



ANDROID STATIC ANALYSIS REPORT



 Shattered Pixel Dungeon (0.9.0)

File Name: installer72.apk

Package Name: com.shatteredpixel.shatteredpixeldungeon






Scan Date: May 31, 2022, 9:15 a.m.

App Security Score: 61/100 (LOW RISK)

Grade:



FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
0	5	1	1	0

FILE INFORMATION

File Name: installer72.apk

Size: 7.91MB

MD5: fbe944852cbd1bd80ca699c205685433

SHA1: 19c1465aa853b45ba0a37172c159185388a18ee9

SHA256: 5aa367de35924f4023d600ef2830bf730d8bce4d5d4562e2f5c5b79f49867777

APP INFORMATION

App Name: Shattered Pixel Dungeon

Package Name: com.shatteredpixel.shatteredpixeldungeon

Main Activity: com.shatteredpixel.shatteredpixeldungeon.android.AndroidLauncher

Target SDK: 30

Min SDK: 9

Max SDK:

Android Version Name: 0.9.0

Android Version Code: 480

APP COMPONENTS

Activities: 2

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: True

v3 signature: True

Found 1 unique certificates

Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2014-11-15 07:10:38+00:00

Valid To: 2042-04-02 07:10:38+00:00

Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Serial Number: 0x253c584d

Hash Algorithm: sha256

md5: 0e3ac1330f0873643ad72fa31a40c25a

sha1: 61278137e8a6a1ff2c1e67cde97bc626d959d8f6

sha256: 92a8d7a96447565aed749b12b03251842d65a7354ba67dc2443f4224d772f61c

sha512: e78a721cac0bbbfe59c54698d3b9b4a7fa9f8b6ffc3306da31df9622d2823dcc8c5a945523470487d12c77e7e3777571166912e7e762dc0cd9dbbb43f0570776

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 1d74f5c8316f0d08a82aeb41026ba9d477001dd0d434eaefb733b5f0f159b4ac

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

APKID ANALYSIS

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Compiler	r8

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
				com/shatteredpixel/shatteredpixeldungeon/items/wands/WandOfCorruption.java com/shatteredpixel/shatteredpixeldungeon/items/potions/PotionOfMindVision.java com/shatteredpixel/shatteredpixeldungeon/windows/WndSadGhost.java com/shatteredpixel/shatteredpixeldungeon/levels/traps/DisarmingTrap.java com/shatteredpixel/shatteredpixeldungeon/items/scrolls/ScrollOfLullaby.java com/shatteredpixel/shatteredpixeldungeon/actors/mobs/NewDM300.java com/shatteredpixel/shatteredpixeldungeon/items/ques

NO	ISSUE	SEVERITY	STANDARDS	FILES
				t/Pickaxe.java com/shatteredpixel/shatteredpixeldungeon/actors/mobs/Mimic.java com/shatteredpixel/shatteredpixeldungeon/items/TomeOfMastery.java com/shatteredpixel/shatteredpixeldungeon/items/potions/PotionOfLevitation.java com/shatteredpixel/shatteredpixeldungeon/items/DewVial.java com/shatteredpixel/shatteredpixeldungeon/items/scrolls/ScrollOfTerror.java com/shatteredpixel/shatteredpixeldungeon/items/artifacts/EtherealChains.java a/b/a/m/a/b.java com/shatteredpixel/shatteredpixeldungeon/items/EquipableItem.java com/shatteredpixel/shatteredpixeldungeon/actors/mobs/CrystalMimic.java com/shatteredpixel/shatteredpixeldungeon/items/food/Food.java com/shatteredpixel/shatteredpixeldungeon/items/artifacts/HornOfPlenty.java com/shatteredpixel/shatteredpixeldungeon/items/artifacts/TimekeepersHourglass.java com/shatteredpixel/shatteredpixeldungeon/items/scrolls/exotic/ScrollOfPassage.java com/shatteredpixel/shatteredpixeldungeon/items/artifacts/AlchemistsToolkit.java com/shatteredpixel/shatteredpixeldungeon/items/potions/Potion.java com/shatteredpixel/shatteredpixeldungeon/items/armor/Armor.java com/shatteredpixel/shatteredpixeldungeon/actors/mobs/DM201.java com/shatteredpixel/shatteredpixeldungeon/levels/traps/TeleportationTrap.java com/shatteredpixel/shatteredpixeldungeon/levels/traps/PitfallTrap.java com/shatteredpixel/shatteredpixeldungeon/items/artifacts/ChaliceOfBlood.java a/b/a/m/a/y/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/shatteredpixel/shatteredpixeldungeon/items/scrol ls/ScrollOfRemoveCurse.java com/shatteredpixel/shatteredpixeldungeon/actors/buff s/Burning.java com/shatteredpixel/shatteredpixeldungeon/actors/mo bs/RipperDemon.java com/shatteredpixel/shatteredpixeldungeon/items/spell s/PhaseShift.java com/shatteredpixel/shatteredpixeldungeon/actors/mo bs/Thief.java com/watabou/noosa/Game.java com/shatteredpixel/shatteredpixeldungeon/actors/mo bs/GoldenMimic.java com/shatteredpixel/shatteredpixeldungeon/items/food /MysteryMeat.java com/shatteredpixel/shatteredpixeldungeon/levels/trap s/AlarmTrap.java com/shatteredpixel/shatteredpixeldungeon/items/poti ons/PotionOfInvisibility.java com/shatteredpixel/shatteredpixeldungeon/items/artif acts/Artifact.java com/shatteredpixel/shatteredpixeldungeon/scenes/Ga meScene.java com/shatteredpixel/shatteredpixeldungeon/actors/buff s/Combo.java com/shatteredpixel/shatteredpixeldungeon/items/artif acts/LloydsBeacon.java com/shatteredpixel/shatteredpixeldungeon/items/arm or/ClassArmor.java com/shatteredpixel/shatteredpixeldungeon/items/spell s/BeaconOfReturning.java com/shatteredpixel/shatteredpixeldungeon/actors/buff s/Hunger.java com/shatteredpixel/shatteredpixeldungeon/items/spell s/MagicalPorter.java com/shatteredpixel/shatteredpixeldungeon/items/artif acts/TalismanOfForesight.java com/shatteredpixel/shatteredpixeldungeon/plants/Fad eleaf.java com/shatteredpixel/shatteredpixeldungeon/actors/mo bs/DM200.java

