MOBSF

ANDROID STATIC ANALYSIS REPORT

Open Sudoku (3.5.1)

File Name:	installer380.apk
Package Name:	org.moire.opensudoku
Scan Date:	May 31, 2022, 4:47 p.m.
App Security Score:	57/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	8	1	1	1

FILE INFORMATION

File Name: installer380.apk
Size: 1.45MB
MD5: 89996dcae62d891f25ce5b218030b478
SHA1: d3e3f30f94d0ffa76d449a9aed95128e4f58590d
SHA256: 532addd08263f0a959cc29f7e998f0a9c8bd7675b5f2581903655d0ab8d823ae

APP INFORMATION

App Name: Open Sudoku
Package Name: org.moire.opensudoku
Main Activity: org.moire.opensudoku.gui.TitleScreenActivity
Target SDK: 30
Min SDK: 14
Max SDK:
Android Version Name: 3.5.1
Android Version Code: 20201017

APP COMPONENTS

Activities: 11
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 4
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: 2018-06-02 05:14:20+00:00
Valid To: 2045-10-18 05:14:20+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x1c2d48b1
Hash Algorithm: sha256
md5: a3536645310b57ef46b315ebb9be6267
sha1: 5c9933e03adcf2ada180ecffb4feff37a5882388
sha256: a54ce29ebb02fcb9b478620572f7c4dd39b903736fe6199687471ba729f4613a
sha512: 6e8e7bed988014565aa443a63e930e9990f259df5338a94003b28769a88840629ff21e47482462e94236d0eee8749fba318775351e683e7b69ffcebdb53d0333
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: bdc6e26d75f595b1a3d81f94f9917f686387c8268bb6dff31cd7ebd7611c028f

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.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
org.moire.opensudoku.gui.FileImportActivity	Schemes: file://, http://, Hosts: *, Path Patterns: .*\\.sdm, .*\\.opensudoku,

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	Activity (org.moire.opensudoku.gui.SudokuEditActivity) 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.
3	Activity (org.moire.opensudoku.gui.FileImportActivity) 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.
4	Activity (org.moire.opensudoku.gui.ImportSudokuActivity) 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.
5	Activity (org.moire.opensudoku.gui.SudokuImportActivity) 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
				b/d/k/s.java b/d/k/t.java b/d/d/c/b.java b/d/e/j.java

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	b/d/d/c/a.java b/d/g/b.java org/moire/opensudoku/gui/f1.java b/d/k/v.java b/d/k/b.java b/a/k/a/a.java org/moire/opensudoku/gui/n1/a.java b/k/a/a/h.java org/moire/opensudoku/gui/SudokuExportActivity.java org/moire/opensudoku/gui/SudokuImportActivity.java b/d/k/a0.java org/moire/opensudoku/gui/m1/b.java b/d/g/b.java b/d/e/c.java b/d/k/h.java org/moire/opensudoku/gui/FolderListActivity.java org/moire/opensudoku/gui/SudokuListActivity.java b/d/d/c/f.java b/d/e/g.java c/a/a/b/a.java b/d/e/e.java b/d/e/f.java org/moire/opensudoku/gui/e1.java b/a/o/g.java b/i/a/b.java b/d/k/f.java b/d/e/k.java org/moire/opensudoku/gui/SudokuEditActivity.java b/d/k/b0/c.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	org/moire/opensudoku/gui/FolderListActivity.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	c/a/a/b/b.java c/a/a/b/a.java

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 ['network connectivity'].
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 user/application initiated network communications.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
6	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files 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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
schemas.android.com	ok	No Geolocation information available.
opensudoku.moire.org	ok	**IP:** 188.114.97.0 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **View:** Google Map

EMAILS

EMAIL	FILE
opensudoku@moire.org	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.