# ANDROID STATIC ANALYSIS REPORT

## Cake Wallet (4.2.3)

| | |
|---|---|
| File Name: | CakeWallet.apk |
| Package Name: | com.cakewallet.cake_wallet |
| Average CVSS Score: | 7.4 |
| App Security Score: | 40/100 (HIGH RISK) |
| Trackers Detection: | 1/405 |
| Scan Date: | Aug. 16, 2021, 4:32 p.m. |

## FILE INFORMATION

**File Name:** CakeWallet.apk
**Size:** 66.45MB
**MD5:** cb40bebcc56b2a0c182c00144991a20b
**SHA1:** 2a67c41b60c971db56e43d2ebe551aa4ab2a0a2b
**SHA256:** 779855f92a53b509ff905ca9bb4b7a9b932a966f199e75d7630fd9d62b6cf749

## APP INFORMATION

**App Name:** Cake Wallet
**Package Name:** com.cakewallet.cake_wallet
**Main Activity:** com.cakewallet.cake_wallet.MainActivity
**Target SDK:** 29
**Min SDK:** 21
**Max SDK:**
**Android Version Name:** 4.2.3
**Android Version Code:** 55

## APP COMPONENTS

**Activities:** 4
**Services:** 7
**Receivers:** 3
**Providers:** 3
**Exported Activities:** 0
**Exported Services:** 1
**Exported Receivers:** 1
**Exported Providers:** 0

## CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=US, ST=New York, L=New York, O=Cake Wallet LTD, OU=IT, CN=Magic
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-01-01 06:15:44+00:00
Valid To: 2047-05-19 06:15:44+00:00
Issuer: C=US, ST=New York, L=New York, O=Cake Wallet LTD, OU=IT, CN=Magic
Serial Number: 0x359e7b01
Hash Algorithm: sha256
md5: 1532162014fe472f6d03feac32c42bda
sha1: 8c5deda3ae734bd9075993d59f1db57f03c8fbec
sha256: c54053ab0f10d9541762a3da7665ae3dba5e7c743ab4f108a5349d62ac106ef5
sha512: 751432a81d234f1a2cad7a198a17dbfff76cd2808eb4ad025347f92cb90fb9c5bb34c542bf90d3c3ad376fcedaa35fdc7a8658899e8f4dde97f067ed8e3231de
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: c7044d20aa4232937a71290396580ce615475f8f946003c5efb27e53f41f5bf7

| STATUS | DESCRIPTION |
|---|---|
| secure | Application is signed with a code signing certificate |

| STATUS | DESCRIPTION |
|---|---|
| warning | Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android <7.0 |

## APPLICATION PERMISSIONS

| PERMISSION | STATUS | INFO | DESCRIPTION |
|---|---|---|---|
| android.permission.INTERNET | normal | full Internet access | Allows an application to create network sockets. |
| android.permission.USE_FINGERPRINT | normal | allow use of fingerprint | This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead. |
| android.permission.WRITE_EXTERNAL_STORAGE | dangerous | read/modify/delete external storage contents | Allows an application to write to external storage. |
| android.permission.WRITE_INTERNAL_STORAGE | 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. |
| android.permission.CAMERA | dangerous | take pictures and videos | Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time. |
| android.permission.ACCESS_NETWORK_STATE | normal | view network status | Allows an application to view the status of all networks. |
| android.permission.USE_BIOMETRIC | normal | | Allows an app to use device supported biometric modalities. |
| android.permission.WAKE_LOCK | normal | prevent phone from sleeping | Allows an application to prevent the phone from going to sleep. |
| com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE | unknown | Unknown permission | Unknown permission from android reference |
| com.google.android.c2dm.permission.RECEIVE | signature | C2DM permissions | Permission for cloud to device messaging. |

## 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<br>Build.MANUFACTURER check<br>Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table></td></tr>
<tr><td>classes2.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table></td></tr>
</table>

