/adapters/ConnectionsAdapter.java com/emanuelef/remote_capture/adapters/PayloadAdapter.java com/emanuelef/remote_capture/fragments/AppsFragment.java com/emanuelef/remote_capture/fragments/AppsToggles.java com/emanuelef/remote_capture/fragments/BlacklistsFragment.java com/emanuelef/remote_capture/fragments/ConnectionPayload.java com/emanuelef/remote_capture/fragments/ConnectionsFragment.java com/emanuelef/remote_capture/fragments/EditListFragment.java com/emanuelef/remote_capture/fragments/FirewallStatus.java com/emanuelef/remote_capture/fragments/StatusFragment.java com/emanuelef/remote_capture/fragments/mitmwizard/InstallCertificate.java com/emanuelef/remote_capture/fragments/prefs/GeoipSettings.java com/emanuelef/remote_capture/fragments/prefs/PortMapFragment.java com/emanuelef/remote_capture/model/AppDescriptor.java com/emanuelef/remote_capture/model/Blocklist.java com/emanuelef/remote_capture/model/MatchList.java com/emanuelef/remote_capture/pcap_dump/FileDumper.java com/emanuelef/remote_capture/pcap_dump/HTTPServer.java com/emanuelef/remote_capture/views/AppSelectDialog.java com/github/appintro/internal/LogHelper.java com/haipq/android/flagkit/FlagImageView.java org/brotli/dec/IntReader.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/emanuelef/remote_capture/Billing.java
3	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/emanuelef/remote_capture/Billing.java
4	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/emanuelef/remote_capture/Billing.java com/emanuelef/remote_capture/PersistableUriPermission.java com/emanuelef/remote_capture/activities/ConnectionDetailsActivity.java com/emanuelef/remote_capture/model/Prefs.java
5	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/emanuelef/remote_capture/CaptureService.java com/emanuelef/remote_capture/Utils.java com/emanuelef/remote_capture/fragments/prefs/PortMapFragment.java com/emanuelef/remote_capture/model/CaptureSettings.java com/emanuelef/remote_capture/model/Prefs.java
6	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/emanuelef/remote_capture/Utils.java j$/util/concurrent/ThreadLocalRandom.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	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/emanuelef/remote_capture/Utils.java
8	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	cat/ereza/customactivityoncrash/activity/DefaultErrorActivity.java com/emanuelef/remote_capture/Utils.java com/emanuelef/remote_capture/activities/ErrorActivity.java com/emanuelef/remote_capture/fragments/ConnectionOverview.java

SHARED LIBRARY BINARY ANALYSIS

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

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

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	x86_64/libushark.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', '__strlen_chk', '__memcpy_chk', '__memset_chk', '__read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86_64/libndpi.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', '__strrchr_chk', '__strlen_chk', '__strcat_chk', '__strncpy_chk', '__vsprintf_chk', '__memset_chk']	True info Symbols are stripped.

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

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	x86/libushark.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', '__strlen_chk', '__memcpy_chk', '__memset_chk', '__read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	x86/libndpi.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', '__strrchr_chk', '__strlen_chk', '__strcat_chk', '__strncpy_chk', '__vsprintf_chk', '__memset_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	armeabi-v7a/libcapture.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', '__FD_SET_chk', '__FD_ISSET_chk', '__strchr_chk', '__vsprintf_chk', '__memcpy_chk', '__strlen_chk', '__strcat_chk', '__FD_CLR_chk', '__read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	armeabi-v7a/libushark.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', '__strlen_chk', '__memcpy_chk', '__memset_chk', '__read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	armeabi-v7a/libndpi.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', '__strrchr_chk', '__strlen_chk', '__strcat_chk', '__strncpy_chk', '__vsprintf_chk', '__memset_chk']	True info Symbols are stripped.

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

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	arm64-v8a/libushark.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', '__strlen_chk', '__memcpy_chk', '__memset_chk', '__read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	arm64-v8a/libndpi.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', '__strrchr_chk', '__strlen_chk', '__strcat_chk', '__strncpy_chk', '__vsprintf_chk', '__memset_chk']	True info Symbols are stripped.

