



## ANDROID STATIC ANALYSIS REPORT



 BatteryDoctor (1.0)

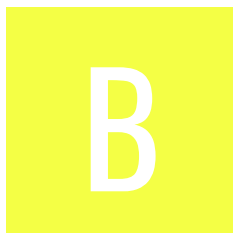
File Name: 2a78ef24571a66f16f0f153400ad518473513452a4e36c082e20fc59bba677da.apk

Package Name: com.free.powerline.batterydoctor

Scan Date: April 26, 2025, 4:34 p.m.

App Security Score: 41/100 (MEDIUM RISK)

Grade:



## FINDINGS SEVERITY

|  HIGH |  MEDIUM |  INFO |  SECURE |  HOTSPOT |
|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| 3                                                                                      | 5                                                                                        | 1                                                                                      | 1                                                                                          | 1                                                                                           |

## FILE INFORMATION

**File Name:** 2a78ef24571a66f16f0f153400ad518473513452a4e36c082e20fc59bba677da.apk

**Size:** 0.59MB

**MD5:** 015893103a16ab984c491180a53e7319

**SHA1:** 98d89b68c01c492b860e17da69c1a4aa9cd3bd2f

**SHA256:** 2a78ef24571a66f16f0f153400ad518473513452a4e36c082e20fc59bba677da

## APP INFORMATION

**App Name:** BatteryDoctor

**Package Name:** com.free.powerline.batterydoctor

**Main Activity:** com.free.powerline.batterydoctor.MainActivity

**Target SDK:** 9

**Min SDK:** 9

**Max SDK:** 19

**Android Version Name:** 1.0

**Android Version Code:** 1

## APP COMPONENTS

Activities: 1  
Services: 1  
Receivers: 1  
Providers: 0  
Exported Activities: 0  
Exported Services: 0  
Exported Receivers: 1  
Exported Providers: 0

## CERTIFICATE INFORMATION

Binary is signed  
v1 signature: True  
v2 signature: False  
v3 signature: False  
v4 signature: False  
X.509 Subject: C=CN, ST=Beijing, L=Beijing, O=mobike, OU=software, CN=mobike.com  
Signature Algorithm: rsassa\_pkcs1v15  
Valid From: 2017-06-09 03:30:05+00:00  
Valid To: 2117-05-16 03:30:05+00:00  
Issuer: C=CN, ST=Beijing, L=Beijing, O=mobike, OU=software, CN=mobike.com  
Serial Number: 0x338fd404  
Hash Algorithm: sha256  
md5: f44ff91ba587ade42e2b76541974baab  
sha1: f3d8d9d598839f4411658b77dfa5d98ad2dab3e  
sha256: 02f917129360f4a845a9a270bc5ccfd35d9aeb184e38bb32f2dca5d872a0af18  
sha512: 041d13e76b3ef795f7085e433290dc0cd5681b5189628f55abf5d8cf5a7e96ea67859574be197fd9f30bfd68ad7bee93c18465c7d011fc27d584314887750808  
Found 1 unique certificates

## APPLICATION PERMISSIONS

| PERMISSION                        | STATUS    | INFO                          | DESCRIPTION                                                                                                                 |
|-----------------------------------|-----------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| android.permission.WRITE_SETTINGS | dangerous | modify global system settings | Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration. |