## NETWORK SECURITY

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

## MANIFEST ANALYSIS

| NO | ISSUE | SEVERITY | DESCRIPTION |
|---|---|---|---|
| 1 | Service (io.flutter.plugins.firebasemessaging.FlutterFirebaseMessagingService) is not Protected.<br>An intent-filter exists. | high | A Service 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 Service is explicitly exported. |
| 2 | Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked.<br>Permission: com.google.android.c2dm.permission.SEND<br>[android:exported=true] | high | 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

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| | | | | io/flutter/embedding/engine/systemchannels/MouseCursorChannel.java<br>com/baseflow/permissionhandler/Permiss |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 1 | The App logs information. Sensitive information should never be logged. | info | CVSS V2: 7.5 (high)<br>CWE: CWE-532 Insertion of Sensitive Information into Log File<br>OWASP MASVS: MSTG-STORAGE-3 | ionUtils.java<br>io/flutter/embedding/engine/systemchannels/AccessibilityChannel.java<br>io/flutter/plugin/platform/SingleViewPresentation.java<br>io/flutter/plugin/common/EventChannel.java<br>io/flutter/embedding/engine/systemchannels/SystemChannel.java<br>io/flutter/embedding/engine/systemchannels/LifecycleChannel.java<br>io/flutter/embedding/android/FlutterView.java<br>com/it_nomads/fluttersecurestorage/ciphers/RSACipher18Implementation.java<br>io/flutter/plugins/firebasemessaging/FlutterFirebaseMessagingService.java<br>io/flutter/Log.java<br>io/flutter/embedding/android/FlutterSplashView.java<br>io/flutter/embedding/engine/FlutterEngineConnectionRegistry.java<br>io/flutter/view/FlutterNativeView.java<br>io/flutter/view/FlutterView.java<br>io/flutter/embedding/android/FlutterFragment.java<br>io/flutter/embedding/engine/systemchannels/PlatformViewsChannel.java<br>io/flutter/embedding/engine/systemchannels/KeyEventChannel.java<br>io/flutter/embedding/android/FlutterActivity.java<br>io/flutter/embedding/android/FlutterActivityAndFragmentDelegate.java<br>io/flutter/plugin/common/MethodChannel.java<br>com/it_nomads/fluttersecurestorage/FlutterSecureStoragePlugin.java<br>io/flutter/embedding/engine/systemchannels/TextInputChannel.java<br>io/flutter/embedding/engine/dart/DartExecutor.java<br>de/mintware/barcode_scan/ActivityHelper.java<br>io/flutter/plugins/webviewflutter/FlutterWebViewClient.java<br>io/flutter/plugin/editing/TextInputPlugin.java<br>io/flutter/embedding/engine/loader/FlutterLoader.java<br>io/flutter/embedding/engine/systemchannels/NavigationChannel.java<br>io/flutter/embedding/engine/systemchannels/DeferredComponentChannel.java<br>io/flutter/embedding/engine/dart/DartMessenger.java<br>io/flutter/embedding/engine/renderer/FlutterRenderer.java<br>io/flutter/embedding/android/FlutterSurfaceView.java<br>io/flutter/plugins/urllauncher/UrlLauncherPlugin.java<br>io/flutter/embedding/engine/systemchannels/PlatformChannel.java<br>io/flutter/plugins/firebasemessaging/FirebaseMessagingPlugin.java<br>io/flutter/plugins/urllauncher/MethodCallHandlerImpl.java<br>io/flutter/plugin/common/BasicMessageChannel.java<br>io/flutter/embedding/android/AndroidKeyProcessor.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| | | | | Processor.java<br>io/flutter/embedding/engine/plugins/shim/ShimPluginRegistry.java<br>com/it_nomads/fluttersecurestorage/ciphers/StorageCipher18Implementation.java<br>com/baseflow/permissionhandler/ServiceManager.java<br>me/dm7/barcodescanner/zxing/ZXingScannerView.java<br>io/flutter/plugins/webviewflutter/DisplayListenerProxy.java<br>io/flutter/embedding/engine/deferredcomponents/PlayStoreDeferredComponentManager.java<br>com/mr/flutter/plugin/filepicker/FileUtils.java<br>io/flutter/embedding/android/FlutterTextureView.java<br>io/flutter/embedding/engine/systemchannels/LocalizationChannel.java<br>io/flutter/app/FlutterActivityDelegate.java<br>io/flutter/plugin/platform/PlatformViewsController.java<br>io/flutter/embedding/engine/loader/ResourceExtractor.java<br>io/flutter/embedding/engine/FlutterJNI.java<br>io/flutter/plugins/webviewflutter/InputAwareWebView.java<br>io/flutter/view/AccessibilityViewEmbedder.java<br>io/flutter/plugin/editing/ListenableEditingState.java<br>io/flutter/embedding/engine/systemchannels/SettingsChannel.java<br>io/flutter/plugin/platform/PlatformPlugin.java<br>io/flutter/embedding/engine/plugins/util/GeneratedPluginRegister.java<br>io/flutter/embedding/engine/plugins/shim/ShimRegistrar.java<br>com/mr/flutter/plugin/filepicker/FilePickerDelegate.java<br>de/mintware/barcode_scan/BarcodeScannerActivity.java<br>io/flutter/view/AccessibilityBridge.java<br>com/baseflow/permissionhandler/PermissionManager.java<br>io/flutter/embedding/engine/systemchannels/RestorationChannel.java<br>io/flutter/plugin/editing/InputConnectionAdaptor.java<br>io/flutter/embedding/android/FlutterFragmentActivity.java<br>me/dm7/barcodescanner/core/CameraPreview.java<br>com/baseflow/permissionhandler/AppSettingsManager.java<br>io/flutter/embedding/engine/FlutterEngine.java |