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

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	x86_64/libushark.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', '__strlen_chk', '__memcpy_chk', '__memset_chk', '__read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	x86_64/libndpi.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', '__strrchr_chk', '__strlen_chk', '__strcat_chk', '__strncpy_chk', '__vsprintf_chk', '__memset_chk']	True info Symbols are stripped.

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

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	x86/libushark.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', '__strlen_chk', '__memcpy_chk', '__memset_chk', '__read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	x86/libndpi.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', '__strrchr_chk', '__strlen_chk', '__strcat_chk', '__strncpy_chk', '__vsprintf_chk', '__memset_chk']	True info Symbols are stripped.

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	armeabi-v7a/libcapture.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', '__FD_SET_chk', '__FD_ISSET_chk', '__strchr_chk', '__vsprintf_chk', '__memcpy_chk', '__strlen_chk', '__strcat_chk', '__FD_CLR_chk', '__read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
27	armeabi-v7a/libushark.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', '__strlen_chk', '__memcpy_chk', '__memset_chk', '__read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
28	armeabi-v7a/libndpi.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', '__strrchr_chk', '__strlen_chk', '__strcat_chk', '__strncpy_chk', '__vsprintf_chk', '__memset_chk']	True info Symbols are stripped.

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

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

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
31	arm64-v8a/libushark.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', '__strlen_chk', '__memcpy_chk', '__memset_chk', '__read_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
32	arm64-v8a/libndpi.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', '__strrchr_chk', '__strlen_chk', '__strcat_chk', '__strncpy_chk', '__vsprintf_chk', '__memset_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/emanuelef/remote_capture/CaptureService.java com/emanuelef/remote_capture/Geolocation.java com/emanuelef/remote_capture/Utils.java com/emanuelef/remote_capture/activities/MainActivity.java
00013	Read file and put it into a stream	file	com/emanuelef/remote_capture/Geolocation.java com/emanuelef/remote_capture/Utils.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/emanuelef/remote_capture/CaptureService.java com/emanuelef/remote_capture/PersistableUriPermission.java com/emanuelef/remote_capture/Utils.java com/emanuelef/remote_capture/activities/ErrorActivity.java com/emanuelef/remote_capture/activities/MainActivity.java com/emanuelef/remote_capture/activities/prefs/EditCtrlPermissions.java com/emanuelef/remote_capture/fragments/BlacklistsFragment.java com/emanuelef/remote_capture/fragments/ConnectionOverview.java com/emanuelef/remote_capture/fragments/FirewallStatus.java com/emanuelef/remote_capture/fragments/MalwareStatusFragment.java com/emanuelef/remote_capture/fragments/mitmwizard/InstallAddon.java
00035	Query the list of the installed packages	reflection	com/emanuelef/remote_capture/Utils.java
00192	Get messages in the SMS inbox	sms	com/emanuelef/remote_capture/Utils.java
00130	Get the current WIFI information	wifi collection	com/emanuelef/remote_capture/Utils.java
00121	Create a directory	file command	com/emanuelef/remote_capture/Utils.java
00024	Write file after Base64 decoding	reflection file	com/emanuelef/remote_capture/Utils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00012	Read data and put it into a buffer stream	file	com/emanuelef/remote_capture/Utils.java
00134	Get the current WiFi IP address	wifi collection	com/emanuelef/remote_capture/Utils.java
00125	Check if the given file path exist	file	com/emanuelef/remote_capture/Utils.java com/emanuelef/remote_capture/activities/MainActivity.java
00112	Get the date of the calendar event	collection calendar	com/emanuelef/remote_capture/Utils.java
00094	Connect to a URL and read data from it	command network	com/emanuelef/remote_capture/Utils.java
00036	Get resource file from res/raw directory	reflection	com/emanuelef/remote_capture/CaptureService.java com/emanuelef/remote_capture/Utils.java
00091	Retrieve data from broadcast	collection	com/emanuelef/remote_capture/model/CaptureSettings.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/emanuelef/remote_capture/activities/ErrorActivity.java
00162	Create InetSocketAddress object and connecting to it	socket	com/emanuelef/remote_capture/pcap_dump/TCPDumper.java
00163	Create new Socket and connecting to it	socket	com/emanuelef/remote_capture/pcap_dump/TCPDumper.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	6/25	android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, 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
www.language	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.wireshark.org	ok	**IP:** 104.26.10.240 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.manifestations	ok	No Geolocation information available.
etherx.jabber.org	ok	**IP:** 208.68.163.210 **Country:** United States of America **Region:** Iowa **City:** Monticello **Latitude:** 42.238514 **Longitude:** -91.189705 **View:** Google Map
www.a	ok	No Geolocation information available.
play.google.com	ok	**IP:** 142.251.30.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
t.me	ok	**IP:** 149.154.167.99 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Lowestoft **Latitude:** 52.475201 **Longitude:** 1.751590 **View:** Google Map
www.hortcut	ok	No Geolocation information available.
pcapdroid.org	ok	**IP:** 185.53.129.106 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
rules.emergingthreats.net	ok	**IP:** 34.193.191.139 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.crossfire	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
emanuele-f.github.io	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.googleorganizationautocompleterequirementsconservative	ok	No Geolocation information available.
www.recent	ok	No Geolocation information available.
www.years	ok	No Geolocation information available.
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
search.arin.net	ok	**IP:** 192.136.136.47 **Country:** United States of America **Region:** Virginia **City:** Centreville **Latitude:** 38.851059 **Longitude:** -77.462257 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.risktabsprev10pxrise25pxblueding300ballfordearnwildbox.fairlackverspairjunetechifpickevil	ok	No Geolocation information available.
www.css	ok	No Geolocation information available.
www.style	ok	**IP:** 99.83.155.228 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
.jpg	ok	No Geolocation information available.
dontkillmyapp.com	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.c	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.icon	ok	No Geolocation information available.
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
www.in	ok	No Geolocation information available.
www.interpretation	ok	No Geolocation information available.
www.world	ok	**IP:** 99.83.155.228 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.606209 **Longitude:** -122.332069 **View:** Google Map
download.db-ip.com	ok	**IP:** 104.26.4.15 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
.css	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.text-decoration	ok	No Geolocation information available.
www.wencodeuricomponent	ok	No Geolocation information available.
www.speedtest.net	ok	**IP:** 104.17.147.22 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
jabber.org	ok	**IP:** 54.39.46.213 **Country:** Canada **Region:** Quebec **City:** Montreal **Latitude:** 45.508839 **Longitude:** -73.587807 **View:** Google Map
raw.githubusercontent.com	ok	**IP:** 185.199.108.133 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

