MOBSF

ANDROID STATIC ANALYSIS REPORT

Barnacle Wifi Tether (0.6.7 (evo))

File Name:	installer65.apk
Package Name:	net.szym.barnacle
Scan Date:	May 31, 2022, 8:35 a.m.
App Security Score:	40/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	4	1	1	0

FILE INFORMATION

File Name: installer65.apk
Size: 0.13MB
MD5: 970e0b326903faef87930dc24df30b1f
SHA1: 7c6181ef16cdf51d4f5204904543cb02accf38aa
SHA256: efa0cbdaffab428dc08379dfbdfafee0d90aeb61cf3da12929fd772c820f8960

APP INFORMATION

App Name: Barnacle Wifi Tether
Package Name: net.szym.barnacle
Main Activity: StatusActivity
Target SDK: 6
Min SDK: 3
Max SDK:
Android Version Name: 0.6.7 (evo)
Android Version Code: 39

APP COMPONENTS

Activities: 3
Services: 1
Receivers: 2
Providers: 0
Exported Activities: 0
Exported Services: 0
Exported Receivers: 2
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: 2012-02-05 12:02:08+00:00
Valid To: 2039-06-23 12:02:08+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x4f2e6fc0
Hash Algorithm: sha1
md5: 0db3f0edcb56f57e79212913a9cf523f
sha1: 3d74209e20f21af619926eff39698e3cfe1c30fd
sha256: 96b5df69bcf7f5bacb43ac19ab2e12e82d6ae41a7917c9e95d77cbe79c7f5f2b
sha512: e78e03e5cdd6d07ff6ff5ce7f031a9c55ad5ae7b053ff80632f9c780f858ba372955f00c10b42933790369d852bd29f5ae0cf774c56ee3d74bb4b19204c93e37

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.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.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>dx</td></tr></table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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	Launch Mode of Activity (StatusActivity) is not standard.	high	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Broadcast Receiver (ToggleReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: net.szym.barnacle.CHANGE_STATE protectionLevel: dangerous [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. However, the protection level of the permission is set to dangerous. This means that a malicious application can request and obtain the permission and interact with the component. If it was set to signature, only applications signed with the same certificate could obtain the permission.
4	Broadcast Receiver (ToggleReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: net.szym.barnacle.ACCESS_STATE protectionLevel: normal [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. However, the protection level of the permission is set to normal. This means that a malicious application can request and obtain the permission and interact with the component. If it was set to signature, only applications signed with the same certificate could 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	net/szym/barnacle/Util.java net/szym/barnacle/BarnacleService.java net/szym/barnacle/BarnacleApp.java net/szym/barnacle/ToggleReceiver.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
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	net/szym/barnacle/WEPPreference.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 ['network connectivity'].
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 does not encrypt files in non-volatile memory.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 not encrypt any data in traffic or does not transmit any data between itself and another trusted IT product.

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
szym.net	ok	**IP:** 208.94.118.224 **Country:** United States of America **Region:** Florida **City:** Lake Mary **Latitude:** 28.759920 **Longitude:** -81.345840 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.paypal.com	ok	**IP:** 151.101.129.21 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

---

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.