Date: 2024-08-05

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

Company Name: Chengdu Hotack Technology Co., Ltd.
FCC ID: 2BFIZ-L007CM
Product Name: PROJECTOR

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.	Software/Firmware is pushed from the manufacturer's authorized servers by means of encryption by OTA. But user can't obtain unauthorized software/firmware cause update packages are encrypted and digitally signed by proprietary key.
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.	All the RF parameters could not be modified through software changed.
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.	All firmware update only comes from manufacturer which manufacturer will ensure that the source of software/firmware is legitimate. They are digitally signed and encrypted using proprietary handshaking, authorization and provisioning protocols. Secure sockets Layer is used as a protocol for encrypting information over the internet.
Q.	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
A.	Before firmware/software updated, there was an encrypted ID code-checking mechanism to ensure the source was authorized by manufacturer. Any unauthorized source will by blocked and fail to install. all source code was encrypted.
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.	This device can be operated as both master and client mode in WIFI 2.4GHz . In 5G, it only can be operated as client mode. For compliance, device will transmit under approved power, and user can't access to change Master/client feature per band.

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.
The Wi-Fi channels are pre-configured in factory. Users are not allowed to change. No interface is provided to read these data, and the data are random password protected.
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.
Third-party software or firmware installation is NOT allowed. The firmware update will not change the Wi-Fi channel plan. The Wi-Fi channel plan is written to the ROM on the Wi-Fi module. The hardware is locked with Actiontec firmware, because we use AES, RSA, HASH mechanisms.
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.
N/A

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.	Configurations permitted through the UI include UI language, receiver name, USB access, connection PIN, selection of WiFi channel, transmit power, IP address, local and remote management. Configurations are allowed for all users.
	a. What parameters are viewable and configurable by different parties?
	Authorized channel, bandwidth, and modulation.
	b. What parameters are accessible or modifiable by the professional installer or system integrators?
	This is not professional install device.
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	This is not professional install device.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	There is no such control. The parameters are preconfigured based on the sales area in manufacture.
	c. What parameters are accessible or modifiable by the end-user?
	There is no such control. The parameters are preconfigured based on the sales area in manufacture.

	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
	No.
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?
	There is no such control. The parameters are preconfigured based on the sales area in manufacture.
	d. Is the country code factory set? Can it be changed in the UI?
	The country code is factory set. It can NOT 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.?
	e. What are the default parameters when the device is restarted?
	The parameters saved last time will preserve after the device is restarted.
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 v01r03.
A.	No.
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.	This device can be operated as both master and client mode . For compliance, device will transmit under approved power, and user can't access to change Master/client feature per band.This Device was verified by 3rd party lab and compliant to FCC rule.
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.	There is three type antenna for this product. It can't be connected to other antenna.

Signature:

Star Hu

Company: Chengdu Hotack Technology Co., Ltd.
Title: Manager
Name: Star Hu
Address: 501-502, Unit 3, Building 13, No. 666 Jinfenghuang Avenue, High-tech Industry Park, Jinniu District, Chengdu, China