# ANDROID STATIC ANALYSIS REPORT

## Cards Score Keeper (1.0.3)

| | |
|---|---|
| File Name: | installer3773.apk |
| Package Name: | io.github.thachillera.cardsscorekeeper |
| Scan Date: | May 31, 2022, 7:22 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:** installer3773.apk
**Size:** 2.01MB
**MD5:** 5538cc4ef00992477e3d05291874fa05
**SHA1:** cab01d6bb2fd758d59e3ba9c7cedf57b20a9c7b4
**SHA256:** e0962d0e3b5ea7bc481f6ddbf912af81d7914afbf07a438b83ae4ad7015865f5

# APP INFORMATION

**App Name:** Cards Score Keeper
**Package Name:** io.github.thachillera.cardsscorekeeper
**Main Activity:** io.github.thachillera.cardsscorekeeper.interfaces.GameSelectActivity
**Target SDK:** 28
**Min SDK:** 25
**Max SDK:**
**Android Version Name:** 1.0.3
**Android Version Code:** 3

# APP COMPONENTS

**Activities:** 4<br>
**Services:** 0<br>
**Receivers:** 0<br>
**Providers:** 0<br>
**Exported Activities:** 0<br>
**Exported Services:** 0<br>
**Exported Receivers:** 0<br>
**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: 2019-12-20 06:55:48+00:00
Valid To: 2047-05-07 06:55:48+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x6fa27005
Hash Algorithm: sha256
md5: 283f4fe91c74a915ab0f35ce5bcbd7a9
sha1: 0ff050eb95ef24a79cc3d3909380721fbbcaae1c
sha256: eb7e62b1bc14a33cf1b326577f62d593392c84f8ad8f0b44a8dc15f1e3a71a09
sha512: 99054f8758e9c780ffd7932c7c217e1bcabfa97e738c05676512bce415cc7189cdd052d4c80cccf65eb7398adc103a7a0c257633ddbc55caf6ad2acf1b131b9f
```

| 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

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8</td></tr></table></td></tr>
</table>

## 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=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 |
|---|---|---|---|---|

## 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. |

| NO | IDENTIFIER | REQUIREMENT | FEATURE | DESCRIPTION |
|---|---|---|---|---|
| 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. |

## 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.