

ANDROID STATIC ANALYSIS REPORT



Selfnet Wi-Fi Setup (1.1.2)

File Name:	installer276.apk
Package Name:	de.selfnet.wifisetup
Scan Date:	May 31, 2022, 9:42 a.m.
App Security Score:	56/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	≪ HOTSPOT
1	1	0	1	1

FILE INFORMATION

File Name: installer276.apk

Size: 0.09MB

MD5: 60b579eb9fecb8869ee2a617a0d42b11

SHA1: c128ea94f3eb08ccb0795c9128c2992eb5c6ff10

SHA256: 9f03c61b419211ed950aa6252caaaee551ce3cd9094e4fc34ed0ce7719d5a79e

i APP INFORMATION

App Name: Selfnet Wi-Fi Setup
Package Name: de.selfnet.wifisetup

Main Activity: de.selfnet.wifisetup.LogonScreen

Target SDK: 26 Min SDK: 23 Max SDK:

Android Version Name: 1.1.2 Android Version Code: 4

EE APP COMPONENTS

Activities: 2 Services: 0 Receivers: 0 Providers: 0

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

***** 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: 2019-06-14 07:37:48+00:00 Valid To: 2046-10-30 07:37:48+00:00

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

Serial Number: 0x7127df9c Hash Algorithm: sha256

md5: b77fe8fa73e6f948a9aa3e29c1f5dd70

sha1: 3d647a3f53002032e76a969c01849e7e4cbbc8b0

sha256: ddf82948260c8672e1b0202cb5931af47166c2c0723874d81735ccf9dca228df

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_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.CHANGE_WIFI_STATE	normal	change Wi- Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.

ক্ল APKID ANALYSIS

FILE	DETAILS			
classes.dex	FINDINGS	DETAILS		
Clusses.dex	Compiler	r8 without marker (suspicious)		



NO	SCOPE	SEVERITY	DESCRIPTION

Q MANIFEST ANALYSIS

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

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	de/selfnet/wifisetup/LogonScreen.jav a

■ NIAP ANALYSIS v1.3

N	Ю	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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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	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.
8	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
--------	--------	-------------

DOMAIN	STATUS	GEOLOCATION
my.selfnet.de	ok	IP: 141.70.124.17 Country: Germany Region: Baden-Wurttemberg City: Stuttgart Latitude: 48.782318 Longitude: 9.177020 View: Google Map
www.selfnet.de	ok	IP: 141.70.124.17 Country: Germany Region: Baden-Wurttemberg City: Stuttgart Latitude: 48.782318 Longitude: 9.177020 View: Google Map

EMAILS

EMAIL	FILE
anonymous@email.service	de/selfnet/wifisetup/LogonScreen.java
support@selfnet.de your@email.com	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.

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