MOBSF

ANDROID STATIC ANALYSIS REPORT

🤖 DNSSetter (0.1)

File Name: installer12.apk

Package Name: be.brunoparmentier.dnssetter

Scan Date: May 30, 2022, 3:36 p.m.

App Security Score: 55/100 (MEDIUM RISK)

Grade: B

◕ FINDINGS SEVERITY

🐞 HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
1	2	1	1	0

📦 FILE INFORMATION

File Name: installer12.apk
Size: 0.06MB
MD5: af488de9d005120545db6d45c5f80f21
SHA1: f5967e48fe103c5d976baa5632b002c27ee2b2e6
SHA256: b5275a5a72120d33ce7dd741b76c9d0934640ecded017de5df21e0a44576fbdf

ℹ APP INFORMATION

App Name: DNSSetter
Package Name: be.brunoparmentier.dnssetter
Main Activity: be.brunoparmentier.dnssetter.MainActivity
Target SDK: 21
Min SDK: 15
Max SDK:
Android Version Name: 0.1
Android Version Code: 1

▣▢ APP COMPONENTS

Activities: 2
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: 2014-11-09 07:18:42+00:00
Valid To: 2042-03-27 07:18:42+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x25717383
Hash Algorithm: sha256
md5: e4d78ae9d0524b0ec5f98787869abb03
sha1: 6e822d92607d20fd51ad378da310912aa8c1578c
sha256: 811b3b31906e9545957323f44f3ad48529a79f056c4d1a61a047163d875ccf57
sha512: 48a35ae0fe69efd5359568766b66e0e9cf37860101bc0ebd0cf4ab717eb8308bf52e526de06e418e7fcebbbf383868442856b784dc2d770b64d5555961fe981b

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.ACCESS_SUPERUSER	unknown	Unknown permission	Unknown permission from android reference

⌘ APKID ANALYSIS

FILE	DETAILS	
classes.dex	**FINDINGS**	**DETAILS**
	Compiler	dx

🔒 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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	eu/chainfire/libsuperuser/ShellOnMainThreadException.java eu/chainfire/libsuperuser/Debug.java eu/chainfire/libsuperuser/ShellNotClosedException.java be/brunoparmentier/dnssetter/MainActivity.java eu/chainfire/libsuperuser/StreamGobbler.java eu/chainfire/libsuperuser/HideOverlaysReceiver.java eu/chainfire/libsuperuser/Shell.java eu/chainfire/libsuperuser/Application.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	eu/chainfire/libsuperuser/Debug.java be/brunoparmentier/dnssetter/AboutFragment.java be/brunoparmentier/dnssetter/MainActivity.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 no hardware resources.
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 no network communications.
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 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
www.gnu.org	ok	**IP:** 209.51.188.116 **Country:** United States of America **Region:** Massachusetts **City:** Boston **Latitude:** 42.358429 **Longitude:** -71.059769 **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.