MOBSF

ANDROID STATIC ANALYSIS REPORT

OpenFool (0.3.0)

File Name:	installer3804.apk
Package Name:	ru.hyst329.openfool
Scan Date:	May 31, 2022, 6:11 p.m.
App Security Score:	61/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	5	2	2	0

FILE INFORMATION

File Name: installer3804.apk
Size: 17.73MB
MD5: 4778675e2c2d5c867f704523e2411b8b
SHA1: 2b5451e7287063ff9eda0a791516f2f713c1ed5d
SHA256: 04c8764f5e00b277d451946b7ca2b073937c7a08d2086ab1c5ddc360eb893066

APP INFORMATION

App Name: OpenFool
Package Name: ru.hyst329.openfool
Main Activity: ru.hyst329.openfool.AndroidLauncher
Target SDK: 28
Min SDK: 14
Max SDK:
Android Version Name: 0.3.0
Android Version Code: 30

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: 2018-08-22 08:51:34+00:00
Valid To: 2046-01-07 08:51:34+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x48e1f80b
Hash Algorithm: sha256
md5: 11f6980619143b6cd533dcf02e52064c
sha1: 732924e6f01d058380d9ead60b408948451305c7
sha256: c45d70fc75e5de9477d3cb109cda2551b598f1cd579d07dff286b33a5ece2074
sha512: 22c7ddf073535c48f0e2c89ca9d2c9d43606fdb44c888004766595ed90a69e3b1f2af0382db0dc8b787ac4a57fb9757ba69c2fd23ea049399e061044a65dde0d

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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: DETAILS Compiler: r8

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION

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	ru/hyst329/openfool/NewGameScreen.java com/badlogic/gdx/backends/android/AndroidFragmentApplication.java com/badlogic/gdx/input/RemoteInput.java com/badlogic/gdx/backends/android/AndroidLiveWallpaper.java ch/qos/logback/core/net/DefaultSocketConnector.java ru/hyst329/openfool/Player.java com/badlogic/gdx/backends/android/surfaceview/GdxEglConfigChooser.java ch/qos/logback/core/subst/Node.java com/badlogic/gdx/backends/android/surfaceview/GLSurfaceView20API18.java com/badlogic/gdx/backends/android/surfaceview/GLSurfaceView20.java com/badlogic/gdx/graphics/glutils/ETC1.java com/badlogic/gdx/backends/android/AndroidLiveWallpaperService.java com/kotcrab/vis/usl/Parser.java ru/hyst329/openfool/PlayerTesting.java ch/qos/logback/classic/spi/PackagingDataCalculator.java com/kotcrab/vis/usl/Main.java ch/qos/logback/classic/net/SimpleSocketServer.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				ch/qos/logback/classic/spi/ThrowableProxy.java ch/qos/logback/classic/pattern/TargetLengthBasedClassNameAbbreviator.java com/kotcrab/vis/usl/IncludeLoader.java com/badlogic/gdx/backends/android/surfaceview/GLSurfaceViewAPI18.java com/badlogic/gdx/backends/android/AndroidOnscreenKeyboard.java ch/qos/logback/classic/selector/servlet/ContextDetachingSCL.java com/badlogic/gdx/backends/android/AndroidApplicationLogger.java com/badlogic/gdx/backends/android/ZipResourceFile.java org/slf4j/helpers/Util.java com/badlogic/gdx/backends/android/AndroidGraphicsLiveWallpaper.java
2	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	ch/qos/logback/classic/joran/action/ConfigurationAction.java ch/qos/logback/core/net/ssl/SSL.java ch/qos/logback/core/rolling/helper/DateTokenConverter.java ch/qos/logback/classic/ClassicConstants.java ch/qos/logback/core/CoreConstants.java ch/qos/logback/core/db/BindDataSourceToJNDIAction.java ch/qos/logback/classic/gaffer/GafferConfigurator.java ch/qos/logback/classic/sift/JNDIBasedContextDiscriminator.java ch/qos/logback/core/rolling/helper/IntegerTokenConverter.java ch/qos/logback/classic/sift/ContextBasedDiscriminator.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	com/badlogic/gdx/math/MathUtils.java com/badlogic/gdx/math/RandomXS128.java
4	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 com/badlogic/gdx/files/FileHandle.java com/badlogic/gdx/backends/android/APKExpansionSupport.java
5	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	ch/qos/logback/core/net/ssl/SSLContextFactoryBean.java
6	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/files/FileHandle.java com/badlogic/gdx/utils/SharedLibraryLoader.java
7	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

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided 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 no hardware resources.
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 no 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_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_HTTPS_EXT.1.3	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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
logback.qos.ch	ok	**IP:** 83.173.251.158 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	**IP:** 83.166.144.67 **Country:** Switzerland **Region:** Geneve **City:** Carouge **Latitude:** 46.180962 **Longitude:** 6.139210 **View:** Google Map
apps.kotcrab.com	ok	**IP:** 178.62.128.93 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
raw.githubusercontent.com	ok	**IP:** 185.199.110.133 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.w3.org	ok	**IP:** 128.30.52.100 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.365078 **Longitude:** -71.104523 **View:** Google Map

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.