ANDROID STATIC ANALYSIS REPORT

Sudoku (3.0.1)

File Name:	installer48.apk
Package Name:	org.secuso.privacyfriendlysudoku
Scan Date:	May 31, 2022, 10:30 a.m.
App Security Score:	**46/100 (MEDIUM RISK)**
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
2	5	2	1	0

FILE INFORMATION

File Name: installer48.apk
Size: 3.18MB
MD5: 3da4b55b52ad668d7a88c8c731f76519
SHA1: 012a0d40c76156c28fc01f437a58c36d337c3e4b
SHA256: d5399428e1ffc5982e82e188b70b91dd9d445f6411dec82659167c6cedd46896

APP INFORMATION

App Name: Sudoku
Package Name: org.secuso.privacyfriendlysudoku
Main Activity: org.secuso.privacyfriendlysudoku.ui.SplashActivity
Target SDK: 29
Min SDK: 16
Max SDK:
Android Version Name: 3.0.1
Android Version Code: 10

APP COMPONENTS

Activities: 11
Services: 1
Receivers: 0
Providers: 0
Exported Activities: 1
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: 2016-03-27 20:47:08+00:00
Valid To: 2043-08-13 20:47:08+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x1c564d6b
Hash Algorithm: sha256
md5: 9df81d93f2557c227b1f10d04a52f4db
sha1: 7c3d739c860c1ae53402d4fcfc07a4e9a42afec3
sha256: 2715af26961bf27383ac5efcd3aa7203c1004d189e9b2d7d5f6d7386cd8095d8
sha512: 9e9ff66d833da9bac1df695a1cec274e60fbc6a57a902677c4e2a02852c8c9bb9c5a4999fb47b56a0891b59555ec0de167f1e8b4529b595057c078541a6d3649
```

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.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

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>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
org.secuso.privacyfriendlysudoku.ui.GameActivity	Schemes: sudoku://, http://, https://, Hosts: sudoku.secuso.org,

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.
2	Launch Mode of Activity (org.secuso.privacyfriendlysudoku.ui.GameActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
3	Activity (org.secuso.privacyfriendlysudoku.ui.GameActivity) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.

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	org/secuso/privacyfriendlysudoku/controller/GameStateManager.java org/secuso/privacyfriendlysudoku/controller/NewLevelManager.java org/secuso/privacyfriendlysudoku/controller/GeneratorService.java org/secuso/privacyfriendlysudoku/controller/QQWingController.java org/secuso/privacyfriendlysudoku/controller/qqwing/LogItem.java org/secuso/privacyfriendlysudoku/controller/qqwing/QQWing.java org/secuso/privacyfriendlysudoku/controller/SaveLoadStatistics.java org/secuso/privacyfriendlysudoku/controller/helper/GameInfoContainer.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	org/secuso/privacyfriendlysudoku/controller/NewLevelManager.java org/secuso/privacyfriendlysudoku/controller/QQWingController.java org/secuso/privacyfriendlysudoku/controller/qqwing/QQWing.java
3	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	org/secuso/privacyfriendlysudoku/controller/database/DatabaseHelper.java org/secuso/privacyfriendlysudoku/controller/database/migration/MigrationUtil.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	org/secuso/privacyfriendlysudoku/ui/GameActivity.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 implement functionality to encrypt sensitive data in non-volatile memory.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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
sudoku.secuso.org	ok	**IP:** 129.13.152.9 **Country:** Germany **Region:** Baden-Wurttemberg **City:** Oststadt **Latitude:** 49.009560 **Longitude:** 8.424540 **View:** Google Map
qqwing.com	ok	**IP:** 52.9.93.147 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.774929 **Longitude:** -122.419418 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"about_author" : "Authors:"
"about_author" : "作者:"
"about_author_contributors" : "と貢献者。"
"about_author" : "Autorzy:"
"about_author" : "Fejlesztők:"
"about_author" : "Autoren:"
"about_author" : "作者："
"about_author" : "Autor:"
"about_author" : "Авторы："

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.