MOBSF

ANDROID STATIC ANALYSIS REPORT

OgreSampleBrowser (1.12.5)

File Name:	installer3841.apk
Package Name:	org.ogre.browser
Scan Date:	May 31, 2022, 6:49 p.m.
App Security Score:	56/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	1	0	1	0

FILE INFORMATION

File Name: installer3841.apk
Size: 56.06MB
MD5: 4e7ea9ba322be2cd55f8991f6d11ae3d
SHA1: 3be7875b60e6a899edc38ba5c72756ec27edca3e
SHA256: 637a3bb0e8e8e711e02020228e1f67c2270529d2f1f01618722c05badf7aadff

APP INFORMATION

App Name: OgreSampleBrowser
Package Name: org.ogre.browser
Main Activity: android.app.NativeActivity
Target SDK: 26
Min SDK: 16
Max SDK:
Android Version Name: 1.12.5
Android Version Code: 15

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: 2017-08-07 04:36:47+00:00
Valid To: 2044-12-23 04:36:47+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x7488f0d8
Hash Algorithm: sha256
md5: 042b15c0036c858c2883f27e8a1699ec
sha1: 82debe6c804b1048954a193724265cbc17fbeda2
sha256: 0223694a1136e25ee07dd896ad1358d73eb7bce7aa0b77895cb0a5f1bb49be2e
sha512: ba976c9f6d5c6ff0b518312f8583d813676ee0657b43a8343de377f6af19613725fb50acc674460855895e787500e3c16e40202fb0151c9c7ef2c5abfa99cbe6

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] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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

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/x86/libOgreSampleBrowser.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
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 no hardware resources.
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 no network communications.
6	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.
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 encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.ogre3d.org	ok	**IP:** 46.43.2.142 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** York **Latitude:** 53.957630 **Longitude:** -1.082710 **View:** Google Map
android.googlesource.com	ok	**IP:** 142.250.27.82 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
users.ox.ac.uk	ok	**IP:** 163.1.221.183 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** Oxford **Latitude:** 51.752220 **Longitude:** -1.255960 **View:** Google Map

EMAILS

EMAIL	FILE
paul.baker@univ.ox	lib/x86/libOgreSampleBrowser.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.