MOBSF

ANDROID STATIC ANALYSIS REPORT

NFC Key (1.40)

File Name:	installer171.apk
Package Name:	pl.net.szafraniec.NFCKey
Scan Date:	May 30, 2022, 3:32 p.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	8	1	1	0

FILE INFORMATION

File Name: installer171.apk
Size: 0.27MB
MD5: 34d89c11de9170656751198bb785b35b
SHA1: 6a85ad71e3c71464a6348485ae4ccd8b8721dc11
SHA256: e4bee832981ec0d944a4325bb75da63b8939e5027c46705b8c35695e089765d7

APP INFORMATION

App Name: NFC Key
Package Name: pl.net.szafraniec.NFCKey
Main Activity: MainActivity
Target SDK: 19
Min SDK: 16
Max SDK:
Android Version Name: 1.40
Android Version Code: 23

APP COMPONENTS

Activities: 9
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 3
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: 2014-01-20 06:24:10+00:00
Valid To: 2041-06-07 06:24:10+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x455342dc
Hash Algorithm: sha256
md5: 0ef814543d44a6ed927183698b8b2ed5
sha1: 0f6df982dac3f8484aefa09616b6eb1db66fd926
sha256: db9475619ec63526d7240d7bee629c9d16020c443d3aab1b52dfa4cb0d45a04a
sha512: 3cfb8943af31970e0a91d07562719279f378d6500d84e012b7c3410e56bb9c9d0d3f236c668420020e0b597f284ba033b05fce37f92488b0113126d1b5ad68fd

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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: DETAILS Anti-VM Code: possible Build.SERIAL check Compiler: dx

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
WriteActivity	Schemes: file://, Hosts: *, Mime Types: text/plain, */*, Path Patterns: .*\\.kdb, .*\\..*\\.kdb, .*\\..*\\..*\\.kdb, .*\\..*\\..*\\..*\\.kdb, .*\\..*\\..*\\..*\\..*\\.kdb, .*\\..*\\..*\\..*\\..*\\..*\\.kdb, .*\\..*\\..*\\..*\\..*\\..*\\..*\\.kdb, .*\\..*\\..*\\..*\\..*\\..*\\..*\\..*\\.kdb, .*\\..*\\..*\\..*\\..*\\..*\\..*\\..*\\..*\\.kdb, .*\\.kdbx, .*\\..*\\.kdbx, .*\\..*\\..*\\.kdbx, .*\\..*\\..*\\..*\\.kdbx, .*\\..*\\..*\\..*\\..*\\.kdbx, .*\\..*\\..*\\..*\\..*\\..*\\.kdbx, .*\\..*\\..*\\..*\\..*\\..*\\..*\\.kdbx, .*\\..*\\..*\\..*\\..*\\..*\\..*\\..*\\.kdbx,

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.
2	Activity (WriteActivity) is not Protected. An intent-filter exists.	warning	An Activity 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 Activity is explicitly exported.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Activity (com.ipaulpro.afilechooser.FileChooserActivity) is not Protected. An intent-filter exists.	warning	An Activity 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 Activity is explicitly exported.
4	Activity (ReadActivity) is not Protected. An intent-filter exists.	warning	An Activity 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 Activity is explicitly exported.

</> 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/NFCKey/y.java pl/net/szafraniec/NFCKey/k.java com/ianhanniballake/localstorage/LocalStorageProvider.java
2	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	pl/net/szafraniec/NFCKey/j.java
3	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	com/ipaulpro/afilechooser/c.java com/ianhanniballake/localstorage/LocalStorageProvider.java com/ipaulpro/afilechooser/a/a.java com/ipaulpro/afilechooser/FileChooserActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/ianhanniballake/localstorage/LocalStorageProvider.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application implement DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['NFC'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has no network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
8	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.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption not in accordance with FCS_COP.1.1(1), AES-ECB mode is being used.
12	FCS_CKM.1.1(2)	Optional Security Functional Requirements	Cryptographic Symmetric Key Generation	The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes 128 bit or 256 bit.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 142.251.36.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"Password" : "Password"
"Password" : "Hasło"

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.