MOBSF

ANDROID STATIC ANALYSIS REPORT

KeePass NFC (1.1)

File Name:	installer323.apk
Package Name:	net.lardcave.keepassnfc
Scan Date:	May 31, 2022, 12:46 p.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	6	1	1	0

FILE INFORMATION

File Name: installer323.apk
Size: 0.37MB
MD5: 0f43e93284bda7795bf0727a2f43a82d
SHA1: 510188beb413fbecb0e18125710995bc8de4667d
SHA256: 4d431f2f6d34ab4bdfa323720733b354764b46aa2e2bcf34e9a47c5c5719b846

APP INFORMATION

App Name: KeePass NFC
Package Name: net.lardcave.keepassnfc
Main Activity: net.lardcave.keepassnfc.WriteActivity
Target SDK: 16
Min SDK: 16
Max SDK:
Android Version Name: 1.1
Android Version Code: 2

APP COMPONENTS

Activities: 4
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: 2014-01-09 08:20:41+00:00
Valid To: 2041-05-27 08:20:41+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x2e16f5ef
Hash Algorithm: sha256
md5: cf57ebedaae7b85e17920e26459c7faa
sha1: 0e3180554edb5df6b3c01d8037d3d17c563ad563
sha256: e2738513fc63e60ccff83272e38a6e996ce16a9e24d3fac8bcf9ed97055d0480
sha512: bd9e5c43f76b0c1092eaa1bb1e2cb930a75bea5f3d424c927e5c9b5b6fb8c7ff803a96bed4835c9c2929fb21c868683ce728df726c1e05d86aede1d46ab8dab2

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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: DETAILS Compiler: dx (possible dexmerge) Manipulator Found: dexmerge

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 (net.lardcave.keepassnfc.WriteNFCActivity) 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.
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 (net.lardcave.keepassnfc.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

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	net/lardcave/keepassnfc/DatabaseInfo.java com/ianhanniballake/localstorage/LocalStorageProvider.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	com/ipaulpro/afilechooser/FileChooserActivity.java com/ianhanniballake/localstorage/LocalStorageProvider.java com/ipaulpro/afilechooser/FileListFragment.java
3	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 invoke platform-provided 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.
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.
9	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.
10	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.

framework capable of performing static and dynamic analysis.