

#### ANDROID STATIC ANALYSIS REPORT



CCC Camp 2019 Wifi Setup (0.26)

File Name:	installer87.apk
Package Name:	nl.eventinfra.wifisetup
Scan Date:	May 31, 2022, 11:09 a.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	

#### FINDINGS SEVERITY

兼 HIGH	▲ MEDIUM	<b>i</b> INFO	✓ SECURE	ℚ HOTSPOT
1	2	1	1	1

#### FILE INFORMATION

File Name: installer87.apk

Size: 2.24MB

MD5: ba0b5f980551a00242bb7ee7c921a13b

SHA1: 6e44da52b13726d7c752bc87fee369a93342e8a7

SHA256: 36e9392ddb1f6330370abe99c374ec69a5287a3a91fdd816dfea6ce89f11d9a0

#### **i** APP INFORMATION

App Name: CCC Camp 2019 Wifi Setup Package Name: nl.eventinfra.wifisetup

Main Activity: nl.eventinfra.wifisetup.WifiSetup

Target SDK: 26 Min SDK: 18 Max SDK:

Android Version Name: 0.26
Android Version Code: 20190813

#### **EE** APP COMPONENTS

Activities: 1 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: 2018-12-28 09:14:06+00:00 Valid To: 2046-05-15 09:14:06+00:00

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

Serial Number: 0x4ccfaa93 Hash Algorithm: sha256

md5: 9c70ca68c227ee0418aaabc8d7b106d9

sha1: 3bdcbb17288d6398bb80b6b111f7985c3e88a6ef

sha256: 69537d93e97af7a75ef7cbefc98cac9386ac24bf425c39543cfe5ec9837d4ef8

sha512: dd0cad875b46e177bcc1fb66b91e7239ba34b8bec7a71abf59cc68958dbcf144d2782fe86e2a28b065c44a3f5f7e0123e48c351ef3e5fb7b7fac2b1a8c2525b0

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.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.

### **M** APKID ANALYSIS

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

#### **△** NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

# **Q** MANIFEST ANALYSIS

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

## </> CODE ANALYSIS

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	nl/eventinfra/wifisetup/WifiSetup.ja va
2	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	nl/eventinfra/wifisetup/WifiSetup.ja va

#### ■ 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 ['network connectivity'].
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 user/application initiated 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
twitter.com	ok	IP: 104.244.42.129 Country: United States of America Region: California City: San Francisco Latitude: 37.773968 Longitude: -122.410446 View: Google Map

#### **▶** HARDCODED SECRETS

# POSSIBLE SECRETS "Password": "password" "Username": "username@realm"

#### 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.