MOBSF

ANDROID STATIC ANALYSIS REPORT

primitive ftpd (6.5)

File Name:	installer280.apk
Package Name:	org.primftpd
Scan Date:	May 31, 2022, 12:30 p.m.
App Security Score:	48/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	18	1	1	2

FILE INFORMATION

File Name: installer280.apk
Size: 4.73MB
MD5: f8ff3be9af54f5abd335508bebcf55a7
SHA1: ac7b73d9cf2075c512a5c86477e9a52eb921b47b
SHA256: e80838b8b81a2d77f6fcf7d72ad20a424e229db37f95fbb7d1fe25cb0ee95f23

APP INFORMATION

App Name: primitive ftpd
Package Name: org.primftpd
Main Activity: org.primftpd.PrimitiveFtpdActivity
Target SDK: 29
Min SDK: 15
Max SDK:
Android Version Name: 6.5
Android Version Code: 51

APP COMPONENTS

Activities: 12
Services: 4
Receivers: 4
Providers: 1
Exported Activities: 8
Exported Services: 1
Exported Receivers: 4
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=hans
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-02-05 18:04:21+00:00
Valid To: 2037-01-29 18:04:21+00:00
Issuer: CN=hans
Serial Number: 0x4f2ec4a5
Hash Algorithm: sha1
md5: afb5d14da7b3ef174d9ba025480f9070
sha1: 51c87695d7d769fd656e554179ee0984cdda833d
sha256: 7151ae6d56f156e67224e7ca3f9c00da6f7030b66cc8443f3bb4d3f84eeb5c95
sha512: d485245a862c6a5d51e64f3ff6b5027d25dc5a59ff7cebafc2d717553a6bc0b0b1c97227644ef93c9629cf67ab78f8a4ae8422536f7f85cd61d7ffc21ff07590
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: c3bdc451c1e398ddb3ee4115c2d64b2ac4f84adcc482db7a3ecbb7811ace7a82

