

### ANDROID STATIC ANALYSIS REPORT



• Mines3D (1.3)

File Name:	installer180.apk			
Package Name:	cos.premy.mines			
Scan Date:	May 31, 2022, 4:17 p.m.			
App Security Score:	67/100 (LOW RISK)			
Grade:	A			

#### FINDINGS SEVERITY

<b>派</b> HIGH	▲ MEDIUM	<b>i</b> INFO	✓ SECURE	<b>्र</b> HOTSPOT
0	3	1	1	0

#### FILE INFORMATION

File Name: installer180.apk

**Size:** 1.43MB

MD5: 932ee43daf0d5b73d363fd2dd7c39b10

**SHA1**: 24abbcb994d2627fa436517726de309a62ee3c0e

**SHA256**: 533fa559825ce735f85bbacf1f93907d8b7aef570172bb6e828a6203873d4329

### **i** APP INFORMATION

App Name: Mines3D

Package Name: cos.premy.mines

Main Activity: cos.premy.mines.MainActivity

Target SDK: 28 Min SDK: 19 Max SDK:

Android Version Name: 1.3 Android Version Code: 5

#### **APP COMPONENTS**

Activities: 3 Services: 0 Receivers: 0 Providers: 0

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

## **\*** CERTIFICATE INFORMATION

APK is signed v1 signature: True v2 signature: True v3 signature: False

Found 1 unique certificates Subject: CN=Premysl Štastný

Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2017-11-11 16:55:33+00:00 Valid To: 2042-11-05 16:55:33+00:00

Issuer: CN=Premysl Štastný Serial Number: 0x2389947f Hash Algorithm: sha256

md5: 71c0a20317269a52c65a0bcbfa332f09

sha1: 53eea283c64ed2dbbec5983e89fbd5e8abfb5804

sha256: 0449fbf6244098c563ff2ac98302bce4504c5b0af8c816dfff3b9348602e42f6

sha512: 96396fb7ed77588566f0ff9f164bd190ef2f197785cb2dd701ff635824c55006e50762ea1826a93f926e541b33ee8d1fe72b0d5e3a4b5deebe17f88b277a9d07

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 138bc9cddc3236aaec343536d5eec624dc6b5b528aef584ddf12f18554af0be4

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.

# **命 APKID ANALYSIS**

FILE	DETAILS				
classes.dex	FINDINGS	DETAILS			
	Compiler	unknown (please file detection issue!)			

## **△** 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	a/b/f/i/c.java a/b/f/i/t.java a/b/f/b/e.java a/b/f/b/f.java a/b/f/i/v.java a/b/f/h/e.java a/b/g/e/g.java a/b/e/f0.java a/b/f/b/i.java a/b/f/b/i.java a/b/f/a/d/f.java a/b/g/b/a/a.java a/b/f/a/d/b.java a/b/f/a/d/b.java a/b/f/b/i.java a/b/e/e0.java a/b/f/i/h.java a/b/f/i/h.java a/b/f/i/h.java a/b/f/i/h.java a/b/f/i/h.java a/b/f/i/h.java a/b/f/i/h.java a/b/e/g0.java a/b/e/g0.java a/b/e/y.java a/b/e/y.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	cos/premy/mines/i/b.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/libnative- lib.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/x86/libnative-lib.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/arm64-v8a/libnative-lib.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.	True info The shared object has the following fortified functions: ['vsnprintf_chk', 'strlen_chk', 'memmove_chk']	True info Symbols are stripped.

NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/x86_64/libnative-lib.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.	True info The shared object has the following fortified functions: ['memmove_chk', 'strlen_chk', 'vsnprintf_chk']	True info Symbols are stripped.

# ■ NIAP ANALYSIS v1.3

ОИ	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 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 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
schemas.android.com	ok	No Geolocation information available.

#### 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.