LG Electronics USA

Date: January 24, 2024

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES
(594280 D02 U-NII Device Security 1.3, 11/12/15)

Company Name: LG Electronics USA
FCC ID: BEJ-MIB3CLASSIC
Product Name: Car Navigation

SOFTWARE SECURITY DESCRIPTION	
General Description	
Q.	1. Describe how any software/firmware updates for elements than can affect the device's RF parameters will be obtained, downloaded, validated and installed. For software that is accessed through manufacturer's website or device's management system, describe the different levels of security as appropriate.
A.	RF module FW updated can only be done by grantee, update the FW via USB port on the Factory tool. The tool can check the firmware version, set RF Power and MAC address. The SSID, WIFI mode, password and country-specific channel settings of the RF module are made through this firmware.
Q.	2. Describe the RF parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited such that any other software/firmware changes will not allow the device to exceed the authorized RF characteristics?
A.	There are all RF parameters are hard-coded in the factory, you can change the ssid, password, only one RF parameters through the UI.
Q.	3. Describe in detail the authentication protocols that are in place to ensure that the source of the RF-related software/firmware is valid. Describe in detail how the RF-related software is protected against modification.
A.	This device has an 802.11b/g/n/ac protocol. The FW on the device does not support writing to NVM(non-volatile memory) including FW, except through the use of our FW update tools. In addition, through our firmware driver, this RF device is set to use only 802.11n/ac protocol.
Q.	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
A.	Same to answer #3.
Q.	5. For a device that can be configured as a master and client (with active or passive scanning), explain how the device ensures compliance for each mode? In particular, if the device acts as master in some band of operation and client in another; how is compliance ensured in each band of operation?
A.	Master and client settings of the device are fixed with hardcoding and can not be changed.

LG Electronics USA

Third-Party Access Control
1. Explain if any third parties have the capability to operate a U.S.-sold device on any other regulatory domain, frequencies, or in any manner that may allow the device to operate in violation of the device's authorization if activated in the U.S.
No, Any 3rd parties don't have capability to access and change this module. All RF settings are factory hard-coded into country-specific factory codes.
2. Describe, if the device permits third-party software or firmware installation, what mechanisms are provided by the manufacturer to permit integration of such functions while ensuring that the RF parameters of the device cannot be operated outside its authorization for operation in the U.S. In the description include what controls and/or agreements are in place with providers of third-party functionality to ensure the devices' underlying RF parameters are unchanged and how the manufacturer verifies the functionality.
There is only single US version of SW. All US sold devices are locked to the US FCC rule and will never operate in manner that violates the FCC rule. The country lock is located in memory that unaffected by factory reset.
3. For Certified Transmitter modular devices, describe how the module grantee ensures that host manufacturers fully comply with these software security requirements for U-NII devices. If the module is controlled through driver software loaded in the host, describe how the drivers are controlled and managed such that the modular transmitter RF parameters are not modified outside the grant of authorization.
All RF parameter was hardcoded at the factory, any OEM or system integrator will not able to modify, therefore, RF module will remains compliance when used or installed into any system.

SOFTWARE CONFIGURATION DESCRIPTION	
USER- CONFIGURATION GUIDE	
Q.	1. Describe the user configurations permitted through the UI. If different levels of access are permitted for professional installers, system integrators or end-users, describe the differences.
A.	Only the SSID and Password can be configured with the UI.
Q.	a. What parameters are viewable and configurable by different parties?[9]
A.	SSID, Password
Q.	b. What parameters are accessible or modifiable by the professional installer or system integrators?
A.	Not accessible configurations except SSID and Password by UI.
Q.	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
A.	Same to answer #1-b).

Q.	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
A.	Same to answer #1-b).
Q.	c. What parameters are accessible or modifiable by the end-user?
A.	SSID, Password
Q.	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
A.	Not accessible configurations except SSID and Password by UI.
Q.	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?
A.	Same to answer #1-c).
Q.	d. Is the country code factory set? Can it be changed in the UI?
A.	The country code factory is set. Can not change in the UI.
Q.	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
A.	Same to answer #1-d).
Q.	e. What are the default parameters when the device is restarted?
A.	Same as previous setting.
Q.	2. Can the radio be configured in bridge or mesh mode? If yes, an attestation may be required. Further information is available in KDB Publication 905462 D02.
A.	No. This device cannot be configured in a bridge or mesh mode.
Q.	3. For a device that can be configured as a master and client (with active or passive scanning), if this is user configurable, describe what controls exist, within the UI, to ensure compliance for each mode. If the device acts as a master in some bands and client in others, how is this configured to ensure compliance?
A.	The master and client are fixed with hardcoding and can not be changed. Only ssid and password can be changed.
Q.	4. For a device that can be configured as different types of access points, such as point-to-point or point-to-multipoint, and use different types of antennas, describe what controls exist to ensure compliance with applicable limits and the proper antenna is used for each mode of operation.
A.	Two antenna fixed for each purpose (first antenna 5G, Second antenna 2G), and configuration change not possible by UI.

Signature
Company: LG Electronics USA
Title: Team leader, LGEUS NA Policy & Regulatory Affairs
Name: David, Kim