MOBSF

ANDROID STATIC ANALYSIS REPORT

NFC Tag maker (0.14)

File Name:	installer111.apk
Package Name:	pl.net.szafraniec.NFCTagmaker
Scan Date:	May 31, 2022, 9:13 a.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	2	1	1	1

FILE INFORMATION

File Name: installer111.apk
Size: 0.2MB
MD5: 02f51c946fe000a82e420735a7f9e6fe
SHA1: 787bae86695b28756ba128538e3814415e83c40b
SHA256: cd35c695a9f2a2d7a15d21b0cdfc1fbd72beefb8efb6917123da44a29cf9c65f

APP INFORMATION

App Name: NFC Tag maker
Package Name: pl.net.szafraniec.NFCTagmaker
Main Activity: MainActivity
Target SDK: 19
Min SDK: 16
Max SDK:
Android Version Name: 0.14
Android Version Code: 14

APP COMPONENTS

Activities: 8
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: 2014-02-08 06:14:15+00:00
Valid To: 2041-06-26 06:14:15+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x49247014
Hash Algorithm: sha256
md5: 059a962a696c753c0192a7c9cc8b50c4
sha1: e87c71410403154269c4bf943e306402f21d3410
sha256: 2686e04aaae2e0a08ecf7fcfa94a6495fd2f6d292f02d2960ae96400d9ed37e7
sha512: 10bd3eb278e8ce44ef986dfe8f6f0f25a72a292ddab38ed6d88f24a76e9df97af0e0b6210c0eb122cc7bf50cc0b3307c1518cc66be1f634140adc4a28c798d62

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.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

APKID ANALYSIS

FILE	DETAILS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dx</td></tr></table>

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	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	pl/net/szafraniec/NFCTagmaker/CloneReadActivity.java pl/net/szafraniec/NFCTagmaker/MainActivity.java pl/net/szafraniec/NFCTagmaker/CloneWriteNFCActivity.java pl/net/szafraniec/NFCTagmaker/WriteNFCActivity.java pl/net/szafraniec/NFCTagmaker/UltralightHEXEDIT.java
2	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	pl/net/szafraniec/NFCTagmaker/UltralightHEXEDIT.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 ['NFC'].
4	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
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.paypal.com	ok	**IP:** 151.101.129.21 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"donateBitcoin_uri" : "bitcoin:17E32x5ygXkqf5EWJkryZuarUDUFrb8UqQ?label=NFC%20Key"

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.