

# ANDROID STATIC ANALYSIS REPORT



NetSwitch (1.2)

File Name:	installer185.apk
Package Name:	cz.antecky.netswitch
Scan Date:	May 31, 2022, 3:25 p.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	

## FINDINGS SEVERITY

<b>兼</b> HIGH	▲ MEDIUM	<b>i</b> INFO	✓ SECURE	<b>ℚ</b> HOTSPOT
1	3	1	1	0

### FILE INFORMATION

File Name: installer185.apk

Size: 0.06MB

MD5: 5e524d2ba406f0e889305135827d90e3

**SHA1**: d7dbd899cd89d089808fa125fbbb00d82d98c58e

SHA256: 3d48c43d15d57978acf9b765b981a4ea00980bb7a904ec824df23521d83f7065

# **i** APP INFORMATION

App Name: NetSwitch

Package Name: cz.antecky.netswitch

Main Activity: Target SDK: 27 Min SDK: 22 Max SDK:

Android Version Name: 1.2 Android Version Code: 3

#### **EE** APP COMPONENTS

Activities: 0 Services: 1 Receivers: 3 Providers: 0

Exported Activities: O Exported Services: O Exported Receivers: 3 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: 2018-02-06 22:04:49+00:00 Valid To: 2045-06-24 22:04:49+00:00

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

Serial Number: 0x327d6f94 Hash Algorithm: sha256

md5: fc1a41302d2b6cae68ad284b90d59344

sha1: 425409cd8eb2cb520eabebeac5140268a15bc9d4

sha256: 6ee656f5b9ee3206ac61f90c99815153866d4eb84a26efb51ae47e16a0626ab1

sha512: 245545c86dc7ea64cef789bb7cbc3b5985a587847908c995f2a9b2b18b794ecbcc281a706faf6ad2872dba439396d0d5b680a4c3c31bc0cc151c04b031abc023

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.

# **M** APKID ANALYSIS

FILE	DETAILS		
classes.dex	FINDINGS	DETAILS	
	Compiler	dx	



NO	SCOPE	SEVERITY	DESCRIPTION	

# **Q** MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Broadcast Receiver (cz.antecky.netswitch.ui.NetSwitchWidget) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
2	Broadcast Receiver (cz.antecky.netswitch.ui.NetSwitchMobileWidget) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
3	Broadcast Receiver (cz.antecky.netswitch.ui.NetSwitchWiFiWidget) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.

# </> CODE ANALYSIS

NO	O 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	cz/antecky/netswitch/b.java a/a/a.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	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.

#### 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 | <u>Ajin Abraham</u> | <u>OpenSecurity</u>.