EMAILS

EMAIL	FILE
black.silver@hotmail.it	com/emanuelef/remote_capture/activities/ErrorActivity.java
yay@y.u5vcghyy w9oi_2nhels4u@dlilycclglhl.5jlcg_bqh 6h@fo.lwft wireshark-dev@wireshark.org gerald@wireshark.org	apktool_out/lib/x86_64/libushark.so
wireshark-dev@wireshark.org gerald@wireshark.org	apktool_out/lib/x86/libushark.so
wireshark-dev@wireshark.org gerald@wireshark.org	apktool_out/lib/armeabi-v7a/libushark.so
wireshark-dev@wireshark.org gerald@wireshark.org	apktool_out/lib/arm64-v8a/libushark.so
yay@y.u5vcghyy w9oi_2nhels4u@dlilycclglhl.5jlcg_bqh 6h@fo.lwft wireshark-dev@wireshark.org gerald@wireshark.org	lib/x86_64/libushark.so
wireshark-dev@wireshark.org gerald@wireshark.org	lib/x86/libushark.so
wireshark-dev@wireshark.org gerald@wireshark.org	lib/armeabi-v7a/libushark.so
wireshark-dev@wireshark.org gerald@wireshark.org	lib/arm64-v8a/libushark.so

HARDCODED SECRETS

POSSIBLE SECRETS
"username" : "Benutzername"
"username" : "Nazwa"
"password" : "Sandi"
"requesting_unlock_token" : "□□□□□□□□□□□□□"
"socks5_auth_summary" : "□□□□□□□□□□□□□□□□□□□"
"username" : "□□□"
"password" : "Contraseña"
"username" : "■■■■■■■■■■"
"password" : "Пароль"
"password" : "■■■■■■■■■■■"
"username" : "Username"
"password" : "Password"
"password" : "Hasło"
"password" : "Parola"

