Software security for UNII Devices

Varian Medical Systems, Inc.
Oncology Systems
3100 Hansen Way
Palo Alto, CA 94304-1038
UNITED STATES

To Whom It May Concern:

Product/Model: Visual Coaching Device (VCD)

FCC ID: 2AGCP-VCDT711N

General Description

1. Describe how any software/firmware update will be obtained, downloaded, and installed. Software that is accessed through manufacturer's website or device's management system, must describe the different levels of security.

The Visual Coaching Device provides an over the air update mechanism (OTA). The update interface is a dedicated SW interface developed by Varian. Internally the standard Android Open Source mechanism is used. The software packages are signed with a dedicated Varian key and only accepted if the signature is valid.

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?

The Bluetooth and the 5 GHz band of the WIFI are deactivated in the operating system.

3. Describe in detail the authentication protocols that are in place to ensure that the source of the software/firmware is legitimate. Describe in detail how the software is protected against modification.

The software repository is shipped on a physical drive from the CPU Board vendor. The access of the build system is password protected.

4. Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate.

Only signed packages of the operating system and application can be installed on the device.

5. Describe in detail any encryption methods used to support the use of legitimate software/firmware.

The software packages are signed with a pk8 private key, which is secret and password protected. The signature is checked on the device by the x509 certificate.

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?

The Visual Coaching Device only acts as a client.

Third-Party Access Control

1. 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.

The VCD only allows remote upgrades through the provided Varian interface. Only software packages signed with a Varian key are allowed to be installed. The VCD does not provide an app store or similar to install software directly from the Internet.

The software is stored on a SD card inside the VCD which is accessible for Varian service only. A third party could replace this SD card with a manipulated version to feed in its own software configuration. The Android Open Source needs several adaptions to run with the used hardware setup. Therefore this is very unlikely.

2. What prevents third parties from loading non-US versions of the software/firmware on the device? Describe in detail how the device is protected from "flashing" and the installation of third-party firmware such as DD-WRT.

The serial port is not assembled on our PCB. A third party does not have access to the boot loader and can't flash a custom firmware. The only way for an upgrade is the dedicated remote SW interface.

3. For Certified Transmitter modular devices, describe how the module grantee ensures that hosts manufactures 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 parameters are not modified outside the grant of authorization.

The operating system includes all the drivers and configurations and is released as one single package. The VCD only allows the update of the full package and not an individual driver.

The operating system, drivers and configuration is maintained by Varian.

USER CONFIGURATION GUIDE

1. To whom is the UI accessible? (Professional installer, end user, other.)

The VCD is mainly used by the employees of a hospital and their patients. During installation or servicing the VCD is used by trained installers.

a) What parameters are viewable to the professional installer/end-user?9

The following settings are displayed (read only) to an installer:

- Battery status as temperature, charging level, remaining capacity.
- System overview as software version, memory usage, CPU information

b) What parameters are accessible or modifiable by the professional installer?

The installer can adjust the following settings:

- Brightness of the background light
- Enable or disable the screen rotation
- Set the USB port into master mode to power a video goggle.
- Select one of the available WIFI networks as the default network

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

The installer cannot change any parameter which leads into a violation of any regulatory requirement.

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

The coaching application is running in “kiosk mode”. This means the user has no access to the operating system settings. The coaching application itself only provides access to settings which cannot lead to a violation of any regulatory requirement.

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

The end user can adjust the following settings:

- Brightness of the background light
- Enable or disable the screen rotation
- Set the USB port into master mode to power a video goggle.
- Select one of the available WIFI networks as the default network

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

The end user cannot change any parameter which leads into a violation of any regulatory requirement.

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

The coaching application is running in “kiosk mode”. This means the user has no access to the operating system settings. The coaching application itself only provides access to settings which cannot lead to a violation of any regulatory requirement.

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

By default the country code is set to US. After connecting to the access point the country code of the access point is applied. There is no UI to change the country code.

(1) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?

Not applicable since there is no UI to set the country code.

e) What are the default parameters when the device is restarted?

The values which can be modified by the user (see 1a and 1b above) are persistent and still active after a restart.

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.

No, the device only works as a client.

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 only works as a client.

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))

The device does not support different types of access points.