MOBSF

ANDROID STATIC ANALYSIS REPORT

opsu! (0.16.1a)

File Name:	installer3761.apk
Package Name:	fluddokt.opsu.android
Scan Date:	May 31, 2022, 7:52 p.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	7	2	1	1

FILE INFORMATION

File Name: installer3761.apk
Size: 23.03MB
MD5: c457925a8ca3c43fc404fad5d9ed37c0
SHA1: d4a0936d429a4cf922143c3cb5a4052114e4a8fb
SHA256: ce4dac5f223007fffad2575caf9705b40d3933c7b7d5a1992592951a4936ef6b

APP INFORMATION

App Name: opsu!
Package Name: fluddokt.opsu.android
Main Activity: fluddokt.opsu.android.AndroidLauncher
Target SDK: 22
Min SDK: 8
Max SDK:
Android Version Name: 0.16.1a
Android Version Code: 2

APP COMPONENTS

Activities: 1
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: 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: 2019-03-01 12:41:07+00:00
Valid To: 2046-07-17 12:41:07+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x61c3e494
Hash Algorithm: sha256
md5: 35e73c7900bcb47c09ef0a479149b025
sha1: 0d4c6bead7a587f4676acddb4c1cdfbefb8ab1d6
sha256: ea6138791396b92e349bae6839cb2ddd2a41d2bfcd5551549b7401f34e214605
sha512: 1b6ef86b417c585ff449532f31da50c0dae95dc9d61a485591966d36956fd507f529b7742b135cd0a6d412b38d6284f8b70a90a5bb4ecf30fd29531b2f2a6375

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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.BOARD check</td></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.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				itdelatrisu/opsu/render/LegacyCurveRenderState.java fluddokt/opsu/fake/openal/OggInputStream.java com/badlogic/gdx/math/Intersector.java itdelatrisu/opsu/downloads/servers/RippleServer.java itdelatrisu/opsu/downloads/servers/OsuMirrorServer.java com/badlogic/gdx/backends/android/AndroidFragmentApplication.java com/badlogic/gdx/backends/android/AndroidApplication.java itdelatrisu/opsu/beatmap/BeatmapParser.java com/badlogic/gdx/scenes/scene2d/Group.java org/sqldroid/SQLiteDatabase.java com/badlogic/gdx/input/RemoteInput.java org/sqldroid/SQLDroidResultSetMetaData.java fluddokt/opsu/fake/MusicJL3.java itdelatrisu/opsu/beatmap/Beatmap.java fluddokt/opsu/fake/openal/Mp3InputStream.java fluddokt/opsu/fake/gl/GL11.java itdelatrisu/opsu/Utils.java itdelatrisu/opsu/states/MainMenu.java itdelatrisu/opsu/states/GameRanking.java itdelatrisu/opsu/downloads/servers/BloodcatServer.java itdelatrisu/opsu/Opsu.java

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	itdelatrisu/opsu/Opsu.java itdelatrisu/opsu/downloads/servers/MengSkyServer.java com/badlogic/gdx/backends/android/AndroidGraphicsLiveWallpaper.java fluddokt/opsu/fake/ClipGDXSound.java org/sqldroid/SQLDroidBlob.java itdelatrisu/opsu/replay/Replay.java itdelatrisu/opsu/beatmap/ImageLoader.java itdelatrisu/opsu/objects/curves/Curve.java org/sqldroid/SQLDroidDriver.java javazoom2/jl/converter/jlc.java fluddokt/opsu/fake/ResourceLoader.java com/badlogic/gdx/backends/android/surfaceview/GLSurfaceView20API18.java com/badlogic/gdx/backends/android/surfaceview/GLSurfaceView20.java itdelatrisu/opsu/ui/Fonts.java com/badlogic/gdx/backends/android/AndroidLiveWallpaperService.java com/badlogic/gdx/backends/android/AndroidLiveWallpaper.java itdelatrisu/opsu/beatmap/BeatmapDifficultyCalculator.java javazoom2/jl/player/PlayerApplet.java itdelatrisu/opsu/downloads/servers/YaSOnlineServer.java fluddokt/opsu/fake/Log.java org/sqldroid/SQLDroidStatement.java com/jcraft/jogg/Buffer.java itdelatrisu/opsu/beatmap/TimingPoint.java com/badlogic/gdx/utils/GdxNativesLoader.java org/sqldroid/SQLDroidResultSet.java org/sqldroid/SQLDroidPreparedStatement.java itdelatrisu/opsu/skins/SkinLoader.java com/badlogic/gdx/backends/android/su