POSSIBLE SECRETS
"password" : "□□"
"password" : "Şifrə"
"password" : "Passwort"
ME4wEAYHKoZIzj0CAQYFK4EEACEDOgAE6cS1N1P0kaiuxq0g70OVVE0uIOD+t809Etg3k2h11k8uNvfkx3mL1HTjQyzSfdueyY4DqTW7+sk=
EE953D4F988C8AC17575DFFAA1E3BBCE2E29E81D
511140392BFF2CFB4BD825895DD6510CE1807F6D
72777D6939EF150099219BBB68C17220DB28EA8E

PLAYSTORE INFORMATION

Title: PCAPdroid - network monitor

Score: 4.49 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Tools **Play Store URL:** com.emanuelef.remote_capture

Developer Details: Emanuele Faranda, Emanuele+Faranda, None, https://emanuele-f.github.io/PCAPdroid, black.silver@hotmail.it,

Release Date: Oct 26, 2019 **Privacy Policy:** Privacy link

Description:

PCAPdroid is a privacy-friendly open source app which lets you track, analyze and block the connections made by the other apps in your device. It also allows you to export a PCAP dump of the traffic, extract metadata and much more! PCAPdroid simulates a VPN in order to capture the network traffic without root. It does not use a remote VPN server. All the data is processed locally on the device. Features: - Log and examine the connections made by user and system apps - Extract the SNI, DNS query, HTTP URL and the remote IP address - Inspect HTTP requests and replies thanks to the built-in decoders - Inspect the full connections payload as hexdump/text and export it - Decrypt the HTTPS/TLS traffic and export the SSLKEYLOGFILE - Dump the traffic to a PCAP file, download it from a browser, or stream it to a remote receiver for real time analysis (e.g. wireshark) - Create rules to filter out the good traffic and easily spot anomalies - Identify the country and ASN of remote server via offline db lookups - On rooted devices, capture the traffic while other VPN apps are running Paid features: - Firewall: create rules to block individual apps, domains and IP

addresses - Malware detection: detect malicious connections by using third-party blacklists If you plan to use PCAPdroid to perform packet analysis, please check out the specific section of the manual. Join the PCAPdroid community on telegram to discuss and receive updates on the latest features.

SCAN LOGS

Timestamp	Event	Error
2025-08-01 00:58:49	Generating Hashes	OK
2025-08-01 00:58:49	Extracting APK	OK
2025-08-01 00:58:49	Unzipping	OK
2025-08-01 00:58:53	Parsing APK with androguard	OK
2025-08-01 00:59:03	Extracting APK features using aapt/aapt2	OK
2025-08-01 00:59:03	Getting Hardcoded Certificates/Keystores	OK
2025-08-01 00:59:18	Parsing AndroidManifest.xml	OK
2025-08-01 00:59:18	Extracting Manifest Data	OK

2025-08-01 00:59:18	Manifest Analysis Started	OK
2025-08-01 00:59:19	Performing Static Analysis on: PCAPdroid (com.emanuelef.remote_capture)	OK
2025-08-01 00:59:20	Fetching Details from Play Store: com.emanuelef.remote_capture	OK
2025-08-01 00:59:21	Checking for Malware Permissions	OK
2025-08-01 00:59:21	Fetching icon path	OK
2025-08-01 00:59:21	Library Binary Analysis Started	OK
2025-08-01 00:59:21	Analyzing apktool_out/lib/x86_64/libpcapd.so	OK
2025-08-01 00:59:21	Analyzing apktool_out/lib/x86_64/libcapture.so	OK
2025-08-01 00:59:21	Analyzing apktool_out/lib/x86_64/libushark.so	OK
2025-08-01 00:59:22	Analyzing apktool_out/lib/x86_64/libndpi.so	OK
2025-08-01 00:59:22	Analyzing apktool_out/lib/x86/libpcapd.so	OK

