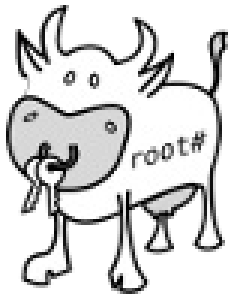
MOBSF

ANDROID STATIC ANALYSIS REPORT



SudoQ (1.0.7)

File Name:	installer44.apk
Package Name:	de.sudoq
Scan Date:	May 31, 2022, 11:11 a.m.
App Security Score:	53/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	4	1	1	0

FILE INFORMATION

File Name: installer44.apk
Size: 2.05MB
MD5: e7b936b8d06fc3f947b0c57068be1c5e
SHA1: 245ac9183bfb8fd794a4d849cd198bc052b0efeb
SHA256: 6ae5c3c2ed25c4a206bb57961212c4bddaeb8beda30866b0e0f0af7133b464b3

APP INFORMATION

App Name: SudoQ
Package Name: de.sudoq
Main Activity: .controller.menus.SplashActivity
Target SDK: 8
Min SDK: 8
Max SDK:
Android Version Name: 1.0.7
Android Version Code: 11

APP COMPONENTS

Activities: 17
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: 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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: DETAILS Compiler: dx (possible dexmerge) Manipulator Found: 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	com/actionbarsherlock/internal/widget/IcsToast.java de/sudoq/controller/sudoku/ActionTreeController.java com/actionbarsherlock/internal/view/menu/MenuItemImpl.java com/actionbarsherlock/internal/widget/ActionBarView.java de/sudoq/view/SudokuLayout.java de/sudoq/controller/menus/GestureBuilder.java de/sudoq/controller/menus/ProfileListActivity.java de/sudoq/model/sudoku/sudokuTypes/SudokuType.java de/sudoq/controller/menus/SplashActivity.java com/actionbarsherlock/internal/nineoldandroids/animation/PropertyValuesHolder.java de/sudoq/controller/menus/SudokuLoadingActivity.java com/actionbarsherlock/widget/SuggestionsAdapter.java de/sudoq/model/solverGenerator/Generator.java de/sudoq/model/solverGenerator/solver/Solver.java com/actionbarsherlock/view/MenuInflater.java de/sudoq/controller/menus/NewSudokuConfigurationActivity.java com/actionbarsherlock/widget/ActivityChooserModel.java com/actionbarsherlock/internal/ActionBarSherlockCompat.java de/sudoq/controller/sudoku/SudokuActivity.java de/sudoq/view/FullScrollLayout.java de/sudoq/controller/menus/SudokuLoadingAdapter.java com/actionbarsherlock/widget/SearchView.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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/solverGenerator/transformations/Transformer.java de/sudoq/model/solverGenerator/Generator.java de/sudoq/model/files/FileManager.java de/sudoq/model/game/Game.java
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/actionbarsherlock/internal/view/menu/MenuBuilder.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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 does not encrypt files 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

DOMAIN	STATUS	GEOLOCATION
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

HARDCODED SECRETS

POSSIBLE SECRETS
"profile_preference_key_id" : "profile_id"
"profile_preference_key_deleted" : "deleted"
"profile_preference_key_name" : "name"
"profile_preference_key_gesture" : "gesture"
"profile_preference_key_cat_profile" : "profilesettings"
"profile_preference_key_cat_assistances" : "assistances"