| PERMISSION                                   | STATUS            | INFO                                         | DESCRIPTION                                                                                                                                                                                                                                      |
|----------------------------------------------|-------------------|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| android.permission.BLUETOOTH                 | normal            | create Bluetooth connections                 | Allows applications to connect to paired bluetooth devices.                                                                                                                                                                                      |
| android.permission.BLUETOOTH_ADMIN           | normal            | bluetooth administration                     | Allows applications to discover and pair bluetooth devices.                                                                                                                                                                                      |
| android.permission.KILL_BACKGROUND_PROCESSES | normal            | kill background processes                    | Allows an application to kill background processes of other applications, even if memory is not low.                                                                                                                                             |
| android.permission.CLEAR_APP_CACHE           | SignatureOrSystem | delete all application cache data            | Allows an application to free phone storage by deleting files in application cache directory. Access is usually very restricted to system process.                                                                                               |
| android.permission.INTERNET                  | normal            | full Internet access                         | Allows an application to create network sockets.                                                                                                                                                                                                 |
| android.permission.READ_PHONE_STATE          | dangerous         | read phone state and identity                | Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on. |
| android.permission.WRITE_EXTERNAL_STORAGE    | dangerous         | read/modify/delete external storage contents | Allows an application to write to external storage.                                                                                                                                                                                              |
| android.permission.MOUNT_UNMOUNT_FILESYSTEMS | dangerous         | mount and unmount file systems               | Allows the application to mount and unmount file systems for removable storage.                                                                                                                                                                  |
| 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.                                                                                                                                                                         |

| PERMISSION                              | STATUS    | INFO                        | DESCRIPTION                                                                                                                                                                                                       |
|-----------------------------------------|-----------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| android.permission.SYSTEM_ALERT_WINDOW  | dangerous | display system-level alerts | Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.                                                                                          |
| android.permission.READ_LOGS            | dangerous | read sensitive log data     | Allows an application to read from the system's various log files. This allows it to discover general information about what you are doing with the phone, potentially including personal or private information. |
| android.permission.RECEIVE_SMS          | dangerous | receive SMS                 | Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.                                                              |
| android.permission.WRITE_SMS            | dangerous | edit SMS or MMS             | Allows application to write to SMS messages stored on your phone or SIM card. Malicious applications may delete your messages.                                                                                    |
| android.permission.READ_SMS             | dangerous | read SMS or MMS             | Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.                                                                             |
| android.permission.UPDATE_APP_OPS_STATS | unknown   | Unknown permission          | Unknown permission from android reference                                                                                                                                                                         |
| android.provider.Telephony.SMS_RECEIVED | unknown   | Unknown permission          | Unknown permission from android reference                                                                                                                                                                         |
| android.permission.CHANGE_WIFI_STATE    | normal    | change Wi-Fi status         | Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.                                                                                     |
| android.permission.CHANGE_NETWORK_STATE | normal    | change network connectivity | Allows applications to change network connectivity state.                                                                                                                                                         |
| android.permission.SEND_SMS             | dangerous | send SMS messages           | Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.                                                                                 |

## APKID ANALYSIS

| FILE        | DETAILS           |                        |
|-------------|-------------------|------------------------|
| classes.dex | FINDINGS          | DETAILS                |
|             | Compiler          | dx (possible dexmerge) |
|             | Manipulator Found | dexmerge               |

## NETWORK SECURITY

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

## CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

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

# Q 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<br>Android 2.3-2.3.2,<br>[minSdk=9] | 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<br>[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  | Broadcast Receiver (com.x.y.b) is not Protected. An intent-filter exists.                          | warning  | A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.                      |
| 4  | High Intent Priority (1000) - {1} Hit(s)<br>[android:priority]                                     | warning  | By setting an intent priority higher than another intent, the app effectively overrides other requests.                                                                                                                                                           |

## </> CODE ANALYSIS

HIGH: 1 | WARNING: 2 | INFO: 1 | SECURE: 0 | SUPPRESSED: 0

| NO | ISSUE                                                                                                     | SEVERITY | STANDARDS                                                                                                                      | FILES                                             |
|----|-----------------------------------------------------------------------------------------------------------|----------|--------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| 1  | <a href="#">Debug configuration enabled.</a><br><a href="#">Production builds must not be debuggable.</a> | high     | CWE: CWE-919: Weaknesses in Mobile Applications<br>OWASP Top 10: M1: Improper Platform Usage<br>OWASP MASVS: MSTG-RESILIENCE-2 | com/free/powerline/batterydoctor/BuildConfig.java |

