

ANDROID STATIC ANALYSIS REPORT



FTP Server (Free) (3.0)

File Name:	installer1.apk
Package Name:	be.ppareit.swiftp_free
Scan Date:	May 31, 2022, 7:55 a.m.
App Security Score:	35/100 (HIGH RISK)
Grade:	C

FINDINGS SEVERITY

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

FILE INFORMATION

File Name: installer1.apk

Size: 2.21MB

MD5: 3c8cb20a7ee121908a1a9e7e7f249ecc

SHA1: c6159e8e032d1c8caf48119b5bbbf1e0136a5df6

SHA256: 11bf01f1e111074218a481a5d6b35865cde8a8abd4f427aeab33fb5f6e831c5c

i APP INFORMATION

App Name: FTP Server (Free)

Package Name: be.ppareit.swiftp_free

Main Activity: be.ppareit.swiftp.gui.MainActivity

Target SDK: 28 Min SDK: 14 Max SDK:

Android Version Name: 3.0
Android Version Code: 30000

EE APP COMPONENTS

Activities: 4 Services: 7 Receivers: 2 Providers: 0

Exported Activities: 1 Exported Services: 1 Exported Receivers: 1 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: 2012-10-11 17:03:05+00:00 Valid To: 2040-02-27 17:03:05+00:00

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

Serial Number: 0x5076fbc9 Hash Algorithm: sha1

md5: f34b7cce6429c3d96045a4eb5778306c

sha1: 631f7a9c878b4fb271c72c011e0f37eb32a73c48

sha256: 1141115127d21941a960860bcda28b87da6088bf8a4d38a6ae749ad0ccbaf4a5

sha512: 9fe2bedaab58f641485b8e8f44b80246697c89f49b319911ba3a1a48e9902555282194f7549a296ae1967801b6947cf6c091c0d672d74c4d798d963b6ff80329

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.	
Certificate algorithm might be vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.	

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.CHANGE_WIFI_MULTICAST_STATE	normal	allow Wi-Fi Multicast reception	Allows an application to receive packets not directly addressed to your device. This can be useful when discovering services offered nearby. It uses more power than the non-multicast mode.
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.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

M APKID ANALYSIS

FILE	DETAILS		
classes.dex	FINDINGS DETAILS		
classes.dex	Compiler	r8	



NO	SCOPE	SEVERITY	DESCRIPTION
	360. 2	02121111	

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	Activity (be.ppareit.swiftp.locale.EditActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
3	Broadcast Receiver (be.ppareit.swiftp.locale.FireReceiver) is not Protected. [android:exported=true]	high	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.
4	Service (be.ppareit.swiftp.gui.FsTileService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_QUICK_SETTINGS_TILE [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.

</> 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	be/ppareit/swiftp/server/TcpListener.java be/ppareit/swiftp/Util.java be/ppareit/swiftp/server/CmdPASV.java be/ppareit/swiftp/server/LocalDataSocket.j ava be/ppareit/swiftp/server/CmdSYST.java com/twofortyfouram/log/Lumberjack.java be/ppareit/swiftp/server/CmdFEAT.java be/ppareit/swiftp/server/CmdMKD.java be/ppareit/swiftp/server/CmdMKD.java be/ppareit/swiftp/server/CmdNLST.java be/ppareit/swiftp/server/CmdNLST.java be/ppareit/swiftp/server/CmdRNTO.java be/ppareit/swiftp/server/CmdOPTS.java be/ppareit/swiftp/server/CmdDTM.java be/ppareit/swiftp/server/CmdMDTM.java be/ppareit/swiftp/server/CmdVSER.java be/ppareit/swiftp/server/CmdSIZE.java be/ppareit/swiftp/server/CmdTemplate.jav a be/ppareit/swiftp/server/CmdCWD.java be/ppareit/swiftp/server/CmdCWD.java be/ppareit/swiftp/server/CmdMLST.java be/ppareit/swiftp/server/CmdMLST.java be/ppareit/swiftp/server/CmdMLST.java be/ppareit/swiftp/server/CmdMLSD.java be/ppareit/swiftp/server/CmdMLSD.java be/ppareit/swiftp/server/CmdAbstractListi ng.java be/ppareit/swiftp/server/CmdAbstractListi ng.java be/ppareit/swiftp/server/CmdCDUP.java

NO	ISSUE	SEVERITY	STANDARDS	be/ppareit/swiftp/FsSettings.java be/ppareit/swiftp/server/CmdQUIT.java be/ppareit/swiftp/server/CmdRNFR.java be/ppareit/swiftp/server/CmdPORT.java be/ppareit/swiftp/NsdService.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	be/ppareit/swiftp/gui/PreferenceFragment. java be/ppareit/swiftp/gui/FolderPickerDialogB uilder.java be/ppareit/swiftp/gui/UserEditFragment.ja va be/ppareit/swiftp/FsService.java be/ppareit/swiftp/utils/FileUtil.java be/ppareit/swiftp/MediaUpdater.java be/ppareit/swiftp/utils/MediaStoreHack.jav a be/ppareit/swiftp/tils/MediaStoreHack.jav a
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	be/ppareit/swiftp/server/CmdRNTO.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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity', '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 user/application initiated 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.

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
--------	--------	-------------

DOMAIN	STATUS	GEOLOCATION
ppareit.github.com	ok	IP: 185.199.109.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map
github.com	ok	IP: 140.82.121.4 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
ppareit.github.io	ok	IP: 185.199.111.153 Country: United States of America Region: Pennsylvania City: California Latitude: 40.065632 Longitude: -79.891708 View: Google Map
www.gnu.org	ok	IP: 209.51.188.116 Country: United States of America Region: Massachusetts City: Boston Latitude: 42.358429 Longitude: -71.059769 View: Google Map



EMAIL	FILE	
pieter.pareit@gmail.com	be/ppareit/swiftp/gui/MainActivity.java	
pieter.pareit@gmail.com	Android String Resource	

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.