MOBSF

ANDROID STATIC ANALYSIS REPORT

MqttPublisher Plugin (V1.0.1)

File Name:	installer101.apk
Package Name:	com.fr3ts0n.androbd.plugin.mqtt
Scan Date:	May 31, 2022, 10:09 a.m.
App Security Score:	48/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	3	1	2	0

FILE INFORMATION

File Name: installer101.apk
Size: 0.11MB
MD5: 8e9e7544ea72fe83bd9eba77230b2c17
SHA1: 102d809b1647de0f910e518c272805d7703ce10b
SHA256: c59022cc1676087bb610a5234f6ed8dc3dbec6a6a189309bf90d29675b1aead0

APP INFORMATION

App Name: MqttPublisher Plugin
Package Name: com.fr3ts0n.androbd.plugin.mqtt
Main Activity: com.fr3ts0n.androbd.plugin.mqtt.SettingsActivity
Target SDK: 25
Min SDK: 16
Max SDK:
Android Version Name: V1.0.1
Android Version Code: 10001

APP COMPONENTS

Activities: 2
Services: 1
Receivers: 1
Providers: 0
Exported Activities: 0
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: 2018-03-19 06:37:10+00:00
Valid To: 2045-08-04 06:37:10+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x5c4b9e5a
Hash Algorithm: sha256
md5: 4cafbcd7a51fd5fd99dd0fbb45b0dd5d
sha1: fcf2a71263a30b0a94ef8f8cd5cdbb9c78c5e172
sha256: 10de7dc04881327b02726e6f08a3cad79742e3b03918c552a8114be611481608
sha512: da3d4effb711aba9cd873133689bdc380adbd3c94be37cda01da8e41c64104cb46f9ddd06038aa168a97de416f3d082e7506e11ffa5fa467f8470f05f33fc62f

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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

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 (com.fr3ts0n.androbd.plugin.mqtt.MqttPlugin) 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.
3	Broadcast Receiver (com.fr3ts0n.androbd.plugin.mqtt.PluginReceiver) 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.

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/fr3ts0n/androbd/plugin/Plugin.java com/fr3ts0n/androbd/plugin/mqtt/MqttPlugin.java com/fr3ts0n/androbd/plugin/PluginReceiver.java com/fr3ts0n/androbd/plugin/mgr/PluginHandler.java
2	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/eclipse/paho/client/mqttv3/internal/wire/MqttPingReq.java org/eclipse/paho/client/mqttv3/internal/wire/MqttDisconnect.java com/fr3ts0n/androbd/plugin/mqtt/MqttPlugin.java org/eclipse/paho/client/mqttv3/internal/wire/MqttConnack.java org/eclipse/paho/client/mqttv3/internal/wire/MqttConnect.java org/eclipse/paho/client/mqttv3/internal/wire/MqttPingResp.java
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	org/eclipse/paho/client/mqttv3/internal/security/SSLSocketFactoryFactory.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 invoke platform-provided DRBG functionality for its cryptographic operations.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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_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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.121.3 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"password" : "Password"
"password" : "Passwort"
"user_name" : "Benutzername"

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.