# MOBSF

## ANDROID STATIC ANALYSIS REPORT

GM Dice (0.1.6)

| | |
|---|---|
| File Name: | installer140.apk |
| Package Name: | de.duenndns.gmdice |
| Scan Date: | May 31, 2022, 5:01 p.m. |
| App Security Score: | 44/100 (MEDIUM RISK) |
| Grade: | B |

# FINDINGS SEVERITY

| HIGH | MEDIUM | INFO | SECURE | HOTSPOT |
|---|---|---|---|---|
| 2 | 2 | 1 | 1 | 0 |

# FILE INFORMATION

**File Name:** installer140.apk
**Size:** 0.06MB
**MD5:** a89fea1b09b301c4399932f3670f8285
**SHA1:** 832ef6273c7b3e511c54206f8631b277325b98f3
**SHA256:** 2f890455cbbc91de2fe040f62ee45073dfb94ee6c494147bc35e6460e741ad74

# APP INFORMATION

**App Name:** GM Dice
**Package Name:** de.duenndns.gmdice
**Main Activity:** .GameMasterDice
**Target SDK:** 8
**Min SDK:** 3
**Max SDK:**
**Android Version Name:** 0.1.6
**Android Version Code:** 7

# 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: 2012-04-20 09:46:49+00:00
Valid To: 2039-09-06 09:46:49+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x4f913089
Hash Algorithm: sha1
md5: 72f304e7b801e940fa6d144f993af805
sha1: 3b68f191a21bbe71821bf255c33382b4f5522454
sha256: a26b42202e9fed321295dd0be832a8fd8babaf875385f2e916b571633dff181e
sha512: 4edd718a69a2a1006296361559357b0d96299fec5e78f887f493e39ae79a42d027fab27bbaf1b22a9340aaf12156a11504059547181ac2b39a89e43352a99c52

| 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. |
| Certificate algorithm might be vulnerable to hash collision | high | Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. |

# APKID ANALYSIS

| FILE | DETAILS |
| --- | --- |
| classes.dex | FINDINGS: DETAILS<br>Compiler: dx (possible dexmerge)<br>Manipulator Found: dexmerge |

# NETWORK SECURITY

| NO | SCOPE | SEVERITY | DESCRIPTION |
| --- | --- | --- | --- |

# MANIFEST ANALYSIS

| 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 |
|---|---|---|---|---|
| 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/duenndns/gmdice/StandardDiceSet.java<br>de/duenndns/gmdice/DiceSet.java<br>de/duenndns/gmdice/DSADiceSet.java<br>de/duenndns/gmdice/Coin.java<br>de/duenndns/gmdice/FUDGEDiceSet.java<br>de/duenndns/gmdice/GameMasterDice.java |
| 2 | The App logs information. Sensitive information should never be logged. | info | CWE: CWE-532: Insertion of Sensitive Information into Log File<br>OWASP MASVS: MSTG-STORAGE-3 | de/duenndns/gmdice/GameMasterDice.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. |
| 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. |

# DOMAIN MALWARE CHECK

| DOMAIN | STATUS | GEOLOCATION |
| --- | --- | --- |
| github.com | ok | **IP:** 140.82.121.3<br>**Country:** United States of America<br>**Region:** California<br>**City:** San Francisco<br>**Latitude:** 37.775700<br>**Longitude:** -122.395203<br>**View:** Google Map |
| www.gnu.org | ok | **IP:** 209.51.188.116<br>**Country:** United States of America<br>**Region:** Massachusetts<br>**City:** Boston<br>**Latitude:** 42.358429<br>**Longitude:** -71.059769<br>**View:** Google Map |

# EMAILS

| EMAIL | FILE |
| --- | --- |
| georg@op-co.de | Android String Resource |

---

## 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.