Sagemcom

SAGEMCOM BROADBAND SAS

RUEIL MALMAISON 2017/6/10

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.

Software Security Description

1. Describe how any software/firmware update will be obtained, downloaded and installed Description: A new software update is initiated through the ACS (Automatic Configuration System), which instruct the software to retrieve a new software image from a given URL.
2. Describe all the radio frequency parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited, such that, it will not exceed the authorized parameters? Description: We set the default parameters we get in the BSP/WiFi driver in OpenRG rg_conf We have only authorized parameters.
3. Are there any authentication protocols in place to ensure that the source of the software/firmware is legitimate? If so, describe in details; if not, explain how the software is secured from modification Description: Per TR-69 specifications, the software initiates a connection to the ACS (ACS cannot connect to the software), based on factory settings . Only the ACS can instruct the software to download a new image and provides the URL. This is a workflow that personal initiate and the ACS is within secured network. The Downloaded firmware is signed with an RSA key which is validated by OpenRG before upgrading
4. Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details Description: Same as #3 above
5. Describe, if any, encryption methods used Description: The image is not encrypted only signed.
6. 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 Description: Not relevant, the device is only master

7. How are unauthorized software/firmware changes prevented? Description: In general, the end user has no access to the flash memory and thus cannot burn a new image on top of the existing one. A new image is only updated per the above described procedure.
8. Is it possible for third parties to load device drivers that could modify the RF parameters, country of operation or other parameters which impact device compliance? If so, describe procedures to ensure that only approved drivers are loaded. Description: The device drivers are part of the entire image containing all software components. There is no telnet or CLI access to a manfucature device, thus a 3rd party have no access to replace a driver at run-time.
9. Explain if any third parties have the capability to operate a US sold device on any other regulatory domain, frequencies, or in any manner that is in violation of the certification. Description: Only the ACS can manage the device. All other management interfaces are disabled
10. What prevents third parties from loading non-US versions of the software/firmware on the device? Description: 3rd parties cannot replace the software on the device, per the answers in "General Description" section. As such, the drivers cannot be replaced to a non-US version.
11. For modular devices, describe how authentication is achieved when used with different hosts. Description: Not relevant, there is no modular device into the device.

In addition to the general security consideration, for devices which have “User Interfaces” (UI) to configure the device in a manner that may impact the operational parameter, the following questions shall be answered by the applicant and the information included in the operational description.

USER CONFIGURATION GUIDE

Sagemcom

1. To whom is the UI accessible? (Professional installer, end user, other.)
   Description:
   The UI is accessible to the end user and professional installer. In addition, a support call personnal can also access the UI when in need.

a) What parameters are viewable to the professional installer/end-user?
   Description:
   The user\installer can set the SSID and Channel Only.

b) What parameters are accessible or modifiable to the professional installer?
   Description:
   Same as end user

   i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
   Description:
   Yes, the UI has input verification that ensures only valid values are entered.

   ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
   Description:
   The end user UI has limitation on the values the user can enter and verification is done on those parameters. The UI itself is located in core network, and changes are then moved through APIs to the ACS, which has value verification per the data model. In addition the driver country code is us and it will not allow invalid settings - need to verify with vendor.

c) What configuration options are available to the end-user?
   Description:
   Wifi related: SSID, Channel

   i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
   Description:
   Yes, the UI has input verification that ensures only valid values are entered.

   ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
   Description:
   The end user UI has limitation on the values the user can enter and verification is done on those parameters. The UI itself is located in core network, and changes are then moved through APIs to the ACS, which has value verification per the data model.

d) Is the country code factory set? Can it be changed in the UI?
   Description:
   The country code is factory set and it cannot be changed via UI

   i) If so, 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?
   Description:
   If the device is restarted all the parameters have their default values from radio calibration done in factory and conform to FCC.

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. Description: There is no such option in the UI to do so.
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? Description: Not relevant, the device is only master.
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)) Description: Not applicable. It cannot be configured differently through OpenRG UI.

How the product comply 15.407(c)
Description: WIFI chip support automatically discontinue transmission in case of either absence of information to transmit or operational failure, if the chip detect absence of information to transmit or operational failure, it will be automatically shut off.