Date: 2023/7/21

SOFTWARE SECURITY REQUIREMENTS FOR FabWash
(FabWash Device Security)

FCC ID: 2AMG4-FABWASH
Product Name: FabWash
Model No.: FabWash

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.	Upgrade by OTA, Any firmware updates can not affect RF parameters.
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.	The RF parameters/limits are stored in a separate part of the non-volatile storage and not updated or changed with the firmware updates.
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.	There are currently no authentication protocols in place to check for a valid firmware outside of product registration and serial number.
Q.	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.
A.	Firmware are not encrypted. RF related parameters/limits are stored in a spate part of non-volatile storage and are not part of the firmware.
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.	The device is client device without radar detection function.

Third-Party Access Control	
Q.	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.
A.	No, third party have no capability to operate.
Q.	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.
A.	Installation of third-party software or firmware is not permitted.
Q.	3. For Certified Transmitter modular devices, describe how the module grantee ensures that host manufacturers fully comply with these software security requirements for FabWash 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.
A.	The RF parameters/limits are stored in a separate part of the non-volatile storage and not updated or changed with the firmware updates, and no interface is open for users to modify

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.	No configuration permitted for the third parts through the UI.
Q	a. What parameters are viewable and configurable by different parties?[9]
A	No parameters are viewable and configurable by third party
Q	b. What parameters are accessible or modifiable by the professional installer or system integrators?
A	No interface is open for users to modify
Q	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
A	No interface is open for users to modify
Q	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
A	Modify is not allowed.
Q	c. What parameters are accessible or modifiable by the end-user?

A	No parameters are accessible or modifiable by the end-user
Q	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
A	The parameters are programmed in flash memory and not accessible to the end-user.
Q	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S.?
A	No interface is provided to user to operate outside its authorization
Q	d. Is the country code factory set? Can it be changed in the UI?
A	The country code is factory set and can not be changed 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	Can not be changed out of factory
Q	e. What are the default parameters when the device is restarted?
A	Same as factory set.
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.	Not supported.
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.	When the device is a client, the parameters are determined by the master. When the device is a master, the RF channel parameters are fixed as band channel 11 and cannot be modified. (The devices cannot connect to each other.)
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.	Only point-to-point type

Signature:

Company: Shining 3D Tech Co., Ltd
Address: No.1398, Xiangbin Road, Wenyan, XiaoShan, HangZhou, ZheJiang, China,
Name: Da Chen
Title: Product Manager

Da Chen

2023-10-18