



ANDROID STATIC ANALYSIS REPORT

app_icon

 VPN Hotspot (2.11.2)

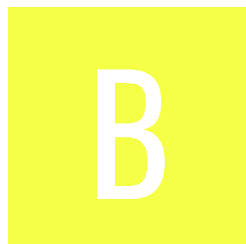
File Name: installer104.apk

Package Name: be.mygod.vpnhotspot

Scan Date: May 31, 2022, 9:26 a.m.






App Security Score: 50/100 (MEDIUM RISK)

Grade:



Trackers Detection: 2/428

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
0	16	1	0	1

FILE INFORMATION

File Name: installer104.apk

Size: 3.14MB

MD5: 7be5b1d6e16cddabcd613956dfb0774c

SHA1: aff7b00819003e8ce9c02515929fd2d4ecb46543

SHA256: 437e80a9880a647ab539bf54173a70708849490507556b7653e9ffd4eb08af83

APP INFORMATION

App Name: VPN Hotspot

Package Name: be.mygod.vpnhotspot

Main Activity: be.mygod.vpnhotspot.MainActivity

Target SDK: 29

Min SDK: 21

Max SDK:

Android Version Name: 2.11.2

Android Version Code: 255

APP COMPONENTS

Activities: 5

Services: 18

Receivers: 3

Providers: 1

Exported Activities: 0

Exported Services: **9**

Exported Receivers: **1**

Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed

v1 signature: True

v2 signature: True

v3 signature: False

Found 1 unique certificates

Subject: C=CN, ST=Mygod, L=Mygod, O=Mygod, OU=Mygod, CN=Mygod

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2014-05-02 09:24:19+00:00

Valid To: 3013-09-02 09:24:19+00:00

Issuer: C=CN, ST=Mygod, L=Mygod, O=Mygod, OU=Mygod, CN=Mygod

Serial Number: 0x5337eff0

Hash Algorithm: sha256

md5: 2db6659af31b446de7f33b348310b7de

sha1: 26828f9821220cf5a9b2fa1f50d8c643c4e5f21c

sha256: 724fffe17e1188533c0d6a7af3c1dc12947cb554323af2b187c1f5ec1963f2b7

sha512: b876e5e612c7e1d03a3b6c3db24f9c00dd315f717b1ab5d5fc4a58fcdb4271eecd875e86a0175705d5ed9f42cd9e20f87972f174fd1f8d585b6db37bf33ce104

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: 84157c0c7442dd3cbd13caca6b2ca346592418644bc40fdca7346f9d1efdd4fb

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.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.CHANGE_NETWORK_STATE	normal	change network connectivity	Allows applications to change network connectivity state.

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.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.LOCAL_MAC_ADDRESS	unknown	Unknown permission	Unknown permission from android reference
android.permission.MANAGE_USB	unknown	Unknown permission	Unknown permission from android reference
android.permission.OVERRIDE_WIFI_CONFIG	unknown	Unknown permission	Unknown permission from android reference
android.permission.READ_WIFI_CREDENTIAL	unknown	Unknown permission	Unknown permission from android reference
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.TETHER_PRIVILEGED	unknown	Unknown permission	Unknown permission from android reference

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_SECURE_SETTINGS	SignatureOrSystem	modify secure system settings	Allows an application to modify the system's secure settings data. Not for use by common applications.
android.permission.WRITE_SETTINGS	dangerous	modify global system settings	Allows an application to modify the system's settings data. Malicious applications can corrupt your system's configuration.
com.android.vending.BILLING	unknown	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
------	---------

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.TAGS check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8
classes2.dex	FINDINGS	DETAILS
	Compiler	r8

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Service (be.mygod.vpnhotspot.manage.RepeaterTileService) 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.
2	Service (be.mygod.vpnhotspot.manage.LocalOnlyHotspotTileService) 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.
3	Service (be.mygod.vpnhotspot.manage.TetheringTileService\$Wifi) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Service (be.mygod.vpnhotspot.manage.TetheringTileService\$Usb) 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.
5	Service (be.mygod.vpnhotspot.manage.TetheringTileService\$Bluetooth) 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.
6	Service (be.mygod.vpnhotspot.manage.TetheringTileService\$Ethernet) 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.
7	Service (be.mygod.vpnhotspot.manage.TetheringTileService\$Ncm) 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.

NO	ISSUE	SEVERITY	DESCRIPTION
8	Service (be.mygod.vpnhotspot.manage.TetheringTileService\$WiGig) 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.
9	Service (be.mygod.vpnhotspot.manage.TetheringTileService\$WifiLegacy) 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.
10	Broadcast Receiver (be.mygod.vpnhotspot.BootReceiver) 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.

</> 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	be/mygod/vpnhotspot/root/RoutingCommands\$Clean\$execute\$2.java be/mygod/vpnhotspot/App.java be/mygod/vpnhotspot/root/RootManager.java be/mygod/vpnhotspot/util/Services\$p2p\$2.java
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	be/mygod/vpnhotspot/net/Routing.java be/mygod/vpnhotspot/preference/UpstreamsPreference.java
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/mygod/vpnhotspot/SettingsPreferenceFragment.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	j\$/util/concurrent/d.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', 'bluetooth', 'location'].
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_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.
12	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
13	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
14	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.
15	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.
16	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
ipinfo.io	ok	IP: 34.117.59.81 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
mygod.be	ok	IP: 104.21.59.170 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
macvendors.co	ok	IP: 188.114.96.0 Country: Spain Region: Madrid, Comunidad de City: Madrid Latitude: 40.416500 Longitude: -3.702560 View: Google Map

DOMAIN	STATUS	GEOLOCATION
mygod-vpnhotspot.firebaseio.com	ok	IP: 35.201.97.85 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 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

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://mygod-vpnhotspot.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
this@repeatermanager.javaclass	be/mygod/vpnhotspot/manage/RepeaterManager\$configure\$1.java

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"firebase_database_url" : "https://mygod-vpnhotspot.firebaseio.com"
"google_api_key" : "AlzaSyADp0gTf25H6H3KxDRKwvp0EaWq_XvYUmg"
"google_crash_reporting_api_key" : "AlzaSyADp0gTf25H6H3KxDRKwvp0EaWq_XvYUmg"
"wifi_password" : "Password"
"wifi_password" : "Password"
"wifi_password" : "Пароль"

POSSIBLE SECRETS
"wifi_password" : "密码"
"wifi_password" : "密碼"

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](#).