ANDROID STATIC ANALYSIS REPORT

Smart Card Emulator (3.3)

File Name:	installer239.apk
Package Name:	com.vsmartcard.acardemulator
Scan Date:	May 31, 2022, 5:47 a.m.
App Security Score:	47/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
2	11	2	1	1

FILE INFORMATION

File Name: installer239.apk
Size: 2.81MB
MD5: 70a40dd44ba86abea627deea8ac3c0c4
SHA1: 4d7914bb64b4f4d83cd5e3b92da8c0cb4c5a6224
SHA256: dce89fcf98613c0f2778afabc314ef80c640716b58bec88cf46007dc40d9175b

APP INFORMATION

App Name: Smart Card Emulator
Package Name: com.vsmartcard.acardemulator
Main Activity: com.vsmartcard.acardemulator.MainActivity
Target SDK: 23
Min SDK: 19
Max SDK:
Android Version Name: 3.3
Android Version Code: 6

APP COMPONENTS

Activities: 3
Services: 2
Receivers: 2
Providers: 0
Exported Activities: 1
Exported Services: 1
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=US, O=Android, CN=Android Debug
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-09-27 09:33:04+00:00
Valid To: 2045-09-19 09:33:04+00:00
Issuer: C=US, O=Android, CN=Android Debug
Serial Number: 0x63147178
Hash Algorithm: sha256
md5: cca72169457dd0177a24e6cd59da96b3
sha1: 56049cbae6bbde9a398116f1b6a89817823cf11f
sha256: 54bb1a406e385b4057144f96c5d2a2f3797be5c9653011e3c866a8c2681c8acd
sha512: 30413a9461e3f6a842631c77693bd4f51969574b571c605043e3c24c2bdeae98cb4b755904fadb1d9dc818b48d1a38b4efb359086c0c4a2e53eeff5a754911ac
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: f3ebb063f462f6747bc67e7f383cb63aee3c4817bbbc8e4cddd5823946a11158
```

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	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 signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.

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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
com.samsung.accessory.permission.ACCESSORY_FRAMEWORK	unknown	Unknown permission	Unknown permission from android reference
com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY	unknown	Unknown permission	Unknown permission from android reference
com.samsung.WATCH_APP_TYPE.Companion	unknown	Unknown permission	Unknown permission from android reference
com.samsung.wmanager.ENABLE_NOTIFICATION	unknown	Unknown permission	Unknown permission from android reference
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.

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.BOARD check</td></tr>
<tr><td>Compiler</td><td>dx (possible dexmerge)</td></tr>
<tr><td>Manipulator Found</td><td>dexmerge</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.vsmartcard.acardemulator.SettingsActivity	Schemes: @string/scheme_vicc://,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.
2	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.
3	Activity (com.vsmartcard.acardemulator.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.
4	Service (com.vsmartcard.acardemulator.EmulatorHostApduService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_NFC_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Broadcast Receiver (com.samsung.android.sdk.accessory.RegisterUponInstallReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver 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 Broadcast Receiver is explicitly exported.
6	Broadcast Receiver (com.samsung.android.sdk.accessory.ServiceConnectionIndicationBroadcastReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver 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 Broadcast Receiver is explicitly exported.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/vsmartcard/acardemulator/SmartcardProviderService.java com/samsung/android/sdk/accessory/d.java com/journeyapps/barcodescanner/camera/FitCenterStrategy.java com/journeyapps/barcodescanner/camera/CameraManager.java com/samsung/android/sdk/accessoryfiletransfer/SAFileTransferIncomingRequestReceiver.java com/samsung/android/sdk/accessory/SASocket.java com/journeyapps/barcodescanner/camera/CenterCropStrategy.java com/samsung/android/sdk/accessory/SAPeerAgent.java pro/javacard/vre/VRE.java com/samsung/android/sdk/accessoryfiletransfer/SAFileTransfer.java

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	Transfer.java com/journeyapps/barcodescanner/CaptureManager.java com/journeyapps/barcodescanner/CameraPreview.java pro/javacard/vre/vRSAPrivateCrtKey.java com/vsmartcard/acardemulator/emulators/EmulatorSingleton.java com/samsung/android/sdk/accessory/RegisterUponInstallReceiver.java com/samsung/android/sdk/accessoryfiletransfer/SAFileTransferCallbackReceiver.java com/samsung/android/sdk/accessory/h.java com/samsung/android/sdk/accessory/SAAdapter.java com/journeyapps/barcodescanner/camera/CameraInstance.java com/journeyapps/barcodescanner/camera/LegacyPreviewScalingStrategy.java pro/javacard/vre/vRSAPrivateKey.java com/vsmartcard/acardemulator/EmulatorHostApduService.java com/vsmartcard/acardemulator/emulators/VICCEmulator.java com/samsung/android/sdk/accessory/SAAgent.java javacard/framework/Util.java com/samsung/android/sdk/accessory/e.java com/samsung/android/sdk/accessory/ServiceConnectionIndicationBroadcastReceiver.java com/samsung/accessory/a/a/d.java com/journeyapps/barcodescanner/camera/AutoFocusManager.java com/samsung/android/sdk/accessory/f.java com/samsung/android/sdk/accessory/SA.java com/samsung/android/sdk/accessoryfiletransfer/b.java com/journeyapps/barcodescanner/DecoderThread.java com/journeyapps/barcodescanner/camera/PreviewScalingStrategy.java com/samsung/android/sdk/accessory/g.java com/samsung/android/sdk/accessoryfiletransfer/SAft.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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/acardemulator/MainActivity.java
3	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/samsung/android/sdk/accessoryfiletransfer/SAFileTransfer.java
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/journeyapps/barcodescanner/CaptureManager.java com/licel/jcardsim/base/Simulator.java
5	MD5 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	pro/javacard/vre/vMessageDigest.java
6	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	pro/javacard/vre/vMessageDigest.java pro/javacard/vre/vRandomData.java
7	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/vsmartcard/acardemulator/emulators/VICCEmulator.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 implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['NFC', 'network connectivity', 'bluetooth', 'camera'].
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 user/application initiated 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	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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys not in accordance with FCS_CKM.1.1(1) using key generation algorithm RSA schemes and cryptographic key sizes of 1024-bit or lower.
12	FCS_CKM.1.1(3),FCS_CKM.1.2(3)	Selection-Based Security Functional Requirements	Password Conditioning	A password/passphrase shall perform [Password-based Key Derivation Functions] in accordance with a specified cryptographic algorithm..
13	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
14	FCS_COP.1.1(3)	Selection-Based Security Functional Requirements	Cryptographic Operation - Signing	The application perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
15	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
16	FIA_X509_EXT.1.1	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The application validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates'].
17	FIA_X509_EXT.1.2	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.
18	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.
19	FIA_X509_EXT.2.2	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	When the application cannot establish a connection to determine the validity of a certificate, the application allow the administrator to choose whether to accept the certificate in these cases or accept the certificate ,or not accept the certificate.
20	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

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.