2025-08-01 00:59:22	Analyzing apktool_out/lib/x86/libcapture.so	OK
2025-08-01 00:59:22	Analyzing apktool_out/lib/x86/libushark.so	OK
2025-08-01 00:59:22	Analyzing apktool_out/lib/x86/libndpi.so	OK
2025-08-01 00:59:23	Analyzing apktool_out/lib/armeabi-v7a/libpcapd.so	OK
2025-08-01 00:59:23	Analyzing apktool_out/lib/armeabi-v7a/libcapture.so	OK
2025-08-01 00:59:23	Analyzing apktool_out/lib/armeabi-v7a/libushark.so	OK
2025-08-01 00:59:23	Analyzing apktool_out/lib/armeabi-v7a/libndpi.so	OK
2025-08-01 00:59:23	Analyzing apktool_out/lib/arm64-v8a/libpcapd.so	OK
2025-08-01 00:59:23	Analyzing apktool_out/lib/arm64-v8a/libcapture.so	OK
2025-08-01 00:59:23	Analyzing apktool_out/lib/arm64-v8a/libushark.so	OK
2025-08-01 00:59:23	Analyzing apktool_out/lib/arm64-v8a/libndpi.so	OK

2025-08-01 00:59:23	Analyzing lib/x86_64/libpcapd.so	OK
2025-08-01 00:59:23	Analyzing lib/x86_64/libcapture.so	OK
2025-08-01 00:59:23	Analyzing lib/x86_64/libushark.so	OK
2025-08-01 00:59:23	Analyzing lib/x86_64/libndpi.so	OK
2025-08-01 00:59:24	Analyzing lib/x86/libpcapd.so	OK
2025-08-01 00:59:24	Analyzing lib/x86/libcapture.so	OK
2025-08-01 00:59:24	Analyzing lib/x86/libushark.so	OK
2025-08-01 00:59:24	Analyzing lib/x86/libndpi.so	OK
2025-08-01 00:59:24	Analyzing lib/armeabi-v7a/libpcapd.so	OK
2025-08-01 00:59:24	Analyzing lib/armeabi-v7a/libcapture.so	OK
2025-08-01 00:59:24	Analyzing lib/armeabi-v7a/libushark.so	OK

2025-08-01 00:59:24	Analyzing lib/armeabi-v7a/libndpi.so	OK
2025-08-01 00:59:24	Analyzing lib/arm64-v8a/libpcapd.so	OK
2025-08-01 00:59:24	Analyzing lib/arm64-v8a/libcapture.so	OK
2025-08-01 00:59:24	Analyzing lib/arm64-v8a/libushark.so	OK
2025-08-01 00:59:24	Analyzing lib/arm64-v8a/libndpi.so	OK
2025-08-01 00:59:24	Reading Code Signing Certificate	OK
2025-08-01 00:59:27	Running APKiD 2.1.5	OK
2025-08-01 00:59:32	Detecting Trackers	OK
2025-08-01 00:59:34	Decompiling APK to Java with JADX	OK
2025-08-01 01:01:03	Converting DEX to Smali	OK

2025-08-01 01:01:03	Code Analysis Started on - java_source	OK
2025-08-01 01:01:12	Android SBOM Analysis Completed	OK
2025-08-01 01:01:22	Android SAST Completed	OK
2025-08-01 01:01:22	Android API Analysis Started	OK
2025-08-01 01:01:25	Android API Analysis Completed	OK
2025-08-01 01:01:26	Android Permission Mapping Started	OK
2025-08-01 01:01:29	Android Permission Mapping Completed	OK
2025-08-01 01:01:30	Android Behaviour Analysis Started	OK
2025-08-01 01:01:33	Android Behaviour Analysis Completed	OK
2025-08-01 01:01:33	Extracting Emails and URLs from Source Code	OK
2025-08-01 01:01:35	Email and URL Extraction Completed	OK

2025-08-01 01:01:35	Extracting String data from APK	OK
2025-08-01 01:01:35	Extracting String data from SO	OK
2025-08-01 01:01:36	Extracting String data from Code	OK
2025-08-01 01:01:36	Extracting String values and entropies from Code	OK
2025-08-01 01:01:38	Performing Malware check on extracted domains	OK
2025-08-01 01:01:44	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.