



## ANDROID STATIC ANALYSIS REPORT



 Dolphin Emulator (5.0-12716)

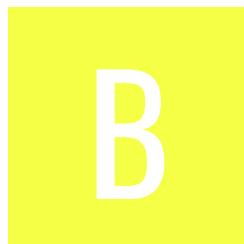
File Name: installer175.apk

Package Name: org.dolphinemu.dolphinemu






Scan Date: May 31, 2022, 8:15 a.m.

App Security Score: 53/100 (MEDIUM RISK)

Grade:



## FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
1	4	1	1	1

## FILE INFORMATION

File Name: installer175.apk

Size: 15.75MB

MD5: 8a454bbadb84e34c3530416837bb02a

SHA1: 96a6e696ec5edab6f3a1eb118ad8a6098ff6572c

SHA256: 892fd671ff35ea16ae98ca920d6aa577230e5baead8c156876e7341713425d29

## APP INFORMATION

App Name: Dolphin Emulator

Package Name: org.dolphinemu.dolphinemu

Main Activity: org.dolphinemu.dolphinemu.ui.main.MainActivity

Target SDK: 29

Min SDK: 21

Max SDK:

Android Version Name: 5.0-12716

Android Version Code: 16869

## APP COMPONENTS

Activities: 7

Services: 4

Receivers: 0

Providers: 2

Exported Activities: 3

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	<a href="#">info</a>	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.
com.android.providers.tv.permission.READ_EPG_DATA	unknown	Unknown permission	Unknown permission from android reference
com.android.providers.tv.permission.WRITE_EPG_DATA	unknown	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.MANUFACTURER check
	Compiler	r8

## NETWORK SECURITY

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

## MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Activity (org.dolphinemu.dolphinemu.activities.AppLinkActivity) 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
----	-------	----------	-----------	-------

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	<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	org/dolphinemu/dolphinemu/features/settings/Utils/SettingsFile.java org/dolphinemu/dolphinemu/Utils/DirectoryInitialization.java org/dolphinemu/dolphinemu/dialogs/MotionAlertDialog.java org/dolphinemu/dolphinemu/services/SyncChannelJobService.java org/dolphinemu/dolphinemu/services/SyncProgramsJobService.java org/dolphinemu/dolphinemu/dialogs/GamePropertiesDialog.java org/dolphinemu/dolphinemu/Utils/EGLHelper.java org/dolphinemu/dolphinemu/Utils/AnalyticsAnalytics.java org/dolphinemu/dolphinemu/Utils/Java_GCAdapter.java org/dolphinemu/dolphinemu/fragments/EmulationFragment.java org/dolphinemu/dolphinemu/features/settings/ui/SettingsFragmentPresenter.java org/dolphinemu/dolphinemu/NativeLibrary.java org/dolphinemu/dolphinemu/Utils/Log.java org/dolphinemu/dolphinemu/Utils/TvUtil.java org/dolphinemu/dolphinemu/activities/AppLinkActivity.java org/dolphinemu/dolphinemu/Utils/Java_WiimoteAdapter.java org/dolphinemu/dolphinemu/features/settings/ui/SettingsActivityPresenter.java



NO	ISSUE	SEVERITY	STANDARDS	FILES
2	<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/nononsenseapps/filepicker/FilePickerActivity.java org/dolphinemu/dolphinemu/utils/DirectoryInitialization.java org/dolphinemu/dolphinemu/utils/FileBrowserHelper.java org/dolphinemu/dolphinemu/activities/CustomFilePickerActivity.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	<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>True <a href="#">info</a></p> <p>The shared object has the following fortified functions: ['__FD_ISSET_chk', '__memmove_chk', '__strlen_chk', '__read_chk', '__vsprintf_chk', '__strcat_chk', '__strchr_chk', '__memcpy_chk', '__FD_SET_chk', '__FD_CLR_chk', '__memset_chk', '__strcpy_chk', '__vsnprintf_chk']</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
2	lib/x86_64/libmain.so	True <a href="#">info</a> The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	True <a href="#">info</a> 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 <a href="#">info</a> 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 <a href="#">info</a> The shared object does not have run-time search path or RPATH set.	None <a href="#">info</a> The shared object does not have RUNPATH set.	True <a href="#">info</a> The shared object has the following fortified functions: ['__memcpy_chk', '__memmove_chk', '__memset_chk', '__vsprintf_chk', '__FD_ISSET_chk', '__FD_SET_chk', '__strlen_chk', '__strcpy_chk', '__strcat_chk', '__strchr_chk', '__read_chk', '__FD_CLR_chk', '__vsnprintf_chk']	True <a href="#">info</a> Symbols are stripped.

## NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	<a href="#">FCS_RBG_EXT.1.1</a>	Security Functional Requirements	Random Bit Generation Services	The application use no DRBG functionality for its cryptographic operations.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.
10	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
11	<a href="#">FCS_HTTPS_EXT.1.2</a>	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
12	<a href="#">FCS_HTTPS_EXT.1.3</a>	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.
13	<a href="#">FIA_X509_EXT.2.1</a>	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.

## DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
amw.wc24.wii.com	ok	IP: 52.22.41.35 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
www.geckocodes.org	ok	IP: 188.114.97.0 Country: Spain Region: Madrid, Comunidad de City: Madrid Latitude: 40.416500 Longitude: -3.702560 View: <a href="#">Google Map</a>
lobby.dolphin-emu.org	ok	IP: 138.201.21.200 Country: Germany Region: Sachsen City: Falkenstein Latitude: 50.477879 Longitude: 12.371290 View: <a href="#">Google Map</a>
art.gametdb.com	ok	IP: 188.165.246.77 Country: France Region: Hauts-de-France City: Roubaix Latitude: 50.694210 Longitude: 3.174560 View: <a href="#">Google Map</a>
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: <a href="#">Google Map</a>

DOMAIN	STATUS	GEOLOCATION
analytics.dolphin-emu.org	ok	IP: 138.201.21.200 Country: Germany Region: Sachsen City: Falkenstein Latitude: 50.477879 Longitude: 12.371290 View: <a href="#">Google Map</a>
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: <a href="#">Google Map</a>
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: <a href="#">Google Map</a>



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

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