



## ANDROID STATIC ANALYSIS REPORT



 WonderDroid X (3.1)

File Name: installer3839.apk

Package Name: com.atelieryl.wonderdroid






Scan Date: May 31, 2022, 6:13 p.m.

App Security Score: 64/100 (LOW RISK)

Grade:



## FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
0	4	1	1	1

## FILE INFORMATION

File Name: installer3839.apk

Size: 3.1MB

MD5: aba1c7e20977fea0256d4258863454eb

SHA1: b15a92d7f0c29886ccb511d1a24059de7aa58f81

SHA256: 88f67e5c91f495ed12b157870aaebd6fa49a1dd2cb875bdf28ae932b163012ed

## APP INFORMATION

App Name: WonderDroid X

Package Name: com.atelieryl.wonderdroid

Main Activity: com.atelieryl.wonderdroid.Select

Target SDK: 28

Min SDK: 14

Max SDK:

Android Version Name: 3.1

Android Version Code: 51

## APP COMPONENTS

Activities: 3

Services: 0

Receivers: 0

Providers: 0

Exported Activities: 0

Exported Services: 0

Exported Receivers: 0

Exported Providers: 0

## CERTIFICATE INFORMATION

APK is signed

v1 signature: True

v2 signature: True

v3 signature: False

Found 1 unique certificates

Subject: C=CA, ST=British Columbia, L=Vancouver, O=Yearbook Labs Company, OU=Atelier Yearbook Labs, CN=Willie Chang

Signature Algorithm: rsassa\_pkcs1v15

Valid From: 2014-10-30 21:58:38+00:00

Valid To: 2039-10-24 21:58:38+00:00

Issuer: C=CA, ST=British Columbia, L=Vancouver, O=Yearbook Labs Company, OU=Atelier Yearbook Labs, CN=Willie Chang

Serial Number: 0xd2c305f

Hash Algorithm: sha256

md5: 6e88d24c74a13bcfaca5490a9e95a0e9

sha1: 1d5bf66f1b8dd0a4165c172d2c077255fe599cac

sha256: 83d05d93f99ff6aeaff3d317e7f3352b31f0bb8d55f6c4b233fcb5b659c40885

sha512: e0e41698c484bda91bf75dbdfd090ef8828aea03c5e1372b7d60263013b3acdf83dcca079a888c8b9c2d4b1d315979930351d6842d7b4d6046104d4d2acb6c91

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 0612958024a1414c3820480b7c1270f102837de6dda12bde468dcaa2d0a6ed4b

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

## APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

## APKID ANALYSIS

FILE	DETAILS
------	---------

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Compiler	r8

## NETWORK SECURITY

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

## MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

## CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	<a href="#">App can read/write to External Storage. Any App can read data written to External Storage.</a>	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/atelieryl/wonderdroid/WonderDroid.java com/atelieryl/wonderdroid/Main.java
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 OWASP MASVS: MSTG-STORAGE-3	com/atelieryl/wonderdroid/utils/RomAdapter.java com/atelieryl/wonderdroid/views/EmuView.java com/atelieryl/wonderdroid/Select.java com/atelieryl/wonderdroid/WonderSwan.java com/atelieryl/wonderdroid/utils/ZipUtils.java com/atelieryl/wonderdroid/views/HardwareButtonPreference.java com/atelieryl/wonderdroid/utils/CpuUtils.java com/atelieryl/wonderdroid/utils/ZipCache.java com/atelieryl/wonderdroid/TouchInputHandler.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/mips/libwonderswan.so	<p>True <b>info</b></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>False <b>high</b></p> <p>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.</p>	<p>Partial RELRO <b>warning</b></p> <p>This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option - z,relro,- z,now to enable full RELRO.</p>	<p>None <b>info</b></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <b>info</b></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <b>warning</b></p> <p>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.</p>	<p>True <b>info</b></p> <p>Symbols are stripped.</p>



NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/armeabi-v7a/libwonderswan.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>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.</p>	<p>Full RELRO <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 <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/armeabi-v7a/libwonderswan-neon.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>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.</p>	<p>Full RELRO <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 <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/x86/libwonderswan.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>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.</p>	<p>Full RELRO <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 <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/armeabi/libwonderswan.so	<p>True <a href="#">info</a></p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True <a href="#">info</a></p> <p>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.</p>	<p>Full RELRO <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 <a href="#">info</a></p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None <a href="#">info</a></p> <p>The shared object does not have RUNPATH set.</p>	<p>False <a href="#">warning</a></p> <p>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.</p>	<p>True <a href="#">info</a></p> <p>Symbols are stripped.</p>

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
2	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity'].
4	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
5	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
6	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.
7	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.
8	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.

## DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
yearbooklabs.com	ok	IP: 66.113.226.146 Country: United States of America Region: Illinois City: Chicago Latitude: 41.882500 Longitude: -87.636703 View: <a href="#">Google Map</a>
github.com	ok	IP: 140.82.121.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: <a href="#">Google Map</a>
play.google.com	ok	IP: 142.251.36.46 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: <a href="#">Google Map</a>
www.flaticon.com	ok	IP: 34.149.47.137 Country: United States of America Region: Texas City: Houston Latitude: 29.941401 Longitude: -95.344498 View: <a href="#">Google Map</a>

# HARDCODED SECRETS

POSSIBLE SECRETS
"pressakey" : "ボタンを押してください"
"pressakey" : "请按下一个按键"
"pressakey" : "請按下一個按鍵"

---

## Report Generated by - MobSF v3.5.2 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.

© 2022 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).