ANDROID STATIC ANALYSIS REPORT

NFCard (1.2.120228)

File Name:	installer375.apk
Package Name:	com.sinpo.xnfc
Scan Date:	May 31, 2022, 6:08 a.m.
App Security Score:	**34/100 (HIGH RISK)**
Grade:	C

◔ FINDINGS SEVERITY

🐛 HIGH	⚠ MEDIUM	ℹ INFO	✔ SECURE	🔍 HOTSPOT
3	1	0	1	0

📦 FILE INFORMATION

File Name: installer375.apk
Size: 0.06MB
MD5: 5f2cf235b46426e294ec4f37b8af77b0
SHA1: d505c4dae0d8bfffb53633acd1f7dbd8eae0f8d8
SHA256: 73ed903209b57d3b69dc9ba4d65409a114d5970307067a5ca4e9549616c8f9b6

ℹ APP INFORMATION

App Name: NFCard
Package Name: com.sinpo.xnfc
Main Activity: NFCard
Target SDK: 11
Min SDK: 10
Max SDK:
Android Version Name: 1.2.120228
Android Version Code: 1

▦ 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=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-08-23 11:33:33+00:00
Valid To: 2040-01-09 11:33:33+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x5036150d
Hash Algorithm: sha1
md5: 27469f752a385f64ee85cd64d7af0d6c
sha1: 10865da7aba7214fe254517b7ba9e2acaa5e32fe
sha256: 2d9fd595996f06cb36ee05803c5903ffc83516c8ac02e698611120a694ca938b
sha512: 58a70dd13705c85a8c59ea1d225dea6d09e6267f17f0d85f316ed03063b1793be6596e426518aabb97b1fbf67ed42add5189e5b6939a7199c00e49d5b812a451

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	DETAILS
Compiler	dx

🔒 NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

🔍 MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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	Launch Mode of Activity (NFCard) 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.
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

DOMAIN	STATUS	GEOLOCATION
code.google.com	ok	**IP:** 142.250.179.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 View: [Google Map](#)
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