

## ANDROID STATIC ANALYSIS REPORT



♠ SudoQ (1.1.0c)

File Name:	installer3840.apk
Package Name:	de.sudoq
Scan Date:	May 31, 2022, 6:45 p.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	

#### FINDINGS SEVERITY

<b>派</b> HIGH	▲ MEDIUM	<b>i</b> INFO	✓ SECURE	♥ HOTSPOT
1	2	1	1	0

#### FILE INFORMATION

File Name: installer3840.apk

Size: 3.67MB

MD5: 7eda910b06fbfb5fcde9a6b33bd18705

SHA1: 74acdd35dd69037d79fb0599e093f43b8facb18d

SHA256: 9b73ca88439f85c32571ef2dceaafc0ddd6c8487fc995730e5f8a8bcb015819f

### **i** APP INFORMATION

App Name: SudoQ

Package Name: de.sudoq

Main Activity: de.sudoq.controller.menus.SplashActivity

Target SDK: 28 Min SDK: 14 Max SDK:

Android Version Name: 1.1.0c Android Version Code: 26

#### **EE** APP COMPONENTS

Activities: 14 Services: 0 Receivers: 0 Providers: 1

Exported Activities: O Exported Services: O Exported Receivers: O Exported Providers: O



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: 2014-08-20 04:53:40+00:00 Valid To: 2042-01-05 04:53:40+00:00

Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Serial Number: 0x30c233e5 Hash Algorithm: sha256

md5: 44eee601cc18846a6d8890dac34904c7

sha1: 122284766be43b2e555f42b999beec7abb3cac66

sha256: 54bb9560503596b26fdc8f4ac082a68c4c565e4289a435169164a03748c66ddb

sha512: 6d17201d158640a39dbefd8b9a5446f1576994e959a56702cc20335596d8ddf7313208b182d2f1cfd75ebda00815024c8bdfc5ce2a12c677ab5c1356f70cb554

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.

# **M** APKID ANALYSIS

FILE	DETAILS		
classes.dex	FINDINGS	DETAILS	
Classes.ucx	Compiler	r8	

## **△** NETWORK SECURITY

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

## **Q** MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

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 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	de/sudoq/model/game/Game.java de/sudoq/model/files/FileManager.java de/sudoq/model/solverGenerator/GenerationAlgo.ja va de/sudoq/model/solverGenerator/transformations/T ransformer.java de/sudoq/model/solverGenerator/Generator.java
				de/sudoq/view/FullScrollLayout.java de/sudoq/model/solverGenerator/FastSolver/DLX1/ AbstractSudokuSolver.java de/sudoq/model/solverGenerator/FastSolver/DLX1/ DancingLinks.java de/sudoq/controller/sudoku/ActionTreeController.ja va de/sudoq/view/SudokuLayout.java dlx/Examples.java de/sudoq/controller/menus/preferences/RestrictTyp esActivity.java de/sudoq/controller/menus/SudokuLoadingActivity.j ava de/sudoq/controller/menus/NewSudokuActivity.java de/sudoq/model/solverGenerator/FastSolver/DLX2/

NO	ISSUE	SEVERITY	STANDARDS	Hexadoku.java <b>អ៊ែស/ចិន្ទ្</b> iveSudokuSolver.java dlx/DefaultHandler.java
2	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	de/sudoq/model/solverGenerator/FastSolver/DLX1/ SamuraiSudokuHandler.java de/sudoq/controller/sudoku/SudokuActivity.java de/sudoq/model/solverGenerator/FastSolver/DLX1/ DLXSudokuSamurai.java de/sudoq/controller/sudoku/hints/HintFormulator.ja va de/sudoq/model/solverGenerator/FastSolver/DLX2/ Samurai.java dlx/VeryNaiveSudokuSolver.java dlx/AbstractSudokuSolver.java de/sudoq/external/dlx/Examples.java dlx/DancingLinks.java de/sudoq/controller/menus/SudokuLoadingAdapter.j ava de/sudoq/model/solverGenerator/GenerationAlgo.ja va de/sudoq/model/solverGenerator/solver/Solver.java de/sudoq/controller/menus/GestureBuilder.java de/sudoq/controller/menus/FrofileListActivity.java de/sudoq/controller/menus/SplashActivity.java de/sudoq/controller/menus/SplashActivity.java de/sudoq/controller/menus/preferences/RestrictTyp esAdapter.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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.
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.

# **Q DOMAIN MALWARE CHECK**

DOMAIN	STATUS	GEOLOCATION
apache.org	ok	IP: 151.101.2.132 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
xml.org	ok	IP: 104.239.240.11 Country: United States of America Region: Texas City: Windcrest Latitude: 29.499678 Longitude: -98.399246 View: Google Map

#### 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.

© 2022 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.