| NO | ISSUE                                                                                                  | SEVERITY | STANDARDS                                                                                                                         | FILES                                                                                                        |
|----|--------------------------------------------------------------------------------------------------------|----------|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| 2  | <a href="#">The App logs information. Sensitive information should never be logged.</a>                | info     | CWE: CWE-532: Insertion of Sensitive Information into Log File<br>OWASP MASVS: MSTG-STORAGE-3                                     | com/free/powerline/batterydoctor/HomeWatcher.java<br>com/nineoldandroids/animation/PropertyValuesHolder.java |
| 3  | <a href="#">Files may contain hardcoded sensitive information like usernames, passwords, keys etc.</a> | warning  | CWE: CWE-312: Cleartext Storage of Sensitive Information<br>OWASP Top 10: M9: Reverse Engineering<br>OWASP MASVS: MSTG-STORAGE-14 | com/free/powerline/batterydoctor/HomeWatcher.java                                                            |
| 4  | <a href="#">The App uses an insecure Random Number Generator.</a>                                      | warning  | CWE: CWE-330: Use of Insufficiently Random Values<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-6    | com/free/powerline/batterydoctor/MainActivity.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  | arm64-v8a/libwapCore.so | <p>True<br/><a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO)<br/><a href="#">info</a></p> <p>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.</p> | <p>False<br/><a href="#">high</a></p> <p>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.</p> | <p>Full RELRO<br/><a href="#">info</a></p> <p>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.</p> | <p>None<br/><a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None<br/><a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p> | <p>False<br/><a href="#">warning</a></p> <p>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.</p> | <p>True<br/><a href="#">info</a></p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT         | NX                                                                                                                                                                | PIE                                                                                                                                                                                                                                                  | STACK CANARY                                                                                                                                                                                                                                                                                                                              | RELRO                                                                                                                                                                                                                                                    | RPATH                                                                                                   | RUNPATH                                                                           | FORTIFY                                                                                                                                                                                                                                                                                                                                            | SYMBOLS STRIPPED                                                  |
|----|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 2  | armeabi/libwapCore.so | <p>True<br/><a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO)<br/><a href="#">info</a></p> <p>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.</p> | <p>False<br/><a href="#">high</a></p> <p>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.</p> | <p>Full RELRO<br/><a href="#">info</a></p> <p>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.</p> | <p>None<br/><a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None<br/><a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p> | <p>False<br/><a href="#">warning</a></p> <p>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.</p> | <p>True<br/><a href="#">info</a></p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT     | NX                                                                                                                                                                | PIE                                                                                                                                                                                                                                                  | STACK CANARY                                                                                                                                                                                                                                                                                | RELRO                                                                                                                                                                                                                                                    | RPATH                                                                                                   | RUNPATH                                                                           | FORTIFY                                                                                                                                                                                                                                                                                                                                            | SYMBOLS STRIPPED                                                  |
|----|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 3  | x86/libwapCore.so | <p>True<br/><a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO)<br/><a href="#">info</a></p> <p>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.</p> | <p>True<br/><a href="#">info</a></p> <p>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.</p> | <p>Full RELRO<br/><a href="#">info</a></p> <p>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.</p> | <p>None<br/><a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None<br/><a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p> | <p>False<br/><a href="#">warning</a></p> <p>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.</p> | <p>True<br/><a href="#">info</a></p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT             | NX                                                                                                                                                                | PIE                                                                                                                                                                                                                                                  | STACK CANARY                                                                                                                                                                                                                                                                                                                              | RELRO                                                                                                                                                                                                                                                    | RPATH                                                                                                   | RUNPATH                                                                           | FORTIFY                                                                                                                                                                                                                                                                                                                                            | SYMBOLS STRIPPED                                                  |
|----|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 4  | armeabi-v7a/libwapCore.so | <p>True<br/><a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO)<br/><a href="#">info</a></p> <p>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.</p> | <p>False<br/><a href="#">high</a></p> <p>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.</p> | <p>Full RELRO<br/><a href="#">info</a></p> <p>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.</p> | <p>None<br/><a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None<br/><a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p> | <p>False<br/><a href="#">warning</a></p> <p>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.</p> | <p>True<br/><a href="#">info</a></p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT        | NX                                                                                                                                                                | PIE                                                                                                                                                                                                                                                  | STACK CANARY                                                                                                                                                                                                                                                                                                                              | RELRO                                                                                                                                                                                                                                                    | RPATH                                                                                                   | RUNPATH                                                                           | FORTIFY                                                                                                                                                                                                                                                                                                                                            | SYMBOLS STRIPPED                                                  |