| NO | ISSUE | SEVERITY | STANDARDS | FILES |
|---|---|---|---|---|
| 2 | Files may contain hardcoded sensitive information like usernames, passwords, keys etc. | warning | CVSS V2: 7.4 (high)<br>CWE: CWE-312 Cleartext Storage of Sensitive Information<br>OWASP Top 10: M9: Reverse Engineering<br>OWASP MASVS: MSTG-STORAGE-14 | io/flutter/plugins/firebase/core/FlutterFirebaseCorePlugin.java<br>io/flutter/plugins/firebasemessaging/FlutterFirebaseMessagingService.java<br>com/unstoppabledomains/resolution/naming/service/ZNS.java<br>io/flutter/embedding/android/FlutterActivityAndFragmentDelegate.java<br>io/flutter/embedding/engine/loader/FlutterLoader.java<br>io/flutter/embedding/engine/loader/ApplicationInfoLoader.java<br>com/it_nomads/fluttersecurestorage/ciphers/StorageCipher18Implementation.java<br>io/flutter/app/FlutterActivityDelegate.java<br>io/flutter/embedding/android/FlutterActivityLaunchConfigs.java |
| 3 | Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole. | warning | CVSS V2: 8.8 (high)<br>CWE: CWE-749 Exposed Dangerous Method or Function<br>OWASP Top 10: M1: Improper Platform Usage<br>OWASP MASVS: MSTG-PLATFORM-7 | io/flutter/plugins/webviewflutter/FlutterWebView.java |
| 4 | The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks. | high | CVSS V2: 7.4 (high)<br>CWE: CWE-649 Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-3 | com/it_nomads/fluttersecurestorage/ciphers/StorageCipher18Implementation.java |
| 5 | App can read/write to External Storage. Any App can read data written to External Storage. | high | CVSS V2: 5.5 (medium)<br>CWE: CWE-276 Incorrect Default Permissions<br>OWASP Top 10: M2: Insecure Data Storage<br>OWASP MASVS: MSTG-STORAGE-2 | io/flutter/plugins/share/Share.java<br>io/flutter/plugins/pathprovider/PathProviderPlugin.java<br>com/mr/flutter/plugin/filepicker/FilePickerDelegate.java |
| 6 | The App uses an insecure Random Number Generator. | warning | CVSS V2: 7.5 (high)<br>CWE: CWE-330 Use of Insufficiently Random Values<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-6 | com/mr/flutter/plugin/filepicker/FileUtils.java |
| 7 | This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it. | info | CVSS V2: 0 (info)<br>OWASP MASVS: MSTG-STORAGE-10 | io/flutter/plugin/platform/PlatformPlugin.java<br>io/flutter/plugin/editing/InputConnectionAdaptor.java |

