SOFTWARE SECURITY FOR U-NII DEVICES

Date: March 30, 2020

FCC ID: 2AUEH-DB133MU2

Pursuant to FCC Part 15E 15.407(i) and KDB 594280 D02 U-NII Device Security, applicant must describe the overall security measures and systems that ensure that only:

1. Authenticated software is loaded and operating the device.
2. The device is not easily modified to operate with RF parameters outside of the authorization

The description of the software must address the following questions in the operational description for the device and clearly demonstrate how the device meets the security requirements.

General Description	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.
	(1) Obtain and download The firmware could be obtained from the companion PC application. User can download the companion PC application from the specific WEB site. (2) Install User can install new firmware by clicking on the UI menu of the companion PC application.
	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?
	Two radio frequency parameters cannot be configured via UI: Channel and Channel Bandwidth. All above two parameters are pre-installed and cannot be configured.
	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.
	Firmware has a private signature inside. If firmware is modified, then it cannot be allowed to be upgraded.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
	Not Supported.
	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?
	Our device works as following configuration: 2412-2462MHz : active scan 5180-5240 / 5745-5825MHz : active scan 5260-5320 / 5500-5720MHz : passive scan This configuration is pre-installed and cannot be configured.

3rd 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.
	The parameters of country, frequencies and etc. are permanent settings and cannot be configured. The device can operate only at authorized frequencies and bandwidth.
	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.
	It is impossible. Our software/firmware has a private signature inside. If firmware is modified, then it cannot be allowed to be upgraded.
	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.
	The driver including modular transmitter parameter is implemented in our product software and cannot be replaced.

User Configuration guide	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.
	Professional installer, system integrators and end-user can select the frequency bands from 2.4GHz or 5GHz.
	a) What parameters are viewable and configurable by different parties?
	Professional installer, system integrators and end-user cannot see any RF parameters, other than frequency bands.
	b) What parameters are accessible or modifiable by the professional installer or system integrators?
	Professional installer, system integrators and end-user cannot access any RF parameters. They can select frequency bands from authorized frequency bands list.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	Professional installer, system integrators and end-user cannot access any RF parameters, other than frequency bands. They can select frequency bands from authorized frequency bands list.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	The parameters of country, frequencies and etc. are permanent settings and cannot be configured.

User Configuration guide	c) What parameters are accessible or modifiable to by the end-user?
	The end user can select frequency bands from authorized frequency bands.
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
	The installers can select frequency bands from authorized frequency bands list.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	The parameters of country, frequencies and etc. are permanent settings and cannot be configured.
	d) Is the country code factory set? Can it be changed in the UI?
	It is factory set and cannot be changed in the UI.
	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
	NA
	e) What are the default parameters when the device is restarted?
	The parameters of country, frequencies and etc. are permanent settings and cannot be configured.
	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.
	Our device does not support mesh mode or bridge mode.
	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?
	Our device works as master mode other than DFS band.
	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. (See Section 15.407(a))
	This device has dedicated antenna and it won't change the type or characteristics.

Signature: Robin Yeh

Name (Printed): Robin Yeh

Title: Deputy Manager

On behalf of Company: LINFINY CORPORATION

Telephone: 03 564 3200

Address: No. 199, Huaya 2nd Rd., Guishan Dist., Taoyuan City 333, Taiwan (R.O.C.)