

ANDROID STATIC ANALYSIS REPORT



Dolphin Emulator (0.13)

File Name:	installer291.apk			
Package Name:	org.dolphinemu.dolphinemu			
Scan Date:	May 31, 2022, 11:49 a.m.			
App Security Score:	54/100 (MEDIUM RISK			
Grade:				

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	≪ HOTSPOT
1	3	1	1	1

FILE INFORMATION

File Name: installer291.apk

Size: 12.58MB

MD5: 9d5e7b730f8a06e0d79da74d12cfac28

SHA1: 97ea32fe2e972d622c38fa8b8f5e58d9b32ca000

SHA256: 66317f752b9b90ff0036f3cd1efe76998f549c88a85de01531cc7583d9b330a6

i APP INFORMATION

App Name: Dolphin Emulator

Package Name: org.dolphinemu.dolphinemu

 ${\it Main Activity:} \ {\it org.} dolphine mu. dolphine mu. activities. Main Activity$

Target SDK: 21 Min SDK: 21 Max SDK:

Android Version Name: 0.13 Android Version Code: 13

EE APP COMPONENTS

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

Exported Activities: O Exported Services: O Exported Receivers: O Exported Providers: O

***** 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.

M APKID ANALYSIS

FILE

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

△ NETWORK SECURITY

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

Q 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	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	org/dolphinemu/dolphinemu/utils/EG LHelper.java org/dolphinemu/dolphinemu/fragme nts/PlatformGamesFragment.java org/dolphinemu/dolphinemu/NativeLi brary.java org/dolphinemu/dolphinemu/services /AssetCopyService.java org/dolphinemu/dolphinemu/utils/CP UHelper.java org/dolphinemu/dolphinemu/model/ GameProvider.java org/dolphinemu/dolphinemu/dialogs/ MotionAlertDialog.java org/dolphinemu/dolphinemu/services /SettingsSaveService.java org/dolphinemu/dolphinemu/fragme nts/EmulationFragment.java org/dolphinemu/dolphinemu/activitie s/SettingsActivity.java org/dolphinemu/dolphinemu/activitie s/EmulationActivity.java org/dolphinemu/dolphinemu/adapter s/GameAdapter.java org/dolphinemu/dolphinemu/activitie s/MainActivity.java org/dolphinemu/dolphinemu/activitie s/MainActivity.java org/dolphinemu/dolphinemu/activitie
2	App can read/write to External Storage. Any App can read data written to External Storage. warning		rage. Any App can read data warning OWASP Top 10: M2: Insecure Data Storage	

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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.	False high 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.	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.	False warning Symbols are available.

■ NIAP ANALYSIS v1.3

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 does not encrypt files 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 not encrypt any data in traffic or does not transmit any data between itself and another trusted IT product.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
amw.wc24.wii.com	ok	IP: 34.225.188.213 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
limadriver.org	ok	No Geolocation information available.
mtw.wc24.wii.com	ok	No Geolocation information available.
schemas.android.com	ok	No Geolocation information available.
rcw.wc24.wii.com	ok	No Geolocation information available.



EMAIL	FILE
6h@fo.lwft w9oi_2nhels4u@dlilycclglhl.5jlcg_bqh yay@y.u5vcghyy	lib/arm64-v8a/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.