## SHARED LIBRARY BINARY ANALYSIS

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

| NO | SHARED OBJECT | NX | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|
| 1 | lib/x86_64/libcw_monero.so | True<br>info<br>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | True<br>info<br>This shared object 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<br>info<br>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. | False<br>info<br>The shared object does not have run-time search path or RPATH set. | False<br>info<br>The shared object does not have RUNPATH set. | True<br>info<br>The shared object has the following fortified functions: ['__memcpy_chk', '__FD_SET_chk', '__FD_ISSET_chk', '__FD_CLR_chk', '__strlen_chk', '__memmove_chk', '__vsnprintf_chk'] | True<br>info<br>Symbols are stripped. |
| 2 | lib/x86_64/libflutter.so | True<br>info<br>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | False<br>high<br>This shared object 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. | Full RELRO<br>info<br>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. | False<br>info<br>The shared object does not have run-time search path or RPATH set. | False<br>info<br>The shared object does not have RUNPATH set. | True<br>info<br>The shared object has the following fortified functions: ['__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__strncpy_chk', '__memmove_chk', '__strlen_chk'] | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|
| 3 | lib/x86_64/libapp.so | False<br>high<br>The shared object does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable. | False<br>high<br>This shared object 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. | No RELRO<br>high<br>This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO. | False<br>info<br>The shared object does not have run-time search path or RPATH set. | False<br>info<br>The shared object does not have RUNPATH set. | False<br>warning<br>The shared object 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. | True<br>info<br>Symbols are stripped. |
| 4 | lib/armeabi-v7a/libcw_monero.so | True<br>info<br>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | True<br>info<br>This shared object 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<br>info<br>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. | False<br>info<br>The shared object does not have run-time search path or RPATH set. | False<br>info<br>The shared object does not have RUNPATH set. | True<br>info<br>The shared object has the following fortified functions: ['__memcpy_chk', '__FD_SET_chk', '__FD_CLR_chk', '__FD_ISSET_chk'] | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|
| 5 | lib/armeabi-v7a/libflutter.so | True<br>info<br>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | True<br>info<br>This shared object 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<br>info<br>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. | False<br>info<br>The shared object does not have run-time search path or RPATH set. | False<br>info<br>The shared object does not have RUNPATH set. | False<br>warning<br>The shared object 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. | True<br>info<br>Symbols are stripped. |
| 6 | lib/armeabi-v7a/libapp.so | False<br>high<br>The shared object does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable. | False<br>high<br>This shared object 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. | No RELRO<br>high<br>This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO. | False<br>info<br>The shared object does not have run-time search path or RPATH set. | False<br>info<br>The shared object does not have RUNPATH set. | False<br>warning<br>The shared object 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. | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|
| 7 | lib/arm64-v8a/libcw_monero.so | True<br>info<br>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | True<br>info<br>This shared object 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<br>info<br>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. | False<br>info<br>The shared object does not have run-time search path or RPATH set. | False<br>info<br>The shared object does not have RUNPATH set. | True<br>info<br>The shared object has the following fortified functions: ['__FD_ISSET_chk', '__memmove_chk', '__strlen_chk', '__memcpy_chk', '__FD_SET_chk', '__FD_CLR_chk', '__vsnprintf_chk'] | True<br>info<br>Symbols are stripped. |
| 8 | lib/arm64-v8a/libflutter.so | True<br>info<br>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | False<br>high<br>This shared object 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. | Full RELRO<br>info<br>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. | False<br>info<br>The shared object does not have run-time search path or RPATH set. | False<br>info<br>The shared object does not have RUNPATH set. | True<br>info<br>The shared object has the following fortified functions: ['__memcpy_chk', '__vsnprintf_chk', '__read_chk', '__strncpy_chk', '__memmove_chk', '__strlen_chk'] | True<br>info<br>Symbols are stripped. |

