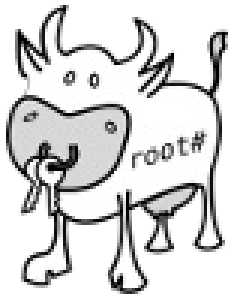
MOBSF

ANDROID STATIC ANALYSIS REPORT



SudoQ (1.0.11c)

File Name:	installer3858.apk
Package Name:	de.sudoq
Scan Date:	May 31, 2022, 6:43 p.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	3	1	1	0

FILE INFORMATION

File Name: installer3858.apk
Size: 2.81MB
MD5: 795a1deaf241c37de696b54b8043da85
SHA1: 914d2a0f408c91ba3d29a6058d848740921daf68
SHA256: a785878187d2ee4185b6c212cd8ee130024552df7cb17bbbca3c07e282947640

APP INFORMATION

App Name: SudoQ
Package Name: de.sudoq
Main Activity: de.sudoq.controller.menus.SplashActivity
Target SDK: 23
Min SDK: 8
Max SDK:
Android Version Name: 1.0.11c
Android Version Code: 21

APP COMPONENTS

Activities: 14
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: True
v3 signature: False
Found 1 unique certificates
Subject: C=DE, ST=Baden-Württemberg, L=Karlsruhe, O=Unknown, OU=Unknown, CN=Jonathan Kieling
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-03-23 10:05:08+00:00
Valid To: 2039-08-09 10:05:08+00:00
Issuer: C=DE, ST=Baden-Württemberg, L=Karlsruhe, O=Unknown, OU=Unknown, CN=Jonathan Kieling
Serial Number: 0x4f6c4ad4
Hash Algorithm: sha1
md5: c71b26f01c41269b940bc7d1b98a0c45
sha1: 913a136add2a05e82ab1ad7fe6e22dc728a0b761
sha256: 338331f29dedcdb505ea66eab75794116d420cbc8d7d6d0f7585a9283fea1e0e
sha512: 9158f5fe6c13a1cd7cf9620d1a8e5933ae43e56347a0405ba330728e4ae25d680fc8ebf3ed62cb48272ae21824aa7e85bf6615a5555ec18196130777b6eadd76
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 4b098754cdc8623b7750f9a209057f12d77ef04946129b381510339c49a6dc73

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.
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: Compiler — DETAILS: dx (possible dexmerge) FINDINGS: Manipulator Found — DETAILS: 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

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	de/sudoq/controller/menus/SudokuLoadingAdapter.java de/sudoq/controller/menus/GestureBuilder.java de/sudoq/controller/menus/ProfileListActivity.java de/sudoq/controller/menus/SplashActivity.java de/sudoq/model/solvingAssistant/SolvingAssistant.java de/sudoq/view/FullScrollLayout.java de/sudoq/controller/menus/preferences/RestrictTypesAdapter.java de/sudoq/controller/sudoku/hints/HintFormulator.java de/sudoq/model/sudoku/sudokuTypes/test4.java de/sudoq/controller/menus/preferences/RestrictTypesActivity.java de/sudoq/controller/menus/SudokuLoadingActivity.java de/sudoq/controller/menus/NewSudokuActivity.java de/sudoq/view/SudokuLayout.java de/sudoq/controller/sudoku/ActionTreeController.java de/sudoq/controller/sudoku/SudokuActivity.java de/sudoq/model/solverGenerator/Generator.java de/sudoq/model/solverGenerator/solver/Solver.java de/sudoq/model/sudoku/sudokuTypes/SudokuType.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	de/sudoq/model/files/FileManager.java de/sudoq/model/game/Game.java de/sudoq/model/solverGenerator/transformations/Transformer.java de/sudoq/model/solverGenerator/Generator.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.
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 not encrypt any data in traffic or does not transmit any data between itself and another trusted IT product.

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.