MOBSF

ANDROID STATIC ANALYSIS REPORT

Dolphin Emulator (5.0-6374)

File Name:	installer195.apk
Package Name:	org.dolphinemu.dolphinemu
Scan Date:	May 31, 2022, 4:04 p.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	6	1	1	1

FILE INFORMATION

File Name: installer195.apk
Size: 13.76MB
MD5: c50dc9e0eadf04e4d69f9bfdb65906b0
SHA1: aaa8fbfe8b564fa5f0fa7744c5459621f1968ea3
SHA256: e3474507b680129077a60a389d94659d3060d268eaef3d2a08e954b22848df6a

APP INFORMATION

App Name: Dolphin Emulator
Package Name: org.dolphinemu.dolphinemu
Main Activity: org.dolphinemu.dolphinemu.ui.main.MainActivity
Target SDK: 25
Min SDK: 21
Max SDK:
Android Version Name: 5.0-6374
Android Version Code: 14523

APP COMPONENTS

Activities: 5
Services: 1
Receivers: 0
Providers: 2
Exported Activities: 2
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-10-28 05:26:09+00:00
Valid To: 2041-03-15 05:26:09+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x205da263
Hash Algorithm: sha256
md5: 778ab363eda87ce3ff57d66969c12896
sha1: f69e215d2768c37595c381c5e8118de310407263
sha256: 4014f9169e3ff08cd8fdf8ac33419d4603ed95582716494a0392853c91148835
sha512: 114267c69e99647a6514b95f5674c146079f3f69b90f63def0c608200b742154d965b234d352631c780829607090aa6bcf439c086b326a66fc572442aa29e48e

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

TITLE	SEVERITY	DESCRIPTION
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.

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.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dx (possible dexmerge)</td></tr><tr><td>Manipulator Found</td><td>dexmerge</td></tr></table>

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.
2	Activity (org.dolphinemu.dolphinemu.ui.main.TvMainActivity) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Activity (org.dolphinemu.dolphinemu.activities.CustomFilePickerActivity) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	rx/internal/schedulers/NewThreadWorker.java rx/plugins/RxJavaPlugins.java
2	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	org/dolphinemu/dolphinemu/utils/FileBrowserHelper.java com/nononsenseapps/filepicker/FilePickerActivity.java org/dolphinemu/dolphinemu/activities/CustomFilePickerActivity.java org/dolphinemu/dolphinemu/model/Game.java org/dolphinemu/dolphinemu/services/DirectoryInitializationService.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	rx/internal/util/RxJavaPluginUtils.java org/dolphinemu/dolphinemu/NativeLibrary.java org/dolphinemu/dolphinemu/model/settings/view/SliderSetting.java org/dolphinemu/dolphinemu/utils/Java_WiimoteAdapter.java org/dolphinemu/dolphinemu/fragments/EmulationFragment.java org/dolphinemu/dolphinemu/utils/EGLHelper.java rx/internal/util/RxRingBuffer.java org/dolphinemu/dolphinemu/utils/Java_GCAdapter.java org/dolphinemu/dolphinemu/services/DirectoryInitializationService.java org/dolphinemu/dolphinemu/ui/settings/SettingsAdapter.java rx/internal/util/IndexedRingBuffer.java org/dolphinemu/dolphinemu/utils/Log.java org/dolphinemu/dolphinemu/ui/settings/SettingsActivityPresenter.java org/dolphinemu/dolphinemu/utils/SettingsFile.java org/dolphinemu/dolphinemu/adapters/GameAdapter.java org/dolphinemu/dolphinemu/model/GameDatabase.java org/dolphinemu/dolphinemu/ui/platform/PlatformGamesPresenter.java org/dolphinemu/dolphinemu/dialogs/MotionAlertDialog.java org/dolphinemu/dolphinemu/model/GameProvider.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	org/dolphinemu/dolphinemu/model/GameDatabase.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/arm64-v8a/libmain.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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.	Partial RELRO warning 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.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning 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 info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/x86_64/libmain.so	True info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True info 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 info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The shared object does not have run-time search path or RPATH set.	None info The shared object does not have RUNPATH set.	False warning 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 info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application use no 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 generate no asymmetric cryptographic keys.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
amw.wc24.wii.com	ok	**IP:** 3.92.106.182 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
nus.shop.wii.com	ok	**IP:** 69.25.139.201 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
analytics.dolphin-emu.org	ok	**IP:** 138.201.21.200 **Country:** Germany **Region:** Sachsen **City:** Falkenstein **Latitude:** 50.477879 **Longitude:** 12.371290 **View:** Google Map
limadriver.org	ok	No Geolocation information available.
www.sfml-dev.org	ok	**IP:** 78.47.82.133 **Country:** Germany **Region:** Sachsen **City:** Falkenstein **Latitude:** 50.477879 **Longitude:** 12.371290 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
geckocodes.org	ok	**IP:** 188.114.96.0 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **View:** Google Map
mtw.wc24.wii.com	ok	No Geolocation information available.
rcw.wc24.wii.com	ok	No Geolocation information available.
dolphin-emu.org	ok	**IP:** 185.31.40.21 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map

EMAILS

EMAIL	FILE
user@sfml-dev.org ftp@example.com	lib/arm64-v8a/libmain.so

EMAIL	FILE
user@sfml-dev.org ftp@example.com 6h@fo.lwft w9oi_2nhels4u@dlilycclglhl.5jlcg_bqh yay@y.u5vcghyy	lib/x86_64/libmain.so

---

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.