| NO | SHARED OBJECT | NX | STACK CANARY | RELRO | RPATH | RUNPATH | FORTIFY | SYMBOLS STRIPPED |
|---|---|---|---|---|---|---|---|---|
| 9 | lib/arm64-v8a/libapp.so | False<br>high<br>The shared object does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as non executable. | False<br>high<br>This shared object 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. | No RELRO<br>high<br>This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO. | False<br>info<br>The shared object does not have run-time search path or RPATH set. | False<br>info<br>The shared object does not have RUNPATH set. | False<br>warning<br>The shared object 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. | True<br>info<br>Symbols are stripped. |
| 10 | lib/x86/libcw_monero.so | True<br>info<br>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable. | True<br>info<br>This shared object 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<br>info<br>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. | False<br>info<br>The shared object does not have run-time search path or RPATH set. | False<br>info<br>The shared object does not have RUNPATH set. | True<br>info<br>The shared object has the following fortified functions: ['__memcpy_chk', '__FD_ISSET_chk', '__FD_CLR_chk', '__FD_SET_chk'] | True<br>info<br>Symbols are stripped. |

## NIAP ANALYSIS v1.3

| NO | IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|---|---|---|---|---|
| 1 | FCS_RBG_EXT.1.1 | Security Functional Requirements | Random Bit Generation Services | The application implement DRBG functionality for its cryptographic operations. |
| 2 | FCS_STO_EXT.1.1 | Security Functional Requirements | Storage of Credentials | The application does not store any credentials to non-volatile memory. |
| 3 | FCS_CKM_EXT.1.1 | Security Functional Requirements | Cryptographic Key Generation Services | The application implement asymmetric key generation. |
| 4 | FDP_DEC_EXT.1.1 | Security Functional Requirements | Access to Platform Resources | The application has access to ['camera', 'network connectivity']. |
| 5 | FDP_DEC_EXT.1.2 | Security Functional Requirements | Access to Platform Resources | The application has access to no sensitive information repositories. |
| 6 | FDP_NET_EXT.1.1 | Security Functional Requirements | Network Communications | The application has user/application initiated network communications. |
| 7 | FDP_DAR_EXT.1.1 | Security Functional Requirements | Encryption Of Sensitive Application Data | The application implement functionality to encrypt sensitive data in non-volatile memory. |
| 8 | FMT_MEC_EXT.1.1 | Security Functional Requirements | Supported Configuration Mechanism | The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options. |
| 9 | FTP_DIT_EXT.1.1 | Security Functional Requirements | Protection of Data in Transit | The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product. |
| 10 | FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2 | Selection-Based Security Functional Requirements | Random Bit Generation from Application | The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate. |
| 11 | FCS_CKM.1.1(1) | Selection-Based Security Functional Requirements | Cryptographic Asymmetric Key Generation | The application generate asymmetric cryptographic keys not in accordance with FCS_CKM.1.1(1) using key generation algorithm RSA schemes and cryptographic key sizes of 1024-bit or lower. |
| 12 | FCS_CKM.1.1(3),FCS_CKM.1.2(3) | Selection-Based Security Functional Requirements | Password Conditioning | A password/passphrase shall perform [Password-based Key Derivation Functions] in accordance with a specified cryptographic algorithm.. |
| 13 | FCS_COP.1.1(1) | Selection-Based Security Functional Requirements | Cryptographic Operation - Encryption/Decryption | The application perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode or AES-GCM (as defined in NIST SP 800-38D) and cryptographic key sizes 256-bit/128-bit. |
| 14 | FCS_COP.1.1(2) | Selection-Based Security Functional Requirements | Cryptographic Operation - Hashing | The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5. |