|----|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 5  | x86_64/libwapCore.so | <p>True<br/><a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO)<br/><a href="#">info</a></p> <p>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.</p> | <p>False<br/><a href="#">high</a></p> <p>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.</p> | <p>Full RELRO<br/><a href="#">info</a></p> <p>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.</p> | <p>None<br/><a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None<br/><a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p> | <p>False<br/><a href="#">warning</a></p> <p>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.</p> | <p>True<br/><a href="#">info</a></p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT           | NX                                                                                                                                                                | PIE                                                                                                                                                                                                                                                  | STACK CANARY                                                                                                                                                                                                                                                                                                                              | RELRO                                                                                                                                                                                                                                                    | RPATH                                                                                                   | RUNPATH                                                                           | FORTIFY                                                                                                                                                                                                                                                                                                                                            | SYMBOLS STRIPPED                                                  |
|----|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 6  | arm64-v8a/libwapCore.so | <p>True<br/><a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO)<br/><a href="#">info</a></p> <p>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.</p> | <p>False<br/><a href="#">high</a></p> <p>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.</p> | <p>Full RELRO<br/><a href="#">info</a></p> <p>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.</p> | <p>None<br/><a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None<br/><a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p> | <p>False<br/><a href="#">warning</a></p> <p>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.</p> | <p>True<br/><a href="#">info</a></p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT         | NX                                                                                                                                                                | PIE                                                                                                                                                                                                                                                  | STACK CANARY                                                                                                                                                                                                                                                                                                                              | RELRO                                                                                                                                                                                                                                                    | RPATH                                                                                                   | RUNPATH                                                                           | FORTIFY                                                                                                                                                                                                                                                                                                                                            | SYMBOLS STRIPPED                                                  |
|----|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 7  | armeabi/libwapCore.so | <p>True<br/><a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO)<br/><a href="#">info</a></p> <p>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.</p> | <p>False<br/><a href="#">high</a></p> <p>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.</p> | <p>Full RELRO<br/><a href="#">info</a></p> <p>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.</p> | <p>None<br/><a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None<br/><a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p> | <p>False<br/><a href="#">warning</a></p> <p>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.</p> | <p>True<br/><a href="#">info</a></p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT     | NX                                                                                                                                                                | PIE                                                                                                                                                                                                                                                  | STACK CANARY                                                                                                                                                                                                                                                                                | RELRO                                                                                                                                                                                                                                                    | RPATH                                                                                                   | RUNPATH                                                                           | FORTIFY                                                                                                                                                                                                                                                                                                                                            | SYMBOLS STRIPPED                                                  |
|----|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 8  | x86/libwapCore.so | <p>True<br/><a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO)<br/><a href="#">info</a></p> <p>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.</p> | <p>True<br/><a href="#">info</a></p> <p>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.</p> | <p>Full RELRO<br/><a href="#">info</a></p> <p>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.</p> | <p>None<br/><a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None<br/><a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p> | <p>False<br/><a href="#">warning</a></p> <p>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.</p> | <p>True<br/><a href="#">info</a></p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT             | NX                                                                                                                                                                | PIE                                                                                                                                                                                                                                                  | STACK CANARY                                                                                                                                                                                                                                                                                                                              | RELRO                                                                                                                                                                                                                                                    | RPATH                                                                                                   | RUNPATH                                                                           | FORTIFY                                                                                                                                                                                                                                                                                                                                            | SYMBOLS STRIPPED                                                  |
|----|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 9  | armeabi-v7a/libwapCore.so | <p>True<br/><a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO)<br/><a href="#">info</a></p> <p>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.</p> | <p>False<br/><a href="#">high</a></p> <p>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.</p> | <p>Full RELRO<br/><a href="#">info</a></p> <p>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.</p> | <p>None<br/><a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None<br/><a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p> | <p>False<br/><a href="#">warning</a></p> <p>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.</p> | <p>True<br/><a href="#">info</a></p> <p>Symbols are stripped.</p> |

