ANDROID STATIC ANALYSIS REPORT

UUID 0xFD6F Scanner (0.9.1.14)

File Name:	installer343.apk
Package Name:	com.emacberry.uuid0xfd6fscan
Scan Date:	May 31, 2022, 4:44 p.m.
App Security Score:	**60/100 (LOW RISK)**
Grade:	A

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	6	1	1	1

FILE INFORMATION

File Name: installer343.apk
Size: 2.54MB
MD5: 5e86bd78bdac5200f6a230734fb71dfd
SHA1: c6c80a5b7e579bd6d899261e95231fab78877ffe
SHA256: f3dd10dfc7aa7f216dc8339ba698413ff7bff6401470b3358db5d6ba26dc113c

APP INFORMATION

App Name: UUID 0xFD6F Scanner
Package Name: com.emacberry.uuid0xfd6fscan
Main Activity: com.emacberry.uuid0xfd6fscan.ScannerActivity
Target SDK: 30
Min SDK: 23
Max SDK:
Android Version Name: 0.9.1.14
Android Version Code: 9114

APP COMPONENTS

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

CERTIFICATE INFORMATION

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=DE, ST=NRW, L=Rietberg, O=emacberry.com, CN=Matthias Marquardt
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-05-31 11:31:18+00:00
Valid To: 2039-05-25 11:31:18+00:00
Issuer: C=DE, ST=NRW, L=Rietberg, O=emacberry.com, CN=Matthias Marquardt
Serial Number: 0x5389bd86
Hash Algorithm: sha1
md5: 3926270e2c5b24a52eef60f9dae702dc
sha1: 31f280acffea758c4dc07e7b192920e743298618
sha256: c2de65425409c334f39f98d181b2003b32c30c9da3dcbb1a0ddc32f7fef0595c
sha512: a14f2c84d2b8f6d30b6e1148137c49f2ee38ed3b7f17bc6e0831c965f2271848e269a962d585250259eeee6ccde37ae687759bf5b992c36040556418d53f634b
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 8740871332e4e0142309a540c36906efc02dcfdc78126826de38021e28aef724
```

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.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal		Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.

APKID ANALYSIS

<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.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table>
</td></tr>
</table>

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	Broadcast Receiver (com.emacberry.uuid0xfd6fscan.BootUpReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.RECEIVE_BOOT_COMPLETED [android:exported=true]	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. 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.

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/emacberry/uuid0xfd6fscan/BootUpReceiver.java com/emacberry/uuid0xfd6fscan/ScannerService.java com/emacberry/uuid0xfd6fscan/ScannerActivity.java com/emacberry/uuid0xfd6fscan/Preferences.java com/emacberry/uuid0xfd6fscan/SettingsActivity.java com/emacberry/uuid0xfd6fscan/LockCheckerApi26.java com/emacberry/uuid0xfd6fscan/NotificationHelper.java
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/emacberry/uuid0xfd6fscan/BuildConfig.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 ['bluetooth', 'location'].

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 implement functionality to encrypt sensitive data in non-volatile memory.
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 encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.

HARDCODED SECRETS

POSSIBLE SECRETS
"PKEY_AUTOSTART" : "AUTOSTART"
"PKEY_AUTOSTARTBLUETOOTH" : "AUTOSTARTBLUETOOTH"
"PKEY_GROUPBYSIGSTRENGTH" : "GROUPBYSIGSTRENGTH"
"PKEY_GROUPMEDVAL" : "GROUPMEDVAL"
"PKEY_GROUPNEARVAL" : "GROUPNEARVAL"

POSSIBLE SECRETS
"PKEY_IGNOREBATTERYOPT" : "BATTERY_OPT"
"PKEY_SCANMODE" : "SCANMODE"
"PKEY_SHOWTOTAL" : "SHOWTOTALBEACONNUM"
"pref01_KEY" : "SETTINGS_01"

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.