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/badlogic/gdx/backends/android/surfaceview/GdxEglConfigChooser.java org/sqldroid/SQLDroidDatabaseMetaData.java org/sqldroid/Log.java itdelatrisu/opsu/states/Game.java itdelatrisu/opsu/ErrorHandler.java com/badlogic/gdx/backends/android/AndroidDaydream.java fluddokt/opsu/fake/AppGameContainer.java fluddokt/opsu/fake/File.java itdelatrisu/opsu/db/ScoreDB.java fluddokt/opsu/fake/Image.java javazoom2/jl/player/jlp.java itdelatrisu/opsu/options/Options.java fluddokt/opsu/fake/Music.java itdelatrisu/opsu/beatmap/HitObject.java org/sqldroid/SQLDroidConnection.java javazoom2/jl/player/advanced/jlap.java com/badlogic/gdx/backends/android/AndroidOnscreenKeyboard.java com/badlogic/gdx/backends/android/surfaceview/GLSurfaceViewAPI18.java itdelatrisu/opsu/downloads/servers/MnetworkServer.java fluddokt/opsu/fake/Font.java itdelatrisu/opsu/replay/ReplayImporter.java fluddokt/opsu/fake/FileSystemLocation.java itdelatrisu/opsu/states/CalibrateOffsetMenu.java itdelatrisu/opsu/states/DownloadsMenu.java fluddokt/opsu/fake/GameOpsu.java com/badlogic/gdx/utils/JsonReader.java fluddokt/opsu/fake/openal/AudioInputStream2.java fluddokt/opsu/fake/AudioDevicePlayer3.java itdelatrisu/opsu/db/BeatmapDB.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				itdelatrisu/opsu/db/BeatmapDB.java fluddokt/opsu/fake/AudioDevicePlayer2.java itdelatrisu/opsu/downloads/servers/HexideServer.java
2	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/sqldroid/SQLiteDatabase.java
3	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	net/lingala/zip4j/crypto/StandardEncrypter.java itdelatrisu/opsu/GameData.java com/badlogic/gdx/math/RandomXS128.java com/badlogic/gdx/math/MathUtils.java itdelatrisu/opsu/options/OptionsOverlay.java net/lingala/zip4j/crypto/AESEncrpyter.java itdelatrisu/opsu/ui/StarStream.java
4	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	itdelatrisu/opsu/Utils.java itdelatrisu/opsu/io/MD5InputStreamWrapper.java
5	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	com/badlogic/gdx/backends/android/AndroidFiles.java fluddokt/opsu/android/AndroidLauncher.java fluddokt/opsu/fake/File.java com/badlogic/gdx/files/FileHandle.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	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	itdelatrisu/opsu/db/ScoreDB.java itdelatrisu/opsu/db/BeatmapDB.java
7	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/badlogic/gdx/utils/SharedLibraryLoader.java com/badlogic/gdx/files/FileHandle.java
8	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/badlogic/gdx/backends/android/AndroidClipboard.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/armeabi-v7a/libgdx-freetype.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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/armeabi-v7a/libgdx.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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/x86/libgdx-freetype.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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/x86/libgdx.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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/armeabi/libgdx-freetype.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.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	lib/armeabi/libgdx.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 does not encrypt files 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
10	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.
11	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
12	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
13	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 certificate path must terminate with a trusted CA certificate'].
14	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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
itdelatrisu.github.io	ok	**IP:** 185.199.111.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
osu.yas-online.nets	ok	No Geolocation information available.
www.shoutcastserver.com	ok	**IP:** 35.186.238.101 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
osu.uu.gl	ok	No Geolocation information available.
www.javazoom.net	ok	No Geolocation information available.
b.ppy.sh	ok	**IP:** 172.67.14.100 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
loli.al	ok	**IP:** 106.185.28.68 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
osu.yas-online.net	ok	**IP:** 151.80.168.2 **Country:** France **Region:** Hauts-de-France **City:** Roubaix **Latitude:** 50.694210 **Longitude:** 3.174560 **View:** Google Map
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:** Google Map
osu.hexide.com	ok	No Geolocation information available.
raw.githubusercontent.com	ok	**IP:** 185.199.111.133 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.server.com	ok	**IP:** 52.8.126.80 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map
osu.mengsky.net	ok	No Geolocation information available.
bloodcat.com	ok	**IP:** 221.162.212.196 **Country:** Korea (Republic of) **Region:** Ulsan-gwangyeoksi **City:** Ulsan **Latitude:** 35.537220 **Longitude:** 129.316666 **View:** Google Map
storage.ripple.moe	ok	**IP:** 136.243.80.59 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map

---

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.