| NO | SHARED OBJECT        | NX                                                                                                                                                                | PIE                                                                                                                                                                                                                                                  | STACK CANARY                                                                                                                                                                                                                                                                                                                              | RELRO                                                                                                                                                                                                                                                    | RPATH                                                                                                   | RUNPATH                                                                           | FORTIFY                                                                                                                                                                                                                                                                                                                                            | SYMBOLS STRIPPED                                                  |
|----|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 10 | x86_64/libwapCore.so | <p>True<br/><a href="#">info</a></p> <p>The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p> | <p>Dynamic Shared Object (DSO)<br/><a href="#">info</a></p> <p>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.</p> | <p>False<br/><a href="#">high</a></p> <p>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.</p> | <p>Full RELRO<br/><a href="#">info</a></p> <p>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.</p> | <p>None<br/><a href="#">info</a></p> <p>The binary does not have run-time search path or RPATH set.</p> | <p>None<br/><a href="#">info</a></p> <p>The binary does not have RUNPATH set.</p> | <p>False<br/><a href="#">warning</a></p> <p>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.</p> | <p>True<br/><a href="#">info</a></p> <p>Symbols are stripped.</p> |

# NIAP ANALYSIS v1.3

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

## ABUSED PERMISSIONS

| TYPE                     | MATCHES | PERMISSIONS                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Malware Permissions      | 10/25   | android.permission.WRITE_SETTINGS, android.permission.INTERNET, android.permission.READ_PHONE_STATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.RECEIVE_SMS, android.permission.READ_SMS, android.permission.SEND_SMS |
| Other Common Permissions | 5/44    | android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN, android.permission.WRITE_SMS, android.permission.CHANGE_WIFI_STATE, android.permission.CHANGE_NETWORK_STATE                                                                                                                                                                                   |

### Malware Permissions:

Top permissions that are widely abused by known malware.

### Other Common Permissions:

Permissions that are commonly abused by known malware.

## SCAN LOGS

| Timestamp           | Event             | Error |
|---------------------|-------------------|-------|
| 2025-04-26 16:34:26 | Generating Hashes | OK    |

|                     |                                                                                 |    |
|---------------------|---------------------------------------------------------------------------------|----|
| 2025-04-26 16:34:26 | Extracting APK                                                                  | OK |
| 2025-04-26 16:34:26 | Unzipping                                                                       | OK |
| 2025-04-26 16:34:26 | Parsing APK with androguard                                                     | OK |
| 2025-04-26 16:34:26 | Extracting APK features using aapt/aapt2                                        | OK |
| 2025-04-26 16:34:26 | Getting Hardcoded Certificates/Keystores                                        | OK |
| 2025-04-26 16:34:27 | Parsing AndroidManifest.xml                                                     | OK |
| 2025-04-26 16:34:27 | Extracting Manifest Data                                                        | OK |
| 2025-04-26 16:34:27 | Manifest Analysis Started                                                       | OK |
| 2025-04-26 16:34:27 | Performing Static Analysis on: BatteryDoctor (com.free.powerline.batterydoctor) | OK |
| 2025-04-26 16:34:27 | Fetching Details from Play Store: com.free.powerline.batterydoctor              | OK |
| 2025-04-26 16:34:28 | Checking for Malware Permissions                                                | OK |