| NO | IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|---|---|---|---|---|
| 15 | FCS_HTTPS_EXT.1.1 | Selection-Based Security Functional Requirements | HTTPS Protocol | The application implement the HTTPS protocol that complies with RFC 2818. |
| 16 | FCS_HTTPS_EXT.1.2 | Selection-Based Security Functional Requirements | HTTPS Protocol | The application implement HTTPS using TLS. |
| 17 | FCS_HTTPS_EXT.1.3 | Selection-Based Security Functional Requirements | HTTPS Protocol | The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid. |
| 18 | FIA_X509_EXT.1.1 | Selection-Based Security Functional Requirements | X.509 Certificate Validation | The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The application validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates']. |
| 19 | FIA_X509_EXT.1.2 | Selection-Based Security Functional Requirements | X.509 Certificate Validation | The application treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE. |
| 20 | FIA_X509_EXT.2.1 | Selection-Based Security Functional Requirements | X.509 Certificate Authentication | The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS. |
| 21 | FIA_X509_EXT.2.2 | Selection-Based Security Functional Requirements | X.509 Certificate Authentication | When the application cannot establish a connection to determine the validity of a certificate, the application allow the administrator to choose whether to accept the certificate in these cases or accept the certificate ,or not accept the certificate. |
| 22 | FPT_TUD_EXT.2.1 | Selection-Based Security Functional Requirements | Integrity for Installation and Update | The application shall be distributed using the format of the platform-supported package manager. |
| 23 | FCS_CKM.1.1(2) | Optional Security Functional Requirements | Cryptographic Symmetric Key Generation | The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit. |

## DOMAIN MALWARE CHECK

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| mainnet.infura.io | good | **IP:** 52.86.9.221<br>**Country:** United States of America<br>**Region:** Virginia<br>**City:** Ashburn<br>**Latitude:** 39.043720<br>**Longitude:** -77.487488<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| downloads.getmonero.org | good | **IP:** 163.171.131.87<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Jose<br>**Latitude:** 37.385639<br>**Longitude:** -121.885277<br>**View:** Google Map |
| apache.org | good | **IP:** 151.101.2.132<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| s.infura.io | good | No Geolocation information available. |
| api.zilliqa.com | good | **IP:** 104.26.8.22<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| www.w3.org | good | **IP:** 128.30.52.100<br>**Country:** United States of America<br>**Region:** Massachusetts<br>**City:** Cambridge<br>**Latitude:** 42.365078<br>**Longitude:** -71.104523<br>**View:** Google Map |
| github.com | good | **IP:** 140.82.121.4<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| www.openssl.org | good | **IP:** 23.50.198.170<br>**Country:** Egypt<br>**Region:** Al Qahirah<br>**City:** Cairo<br>**Latitude:** 30.062630<br>**Longitude:** 31.249670<br>**View:** Google Map |
| updates.getmonero.org | good | **IP:** 104.22.10.221<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |

| DOMAIN | STATUS | GEOLOCATION |
|---|---|---|
| developer.android.com | good | **IP:** 216.58.211.206<br>**Country:** United States of America<br>**Region:** California<br>**City:** Mountain View<br>**Latitude:** 37.405991<br>**Longitude:** -122.078514<br>**View:** Google Map |
| javax.xml.xmlconstants | good | No Geolocation information available. |

## URLS

| URL | FILE |
|---|---|
| http://javax.xml.XMLConstants/feature/secure-processing<br>http://apache.org/xml/features/disallow-doctype-decl<br>http://apache.org/xml/features/nonvalidating/load-external-dtd | com/fasterxml/jackson/databind/ext/DOMDeserializer.java |
| https://mainnet.infura.io/v3/e0c0cb9d12c440a29379df066de587e6<br>https://mainnet.infura.io/v3/d423cf2499584d7fbe171e33b42cfbee<br>https://api.zilliqa.com<br>https://%s.infura.io/v3/%s | com/unstoppabledomains/resolution/Resolution.java |
| https://developer.android.com/guide/topics/permissions/overview | io/flutter/plugin/platform/PlatformPlugin.java |
| https://github.com/flutter/flutter/issues/2897).It | io/flutter/plugin/platform/PlatformViewsController.java |
| https://github.com/flutter/flutter/wiki/Upgrading-pre-1.12-Android-projects | io/flutter/view/FlutterView.java |
| http://localhost:8442/<br>https://downloads.getmonero.org/<br>https://updates.getmonero.org/<br>http://www.openssl.org/support/faq.html | lib/x86_64/libcw_monero.so |
| data:application/dart<br>data:application/dart;<br>https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).<br>https://github.com/flutter/flutter/issues/73620.<br>http://www.w3.org/XML/1998/namespace<br>http://www.w3.org/2000/xmlns/ | lib/x86_64/libflutter.so |
| https://downloads.getmonero.org/<br>https://updates.getmonero.org/<br>http://www.openssl.org/support/faq.html<br>http://localhost:8442/ | lib/armeabi-v7a/libcw_monero.so |
| http://www.w3.org/XML/1998/namespace<br>data:application/dart<br>data:application/dart;<br>http://www.w3.org/2000/xmlns/<br>https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).<br>https://github.com/flutter/flutter/issues/73620. | lib/armeabi-v7a/libflutter.so |
| http://localhost:8442/<br>https://downloads.getmonero.org/<br>https://updates.getmonero.org/<br>http://www.openssl.org/support/faq.html | lib/arm64-v8a/libcw_monero.so |