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	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
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.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Compiler — DETAILS: r8
classes2.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check possible Build.SERIAL check FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Broadcast Receiver (org.primftpd.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.
2	Broadcast Receiver (org.primftpd.StartStopWidgetProvider) 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.
3	Broadcast Receiver (org.primftpd.remotecontrol.PftpdPowerTogglesPlugin) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.painless.pc.permission.CONTROL_PLUGIN [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.
4	Broadcast Receiver (org.primftpd.remotecontrol.TaskerReceiver) 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.
5	Activity (org.primftpd.ui.LeanbackActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Activity (org.primftpd.remotecontrol.TaskerEditActionActivity) 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.
7	Activity (org.primftpd.remotecontrol.TaskerEditConditionActivity) 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.
8	Activity (org.primftpd.share.ReceiveSaveAsActivity) 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.
9	Activity (org.primftpd.share.ReceiveQuickShareActivity) 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.
10	Activity (org.primftpd.filepicker.ResettingFilePickerActivity) 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.
11	Activity (org.primftpd.ui.StartServerAndExitActivity) 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.
12	Activity (org.primftpd.ui.StopServerAndExitActivity) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
13	Service (org.primftpd.services.QuickSettingsService) 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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	eu/chainfire/libsuperuser/BuildConfig.java eu/chainfire/libsuperuser/Shell.java eu/chainfire/libsuperuser/Application.java eu/chainfire/libsuperuser/ShellOnMainThreadException.java eu/chainfire/libsuperuser/Toolbox.java org/primftpd/services/SshServerService.java org/primftpd/filesystem/RootSshFile.java eu/chainfire/libsuperuser/HideOverlaysReceiver.java org/primftpd/services/FtpServerService.java eu/chainfire/libsuperuser/Debug.java org/primftpd/filesystem/RootFile.java eu/chainfire/libsuperuser/StreamGobbler.java org/primftpd/filesystem/RootFtpFileSystemView.java org/primftpd/filesystem/RootFileSystemView.java org/primftpd/services/ServerServiceHandler.java org/primftpd/filesystem/RootSshFileSystemView.java org/primftpd/services/AbstractServerService.java eu/chainfire/libsuperuser/ShellNotClosedException.java eu/chainfire/libsuperuser/R.java eu/chainfire/libsuperuser/Policy.java org/primftpd/filesystem/RootFtpFile.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	org/slf4j/impl/AndroidLoggerFactory.java org/primftpd/StartStopWidgetProvider.java org/primftpd/util/PrngFixes.java org/greenrobot/eventbus/util/AsyncExecutor.java org/greenrobot/eventbus/util/ErrorDialogConfig.java eu/chainfire/libsuperuser/Debug.java org/greenrobot/eventbus/BackgroundPoster.java org/greenrobot/eventbus/util/ExceptionToResourceMapping.java org/slf4j/helpers/Util.java org/slf4j/impl/AndroidLogger.java org/greenrobot/eventbus/EventBus.java org/greenrobot/eventbus/util/ErrorDialogManager.java
3	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	org/primftpd/util/PrngFixes.java
4	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	org/primftpd/prefs/LoadPrefsUtil.java
5	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	org/primftpd/filepicker/nononsenseapps/FilePickerActivity.java org/primftpd/filepicker/ResettingFilePickerActivity.java org/primftpd/util/Defaults.java org/primftpd/services/AndroidPrefsUserManager.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 implement 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 ['network connectivity'].
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_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
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', 'The certificate path must terminate with a trusted CA certificate'].
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
www.slf4j.org	ok	**IP:** 83.173.251.158 **Country:** Switzerland **Region:** Zurich **City:** Zurich **Latitude:** 47.366669 **Longitude:** 8.550000 **View:** Google Map
pftpd.rocks	ok	**IP:** 95.216.156.127 **Country:** Finland **Region:** Uusimaa **City:** Helsinki **Latitude:** 60.169521 **Longitude:** 24.935450 **View:** Google Map
www.amazon.com	ok	**IP:** 108.156.66.76 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
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

DOMAIN	STATUS	GEOLOCATION
su.chainfire.eu	ok	**IP:** 5.79.66.53 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
f-droid.org	ok	**IP:** 148.251.140.42 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map
www.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **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

DOMAIN	STATUS	GEOLOCATION
mina.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
bouncycastle.org	ok	**IP:** 203.32.61.103 **Country:** Australia **Region:** Victoria **City:** Fitzroy **Latitude:** -37.798389 **Longitude:** 144.978333 **View:** Google Map

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"prefTitlePassword" : "Password"
"prefTitlePassword" : "Passwort"
"prefTitleUser" : "Benutzername"
"prefTitlePassword" : "Sandi"
"prefTitlePassword" : "Contraseña"

POSSIBLE SECRETS
"prefTitleUser" : "Usuario"
"prefTitlePassword" : "Pasahitza"
"prefTitlePassword" : "Пароль"
"prefTitlePassword" : "Password"
"couldNotReadKeyAuthKey" : "用于密钥验证的公钥不能被读取。请检查日志。"
"haveToSetPassword" : "首先您需要设置密码"
"prefTitlePassword" : "密码"
"prefTitleUser" : "用户名"
"prefTitlePassword" : "Пароль"
"prefTitlePassword" : "Hasło"
"prefTitlePassword" : "Password"
"prefTitlePassword" : "Jelszó"
"prefTitleUser" : "Felhasználónév"
"prefTitlePassword" : "Palavra-Passe"
"couldNotReadKeyAuthKey" : "無法讀取用來金鑰驗證的公開金鑰。請檢查記錄。"

POSSIBLE SECRETS
"haveToSetPassword" : "你必須先設定密碼"
"prefTitlePassword" : "密碼"
"prefTitleUser" : "使用者名稱"

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.