|                     |                                                     |    |
|---------------------|-----------------------------------------------------|----|
| 2025-04-26 16:34:28 | Fetching icon path                                  | OK |
| 2025-04-26 16:34:28 | Library Binary Analysis Started                     | OK |
| 2025-04-26 16:34:28 | Analyzing apktool_out/lib/arm64-v8a/libwapCore.so   | OK |
| 2025-04-26 16:34:28 | Analyzing apktool_out/lib/armeabi/libwapCore.so     | OK |
| 2025-04-26 16:34:28 | Analyzing apktool_out/lib/x86/libwapCore.so         | OK |
| 2025-04-26 16:34:28 | Analyzing apktool_out/lib/armeabi-v7a/libwapCore.so | OK |
| 2025-04-26 16:34:28 | Analyzing apktool_out/lib/x86_64/libwapCore.so      | OK |
| 2025-04-26 16:34:28 | Analyzing lib/arm64-v8a/libwapCore.so               | OK |
| 2025-04-26 16:34:28 | Analyzing lib/armeabi/libwapCore.so                 | OK |
| 2025-04-26 16:34:28 | Analyzing lib/x86/libwapCore.so                     | OK |
| 2025-04-26 16:34:28 | Analyzing lib/armeabi-v7a/libwapCore.so             | OK |

|                     |                                        |    |
|---------------------|----------------------------------------|----|
| 2025-04-26 16:34:28 | Analyzing lib/x86_64/libwapCore.so     | OK |
| 2025-04-26 16:34:28 | Reading Code Signing Certificate       | OK |
| 2025-04-26 16:34:28 | Running APKiD 2.1.5                    | OK |
| 2025-04-26 16:34:29 | Updating Trackers Database....         | OK |
| 2025-04-26 16:34:29 | Detecting Trackers                     | OK |
| 2025-04-26 16:34:29 | Decompiling APK to Java with JADX      | OK |
| 2025-04-26 16:34:31 | Converting DEX to Smali                | OK |
| 2025-04-26 16:34:31 | Code Analysis Started on - java_source | OK |
| 2025-04-26 16:34:31 | Android SBOM Analysis Completed        | OK |
| 2025-04-26 16:34:31 | Android SAST Completed                 | OK |
| 2025-04-26 16:34:31 | Android API Analysis Started           | OK |

|                     |                                                  |    |
|---------------------|--------------------------------------------------|----|
| 2025-04-26 16:34:31 | Android API Analysis Completed                   | OK |
| 2025-04-26 16:34:32 | Android Permission Mapping Started               | OK |
| 2025-04-26 16:34:32 | Android Permission Mapping Completed             | OK |
| 2025-04-26 16:34:32 | Android Behaviour Analysis Started               | OK |
| 2025-04-26 16:34:32 | Android Behaviour Analysis Completed             | OK |
| 2025-04-26 16:34:32 | Extracting Emails and URLs from Source Code      | OK |
| 2025-04-26 16:34:32 | Email and URL Extraction Completed               | OK |
| 2025-04-26 16:34:32 | Extracting String data from APK                  | OK |
| 2025-04-26 16:34:32 | Extracting String data from SO                   | OK |
| 2025-04-26 16:34:32 | Extracting String data from Code                 | OK |
| 2025-04-26 16:34:32 | Extracting String values and entropies from Code | OK |

|                     |                                               |    |
|---------------------|-----------------------------------------------|----|
| 2025-04-26 16:34:32 | Performing Malware check on extracted domains | OK |
| 2025-04-26 16:34:32 | Saving to Database                            | OK |

---

### Report Generated by - MobSF v4.3.2

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.

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