NO 1	ISSUE The App logs information. Sensitive information should never be logged.	SEVERITY info	CWE: CWE-532: Insertion of Sensitive Information into Log File STANDARDS OWASP MASVS: MSTG-STORAGE-3	FILES com/shatteredpixel/shatteredpixeldungeon/actors/buffs/Preparation.java com/shatteredpixel/shatteredpixeldungeon/items/weapon/missiles/MissileWeapon.java com/shatteredpixel/shatteredpixeldungeon/items/food/FrozenCarpaccio.java com/shatteredpixel/shatteredpixeldungeon/actors/hero/Hero.java com/badlogic/gdx/graphics/glutils/ETC1.java com/shatteredpixel/shatteredpixeldungeon/items/Dewdrop.java com/shatteredpixel/shatteredpixeldungeon/actors/Character.java com/shatteredpixel/shatteredpixeldungeon/items/scrolls/ScrollOfUpgrade.java com/shatteredpixel/shatteredpixeldungeon/items/scrolls/ScrollOfRage.java com/shatteredpixel/shatteredpixeldungeon/items/artifacts/CloakOfShadows.java com/shatteredpixel/shatteredpixeldungeon/windows/WndImp.java com/shatteredpixel/shatteredpixeldungeon/windows/WndWandmaker.java com/shatteredpixel/shatteredpixeldungeon/items/scrolls/ScrollOfIdentify.java com/shatteredpixel/shatteredpixeldungeon/actors/mobs/npcs/Blacksmith.java com/shatteredpixel/shatteredpixeldungeon/actors/mobs/YogFist.java com/shatteredpixel/shatteredpixeldungeon/items/spells/Alchemize.java com/shatteredpixel/shatteredpixeldungeon/items/armor/HuntressArmor.java com/shatteredpixel/shatteredpixeldungeon/items/scrolls/ScrollOfRecharging.java a/b/a/m/a/y/c.java com/shatteredpixel/shatteredpixeldungeon/actors/buffs/Frost.java com/shatteredpixel/shatteredpixeldungeon/windows/WndSettings.java com/shatteredpixel/shatteredpixeldungeon/items/wan
---------	--	------------------	--	---

NO	ISSUE	SEVERITY	STANDARDS	FILES
				<div>ds/WandOfWarding.java</div> <div>com/shatteredpixel/shatteredpixeldungeon/items/scrol</div> <div>ls/ScrollOfTeleportation.java</div> <div>com/shatteredpixel/shatteredpixeldungeon/items/wea</div> <div>pon/melee/MagesStaff.java</div> <div>com/shatteredpixel/shatteredpixeldungeon/actors/mo</div> <div>bs/NewTengu.java</div> <div>com/shatteredpixel/shatteredpixeldungeon/items/spell</div> <div>s/Spell.java</div> <div>com/shatteredpixel/shatteredpixeldungeon/items/Brok</div> <div>enSeal.java</div> <div>com/shatteredpixel/shatteredpixeldungeon/levels/trap</div> <div>s/GuardianTrap.java</div> <div>com/shatteredpixel/shatteredpixeldungeon/items/wan</div> <div>ds/Wand.java</div> <div>com/shatteredpixel/shatteredpixeldungeon/items/Styl</div> <div>us.java</div> <div>com/shatteredpixel/shatteredpixeldungeon/items/scrol</div> <div>ls/Scroll.java</div> <div>a/b/a/m/a/y/b.java</div> <div>com/shatteredpixel/shatteredpixeldungeon/actors/buff</div> <div>s/MagicalSleep.java</div> <div>com/shatteredpixel/shatteredpixeldungeon/items/spell</div> <div>s/ReclaimTrap.java</div> <div>com/shatteredpixel/shatteredpixeldungeon/items/food</div> <div>/Blandfruit.java</div> <div>com/shatteredpixel/shatteredpixeldungeon/items/wan</div> <div>ds/CursedWand.java</div> <div>com/shatteredpixel/shatteredpixeldungeon/items/artif</div> <div>acts/DriedRose.java</div> <div>com/shatteredpixel/shatteredpixeldungeon/items/Arm</div> <div>orKit.java</div> <div>com/shatteredpixel/shatteredpixeldungeon/items/artif</div> <div>acts/SandalsOfNature.java</div> <div>com/shatteredpixel/shatteredpixeldungeon/items/scrol</div> <div>ls/ScrollOfMagicMapping.java</div> <div>com/shatteredpixel/shatteredpixeldungeon/levels/trap</div> <div>s/WarpingTrap.java</div> <div>com/shatteredpixel/shatteredpixeldungeon/actors/mo</div> <div>bs/Mob.java</div> <div>com/shatteredpixel/shatteredpixeldungeon/items/plants/Dre</div>

