DocuSign Envelope ID: 67BD5883-A21C-42FC-BDCD-75BF0EFB1750

Date: November 13, 2018

SOFTWARE SECURITY DESCRIPTION

rev_01

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.

The RF parameters are controlled by authenticated (signed) Augury firmware images. Any firmware update verifies the integrity of the installed firmware to assure that only tested and approved firmware updates are installed on the appliance.

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?

All tests were performed using the highest possible power setting of the RF modules, no additional software/firmware can case the the RF characteristics to exceed the values that were tested for the FCC/IC/RED certification.

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.

All firmware images that may be installed on the appliance are verified for integrity and authenticity. A SHA256 hash value is computed for the software image to assure integrity. An RSA digital signature of the respective hash digest of the software image is provided to authenticate the image source.

4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.

RSA signature of SHA256 digest of a software update image is provided with any software update and verified by the platform before performing firmware upgrade.

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?

DocuSign Envelope ID: 67BD5883-A21C-42FC-BDCD-75BF0EFB1750

Compliance of the RF device of the appliance is controlled by the device firmware image as well as the device initialization configuration file. Both of these components are part of the firmware image that is verified for integrity using the methods detailed above. The configuration as either a master or as a slave cannot control the RF bands used by the wifi or Bluetooth device, and can only select one of the RF channels as defined by the respective standards.

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 RF devices firmware as well as their initialization configuration files control the device function to comply with U.S. standards that may be applicable. No third party component or configuration data may be installed on the appliance in any way that can exceed the limitations of the firmware and device initialization configuration.

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.

The device does not support third-party software/firmware installation. Any configuration of the wireless devices within the appliance cannot exceed the limitations enforced by the pre-installed firmware and configuration.

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.

U-NII isn't for 5GHz bands, This devices is not certified to operate in the 5GHz band, and is is disabled.

DocuSign Envelope ID: 67BD5883-A21C-42FC-BDCD-75BF0EFB1750

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.
a. What parameters are viewable and ~~configurable~~ by different parties?

All professional installers, system integrators and end-users can view the following parameters: Wifi/BLE signal strength, Node 2.0 name and Serial number, Hw Mapping and system mapping.

b. What parameters are accessible or modifiable by the professional installer or system integrators?

Professional installer/System integrators have the ability to:

- Configure which Halo Sensors (BLE peripherals) can interface with NODE 2.0.

- Configure the Node to act as either a wifi client or a wifi AP.

- Define the SSID and credentials of a wifi AP to connect with, when acting as a client.

(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?

The professional installer can only control parameters through an installation app. This limits control only to the attributes detailed above. None of these attributes control the RF communication power or explicitly selects RF.

(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?

The user has no access to any communication attributes of the device. Professional installer may only select operation mode and selected peers to communicate with, as detailed above.

c. What parameters are accessible or modifiable by the end-user?

No parameter is accessible or controlled by an end-user. Only professional installers or system engineers may control the device.

(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?
(2)What controls exist so that the user cannot operate the device outside its authorization in the U.S.?

d. Is the country code factory set? Can it be changed in the UI?

DocuSign Envelope ID: 67BD5883-A21C-42FC-BDCD-75BF0EFB1750

The country code is not configurable by the user. It is fixed by firmware configuration to the respective country code.

(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?

Following a factory reset state, the device is configured to start a wifi AP at channel 7. Alternatively, the device may work as wifi infrastructure client, scanning for pre-defined SSID (i.e., channel will be determined by the infrastructure AP).

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.

The device does not operate in bridge or mesh 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?

The device acts as master following BLE specifications. In addition, it acts as a master (wifi AP) on a fixed authorized wifi channel (7, by default). When acting as a client, the device scans authorized wifi channels for the region.

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))

Not applicable.

By signing this document, we declare that the information stated on this document is true and correct

DocuSigned by:
Shammai Weiss
84C6754597E34DB...

Signature

Name: Isaac s weiss
Position: Head of physical design Email: Info@augury.com
Company name: Augury systems Ltd.
Company number: 514746155
Address: 39 Haatzmaut St., 1st Floor, Haifa, 3303320, Israel
Telephone No: 972-77-4395527 Fax No: 972-77-3013791