# MOBSF

## ANDROID STATIC ANALYSIS REPORT

Block Puzzle (2.0)

| | |
|---|---|
| File Name: | installer275.apk |
| Package Name: | de.mwvb.blockpuzzle |
| Scan Date: | May 31, 2022, 10:18 a.m. |
| App Security Score: | 67/100 (LOW RISK) |
| Grade: | A |

# FINDINGS SEVERITY

| HIGH | MEDIUM | INFO | SECURE | HOTSPOT |
|---|---|---|---|---|
| 0 | 3 | 0 | 1 | 0 |

# FILE INFORMATION

**File Name:** installer275.apk
**Size:** 3.07MB
**MD5:** 2734f85adba98559d96bf3072aec900a
**SHA1:** 12a58bd59d4dab259f787bc440406d99026a7dc7
**SHA256:** ea1c359f145a54c71ab9219d1b744b2ba0e5c34f9e961dadcedff7e4454451cb

# APP INFORMATION

**App Name:** Block Puzzle
**Package Name:** de.mwvb.blockpuzzle
**Main Activity:** de.mwvb.blockpuzzle.MainActivity
**Target SDK:** 30
**Min SDK:** 19
**Max SDK:**
**Android Version Name:** 2.0
**Android Version Code:** 20

# APP COMPONENTS

**Activities:** 1
**Services:** 0
**Receivers:** 0
**Providers:** 1
**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: 2020-10-07 10:24:16+00:00
Valid To: 2048-02-23 10:24:16+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0xbbfbc7ec5880ea71
Hash Algorithm: sha256
md5: b6f5182cc766794b2ba9239a8ca76b03
sha1: e5aa29389f33ad7b9f25f948932fd4daf08a69cb
sha256: 3e20d64ec8d39760698cf45fc529411603d117986094bc360ff75421d3293e6b
sha512: cbb8894be17d3cc8fd033788b4f05ccde0cc237f603bcc20d63445222ef975b7a74aed7e86e28fd5e13d7273112d0aa21242e6afc53e3f303c9e4874fc3059bf
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 4dc504d626720c28c4cb3368e4096e7110685bf47e7b8d03152f5707daa32d6f

| 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. |

# APKID ANALYSIS

| FILE | DETAILS |
| --- | --- |
| classes.dex | FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check<br>Build.MANUFACTURER check<br>FINDINGS: Compiler — DETAILS: 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 |
|---|---|---|---|---|
| 1 | The App uses an insecure Random Number Generator. | warning | CWE: CWE-330: Use of Insufficiently Random Values<br>OWASP Top 10: M5: Insufficient Cryptography<br>OWASP MASVS: MSTG-CRYPTO-6 | de/mwvb/blockpuzzle/logic/Game.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 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. |

| NO | IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|---|---|---|---|---|
| 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 implement functionality to encrypt sensitive data 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. |

---

## 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.