NO	ISSUE	SEVERITY	STANDARDS	FILES
				amfoil.java com/shatteredpixel/shatteredpixeldungeon/items/artif acts/CapeOfThorns.java com/shatteredpixel/shatteredpixeldungeon/items/bom bs/Bomb.java com/shatteredpixel/shatteredpixeldungeon/items/arm or/RogueArmor.java com/shatteredpixel/shatteredpixeldungeon/levels/Leve l.java com/shatteredpixel/shatteredpixeldungeon/scenes/Int erlevelScene.java com/shatteredpixel/shatteredpixeldungeon/items/artif acts/UnstableSpellbook.java com/shatteredpixel/shatteredpixeldungeon/items/poti ons/PotionOfPurity.java com/shatteredpixel/shatteredpixeldungeon/items/poti ons/PotionOfHaste.java
2	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/watabou/utils/Random.java a/b/a/p/b.java a/b/a/p/a.java com/shatteredpixel/shatteredpixeldungeon/levels/roo ms/standard/EntranceRoom.java com/shatteredpixel/shatteredpixeldungeon/scenes/Int erlevelScene.java
3	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	a/b/a/r/p.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	a/b/a/m/a/i.java

🚩 SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/armeabi-v7a/libgdx-freetype.so	<p>True info</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 info</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 info</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 info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/armeabi-v7a/libgdx.so	<p>True info</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 info</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 info</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 info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/x86/libgdx-freetype.so	<p>True info</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 info</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 info</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 info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/x86/libgdx.so	<p>True info</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 info</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 info</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 info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/arm64-v8a/libgdx-freetype.so	<p>True info</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 info</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>Partial RELRO warning</p> <p>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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	lib/arm64-v8a/libgdx.so	<p>True info</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 info</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>Partial RELRO warning</p> <p>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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	lib/armeabi/libgdx-freetype.so	<p>True info</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 info</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 info</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 info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	lib/armeabi/libgdx.so	<p>True info</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 info</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 info</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 info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	lib/x86_64/libgdx-freetype.so	<p>True info</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 info</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 info</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 info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	lib/x86_64/libgdx.so	<p>True info</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 info</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 info</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 info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
libgdx.badlogicgames.com	ok	IP: 95.216.8.184 Country: Finland Region: Uusimaa City: Helsinki Latitude: 60.169521 Longitude: 24.935450 View: Google Map
s9menine.itch.io	ok	IP: 173.255.250.29 Country: United States of America Region: California City: Fremont Latitude: 37.548271 Longitude: -121.988571 View: Google Map
pixeldungeon.watabou.ru	ok	IP: 91.189.114.20 Country: Russian Federation Region: Tul'skaya oblast' City: Donskoy Latitude: 53.971062 Longitude: 38.336269 View: Google Map
twitter.com	ok	IP: 104.244.42.1 Country: United States of America Region: California City: San Francisco Latitude: 37.773968 Longitude: -122.410446 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.alekskomitov.com	ok	IP: 34.117.168.233 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
api.github.com	ok	IP: 140.82.121.5 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
www.transifex.com	ok	IP: 34.254.213.30 Country: Ireland Region: Dublin City: Dublin Latitude: 53.343990 Longitude: -6.267190 View: Google Map
www.freesound.org	ok	IP: 84.89.139.206 Country: Spain Region: Catalunya City: Barcelona Latitude: 41.388790 Longitude: 2.158990 View: Google Map

DOMAIN	STATUS	GEOLOCATION
shatteredpixel.com	ok	IP: 185.199.109.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 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
www.patreon.com	ok	IP: 104.16.7.49 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

EMAILS

EMAIL	FILE
evan@shatteredpixel.com	com/shatteredpixel/shatteredpixeldungeon/android/AndroidLauncher.java

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](#).