MOBSF

ANDROID STATIC ANALYSIS REPORT

NFCard (2.2.150720)

File Name:	installer63.apk
Package Name:	com.sinpo.xnfc
Scan Date:	May 31, 2022, 9:52 a.m.
App Security Score:	30/100 (HIGH RISK)
Grade:	C

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	0	0	1	0

FILE INFORMATION

File Name: installer63.apk
Size: 0.21MB
MD5: edbacde7084363c8bff737b9447139c0
SHA1: 971a3fa1931fea793e1c4f43d44c766084c5dcd7
SHA256: db49657dc8eeac767ae0fde78a90624127ad407c12dc4b951b2ffcc0acf3d9e6

APP INFORMATION

App Name: NFCard
Package Name: com.sinpo.xnfc
Main Activity: com.sinpo.xnfc.MainActivity
Target SDK: 22
Min SDK: 10
Max SDK:
Android Version Name: 2.2.150720
Android Version Code: 15

APP COMPONENTS

Activities: 1
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=86, O=sinpowei@gmail.com, OU=dev.android, CN=sinpowei
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-02-28 08:33:59+00:00
Valid To: 2037-02-21 08:33:59+00:00
Issuer: C=86, O=sinpowei@gmail.com, OU=dev.android, CN=sinpowei
Serial Number: 0x4f4c9177
Hash Algorithm: sha1
md5: 6ea53cf596390ead65646b177175292b
sha1: 4737d86a3b03bf6827a8bc329cd11119bc4ac00c
sha256: 0fa3d96128275a1f276489bceaeca7742673fd4b40c1781db73c44ad8519a84e
sha512: 6e9df12f988f2f55423e6aa8443d6bffb4b8ef0b62b4a7dcaaa8a30a1ce36aafec655f5cf072065b84ea55b9fe8cce4291f2b0278b1bc8e508910419eb7c3803

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.
Certificate algorithm might be vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Compiler — DETAILS: dx

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Launch Mode of Activity (com.sinpo.xnfc.MainActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.
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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.gnu.org	ok	**IP:** 209.51.188.116 **Country:** United States of America **Region:** Massachusetts **City:** Boston **Latitude:** 42.358429 **Longitude:** -71.059769 **View:** Google Map

EMAILS

EMAIL	FILE
sinpowei@gmail.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.