

ANDROID STATIC ANALYSIS REPORT



Smart Card Reader (2.2)

File Name:	installer369.apk		
Package Name:	com.vsmartcard.remotesmartcardreader.app		
Scan Date:	May 31, 2022, 4:11 p.m.		
App Security Score:	45/100 (MEDIUM RISK)		
Grade:			
	45/100 (MEDIUM RISK) B		

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	≪ HOTSPOT
2	4	2	1	1

FILE INFORMATION

File Name: installer369.apk

Size: 0.99MB

MD5: 1e5a583a4b70314257a7dfe02921c64d

SHA1: 672a8f5dc4baf197afa4531251441b40ce929a8b

SHA256: c97d8ca6db1dad6595c7411a68a9b2c3ba1fe16ab3b18c887a2e4fe95b7dadbb

i APP INFORMATION

App Name: Smart Card Reader

Package Name: com.vsmartcard.remotesmartcardreader.app

 ${\it Main\ Activity:} com. vsmartcard. remotes martcard reader. app. Main Activity$

Target SDK: 23 Min SDK: 19 Max SDK:

Android Version Name: 2.2 Android Version Code: 6

B APP COMPONENTS

Activities: 3 Services: 0 Receivers: 0 Providers: 0

Exported Activities: 1 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: 2014-07-20 04:50:01+00:00 Valid To: 2041-12-05 04:50:01+00:00

Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid

Serial Number: 0x59aa6d01 Hash Algorithm: sha256

md5: 93f7b55691d8667dd995856658ff3013

sha1: ba97b9632a38bf9c49fe2fb1e60c1b05ce526686

sha256: 557115967eab3a6023e1fa2ea5f7e3cf237188e021ca3029ab1d88d211f44809

sha512: 82acedce7d8f07d8c76833b376d09ce0efa3f6dd776533007bcb778d43f1050accb39f549974ce3237aa4a7e51a78db970e699dae3b97e220eb452870b604408

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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.

命 APKID ANALYSIS

FILE	DETAILS		
classes.dex	FINDINGS DETAILS		
Classes.ucx	Compiler	dx	

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.vsmartcard.remotesmartcardreader.app.SettingsActivity	Schemes: @string/scheme_vpcd://,

△ NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

Q 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	Launch Mode of Activity (com.vsmartcard.remotesmartcardreader.app.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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Activity (com.vsmartcard.remotesmartcardreader.app.SettingsActivity) 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	com/journeyapps/barcodescanner/a/i.java com/journeyapps/barcodescanner/a/i.java com/journeyapps/barcodescanner/q.java com/journeyapps/barcodescanner/a/t.java com/journeyapps/barcodescanner/a/r.java com/journeyapps/barcodescanner/a/k.java com/journeyapps/barcodescanner/e.java com/journeyapps/barcodescanner/a/m.java com/journeyapps/barcodescanner/a/a.java com/journeyapps/barcodescanner/a/a.java com/journeyapps/barcodescanner/g.java com/journeyapps/barcodescanner/g.java com/journeyapps/barcodescanner/m.java com/journeyapps/barcodescanner/m.java com/journeyapps/barcodescanner/a/j.java com/journeyapps/barcodescanner/y.java com/journeyapps/barcodescanner/y.java com/b/a/b/a/a.java com/b/a/b/a/c.java com/b/a/b/a/c.java com/b/a/b/a/a/a.java com/b/a/b/a/a/a/a.java com/journeyapps/barcodescanner/a/h.java com/journeyapps/barcodescanner/a/h.java com/journeyapps/barcodescanner/a/w.java
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/vsmartcard/remotesmartcardreader/app/M ainActivity.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/journeyapps/barcodescanner/m.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/vsmartcard/remotesmartcardreader/app/M yLogFragment.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', 'network connectivity', 'camera'].
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 user/application initiated 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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.

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.

© 2022 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.