| URL | FILE |
|---|---|
| http://www.w3.org/XML/1998/namespace<br>data:application/dart<br>data:application/dart;<br>http://www.w3.org/2000/xmlns/<br>https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).<br>https://github.com/flutter/flutter/issues/73620. | lib/arm64-v8a/libflutter.so |
| http://localhost:8442/<br>https://downloads.getmonero.org/<br>https://updates.getmonero.org/<br>http://www.openssl.org/support/faq.html | lib/x86/libcw_monero.so |

# ✉ EMAILS

| EMAIL | FILE |
|---|---|
| appro@openssl.org | lib/arm64-v8a/libflutter.so |

# TRACKERS

| TRACKER | CATEGORIES | URL |
|---|---|---|
| Google Firebase Analytics | Analytics | https://reports.exodus-privacy.eu.org/trackers/49 |

# PLAYSTORE INFORMATION

**Title:** Cake Wallet

**Score:** 2.940594 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** 5.0 and up **Category:** Finance **Play Store URL:** com.cakewallet.cake_wallet

**Developer Details:** Cake Technologies LLC, Cake+Technologies+LLC, 8815 Conroy Windermere Road Unit 250 Orlando, FL. 32835, https://cakewallet.com, info@cakewallet.com,

**Release Date:** Jan 1, 2020 **Privacy Policy:** Privacy link

**Description:**

Cake Wallet allows you to safely store, send receive and exchange your Monero, Bitcoin, and Litecoin and also buy Bitcoin with debit/credit cards. With built-in EXCHANGES for XMR, BTC, LTC, ETH, BCH, DASH, USDT, DAI, EOS, XRP, TRX, BNB, ADA, XLM, and NANO ! Features of Cake Wallet: -Create multiple Bitcoin, Litecoin, and Monero Wallets -You control your own seed and keys -Simple interface -EXCHANGE between XMR, BTC, LTC, ETH, BCH, DASH, USDT, EOS, XRP, TRX, BNB, ADA, XLM, and NANO with in-app exchanges -Monero's unique Subaddresses -Supports many fiat currencies -Create multiple accounts within wallets (for Monero) -Address Book to save various crypto addresses -Restore existing wallets using seed or private keys -Restore wallets from blockheight or date -Backup/Restore app to iCloud and other locations -Rescan wallet -Supports the MyMonero 13 word seed to restore your wallets -Adjustable transaction speeds -Coin Control for BTC -Unstoppable Domains for BTC, LTC and XMR -Choose and save your daemon/node -Connects directly to the monero blockchain -3 Color Themes (Light, Dark, Colorful) -EXCHANGE between XMR, BTC, LTC, ETH, BCH, DASH, USDT, EOS, XRP, TRX, BNB, ADA, XLM, and NANO with in-app exchanges -In Mandarin, Russian, Spanish, German, Hindi, Korean, Japanese, Portuguese, Ukrainian Polish and Dutch and more!

## App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

### Risk Calculation

| APP SECURITY SCORE | RISK |
|---|---|
| 0 - 15 | CRITICAL |
| 16 - 40 | HIGH |
| 41 - 70 | MEDIUM |
| 71 - 100 | LOW |

### Report Generated by - MobSF v3.4.5 Beta

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.