MOBSF

ANDROID STATIC ANALYSIS REPORT

Remote Droid (0.1)

File Name:	installer58.apk
Package Name:	in.umairkhan.remotedroid
Scan Date:	May 31, 2022, 9:01 a.m.
App Security Score:	54/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	6	1	2	1

FILE INFORMATION

File Name: installer58.apk
Size: 1.09MB
MD5: 658b69a65d8ccb99aad69be8f93f21ad
SHA1: d4ee54489c1e1638cfbba2ac6acccd09f9b9f2ee
SHA256: 75a4321b9cef426a2782385839f8198fe10ad0c3da721dff5d9604af7a70ff1d

APP INFORMATION

App Name: Remote Droid
Package Name: in.umairkhan.remotedroid
Main Activity: in.omerjerk.remotedroid.app.MainActivity
Target SDK: 21
Min SDK: 18
Max SDK:
Android Version Name: 0.1
Android Version Code: 1

APP COMPONENTS

Activities: 3
Services: 1
Receivers: 0
Providers: 0
Exported Activities: 0
Exported Services: 1
Exported Receivers: 0
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: 2015-04-09 11:50:13+00:00
Valid To: 2042-08-25 11:50:13+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x4107e82d
Hash Algorithm: sha256
md5: 9ea47cbd0c027c4e6a7be8035e0e0010
sha1: 591fd24bbd9e2aa368643da5f9a5fe276ef0cefb
sha256: fabf599ef5b39520b5c87abf9874bfb00fe595833eb0947e7f8ea4bce5debde9
sha512: 7ed0d2d059c239502d0b0eb7a32042c5e74edeffc3fc20457931bda45f729facc1cb123ef0338a150625ca3233cc9d39622864d5e5c5819cdb022c88cce32cfc

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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.CAPTURE_VIDEO_OUTPUT	normal		Allows an application to capture video output.
android.permission.CAPTURE_SECURE_VIDEO_OUTPUT	normal		Allows an application to capture secure video output.
android.permission.ACCESS_SUPERUSER	unknown	Unknown permission	Unknown permission from android reference
android.permission.SYSTEM_ALERT_WINDOW	dangerous	display system-level alerts	Allows an application to show system-alert windows. Malicious applications can take over the entire screen of the phone.
android.permission.INJECT_EVENTS	signature	press keys and control buttons	Allows an application to deliver its own input events (key presses, etc.) to other applications. Malicious applications can use this to take over the phone.

APKID ANALYSIS

FILE	DETAILS
classes.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dx (possible dexmerge)</td></tr><tr><td>Manipulator Found</td><td>dexmerge</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	Service (in.omerjerk.remotedroid.app.ServerService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	com/koushikdutta/async/http/spdy/ByteString.java
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	com/koushikdutta/async/AsyncServer.java in/omerjerk/remotedroid/app/ServerService.java in/omerjerk/remotedroid/app/ClientActivity.java com/koushikdutta/async/http/AsyncHttpRequest.java eu/chainfire/libsuperuser/Debug.java in/omerjerk/remotedroid/app/VideoWindow.java com/koushikdutta/async/ByteBufferList.java com/koushikdutta/async/http/cache/RawHeaders.java com/koushikdutta/async/http/server/AsyncHttpServerRequestImpl.java com/koushikdutta/async/AsyncNetworkSocket.java com/koushikdutta/async/Util.java com/koushikdutta/async/PushParser.java
3	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/koushikdutta/async/dns/Dns.java com/koushikdutta/async/AsyncSSLSocketWrapper.java
4	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/koushikdutta/async/dns/Dns.java com/koushikdutta/async/util/FileCache.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	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	com/koushikdutta/async/http/WebSocketImpl.java
6	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	eu/chainfire/libsuperuser/Application.java eu/chainfire/libsuperuser/Debug.java eu/chainfire/libsuperuser/StreamGobbler.java eu/chainfire/libsuperuser/ShellNotClosedException.java eu/chainfire/libsuperuser/Shell.java eu/chainfire/libsuperuser/ShellOnMainThreadException.java in/omerjerk/remotedroid/app/MainActivity.java
7	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/koushikdutta/async/AsyncSSLSocketWrapper.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 use no 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
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 does not encrypt files 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.
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_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.
11	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
12	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.
13	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 certificate path must terminate with a trusted CA certificate'].
14	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.

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.