

ANDROID STATIC ANALYSIS REPORT



UUID 0xFD6F Scanner (0.9.1.11)

File Name:	installer28.apk
Package Name:	com.emacberry.uuid0xfd6fscan
Scan Date:	May 31, 2022, 6:01 a.m.
App Security Score:	53/100 (MEDIUM RISK)
Grade:	

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	® HOTSPOT
1	4	1	1	1

FILE INFORMATION

File Name: installer28.apk

Size: 2.29MB

MD5: 758d925bd3160e2cf516548ef4b0fd85

SHA1: b2fc37d53aacd39925e6cf5bb706e815e9afb71c

SHA256: 5e597c62685dcb18838d28043cc7d3b6cd92e0b32c743e4d0aa9baaa2bdafb17

i APP INFORMATION

App Name: UUID 0xFD6F Scanner

Package Name: com.emacberry.uuid0xfd6fscan

Main Activity: com.emacberry.uuid0xfd6fscan.ScannerActivity

Target SDK: 29 Min SDK: 23 Max SDK:

Android Version Name: 0.9.1.11 Android Version Code: 9111

APP COMPONENTS

Activities: 2 Services: 1 Receivers: 1 Providers: 1

Exported Activities: O Exported Services: O Exported Receivers: 1 Exported Providers: O



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: 2020-09-04 06:35:15+00:00 Valid To: 2048-01-21 06:35:15+00:00

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

Serial Number: 0x673bc4ef Hash Algorithm: sha256

md5: e186b07282cae8345d6eda3f7f566e60

sha1: 4f79ed2d3b225707e54b51f9eec22403f91f83d1

sha256: 25738b4b0d8c18d71c0e24d6edd30ee927929101d57aa124932b7aff0b1d977a

sha512: 1ec5bcf4fff2bee80d6ab683cba1645ff0e220276d1ca6d149a175da60c9e58fa1b75f93eab9e0261cafc2c03c472c3f7d31c96ce03994600a7397905eed7996

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.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.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

PERMISSION	STATUS	INFO	DESCRIPTION
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.

M APKID ANALYSIS

FILE	DETAILS		
	FINDINGS	DETAILS	
classes.dex	Anti-VM Code	Build.MANUFACTURER check	
	Compiler	r8	

△ 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	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
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/Notification Helper.java com/emacberry/uuid0xfd6fscan/BootUpRec eiver.java com/emacberry/uuid0xfd6fscan/ScannerSer vice.java com/emacberry/uuid0xfd6fscan/ScannerActi vity.java com/emacberry/uuid0xfd6fscan/SettingsActi vity.java com/emacberry/uuid0xfd6fscan/Preferences .java com/emacberry/uuid0xfd6fscan/LockChecke rApi26.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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'].
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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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_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.

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