SOFTWARE SECURITY DECLARATION FOR U-NII DEVICES

Kinoma Create

December 2, 2015

This document is prepared for the Marvell Kinoma Create device, and the document responds to the questions posed in KDB 594280 D02 U-NII Device Security v01r03 (Nov. 12, 2015).

Kinoma Create is a prototyping device for developing internet connected embedded devices. The device is powered by an efficient ARM CPU with Wi-Fi connectivity (802.11ac 1x1), and has a capacitive color touch screen and 66 I/O pins.

The following terminologies are used in this declaration:

1. Host software/firmware: these include host operating system and device driver running on host CPU.
2. Wi-Fi firmware: this refers to the embedded Wi-Fi firmware running on the Wi-Fi connectivity chip. This is specialized software that configures and controls the underlying Wi-Fi hardware, including RF parameter settings.

The following is a summary of security measures taken to ensure FCC compliance:

1. The FCC Region Code is factory-set in OTP (one-time-programmable memory) on the device and is fixed in Wi-Fi firmware.
2. The RF parameter settings are restricted in the Wi-Fi firmware based on Region Code. For FCC region, the RF parameters are restricted to be compliant with FCC rules, for both client and master modes.
3. Kinoma Create is only configured in client mode by default and through the user interface. The user interface does not support access point (master) mode configuration.
4. Kinoma Create uses the same antenna for all modes of operations.
5. Kinoma Create software/firmware updates are retrieved using the HTTPS protocol for secure file transfer and a private certificate for authentication.
6. A non-standard CRC32 based integrity check is built into the Wi-Fi firmware loading procedure to ensure that the source has not been tampered with.
7. An OTP flag is used to invalidate previously released Wi-Fi firmware and make the device inoperable.

SOFTWARE SECURITY DESCRIPTION	
General Description	1. Describe how any software/firmware updates for elements that 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. *[MRVL]* *The user interface of Kinoma Create provides a visual indication to the user when a software update is available. All updates are initiated by the user, there are no automatic updates. Updates are retrieved from a Marvell managed web server hosted on Amazon Cloud Services. The updates are retrieved using the HTTPS protocol* for secure file transfer and a private certificate for authentication. *The RF parameter settings are restricted in the Wi-Fi firmware. Only compiled Wi-Fi firmware binary code is available for download, not source code. Please refer to questions 2 and 3 for RF parameters compliance and additional Wi-Fi firmware security protection.*
	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? *[MRVL]* *The Wi-Fi firmware provides an API which can be called to configure the Wi-Fi band, channel number, bandwidth, and Tx power level. The allowable settings are restricted to Region Code of the device. The Kinoma Create devices have factory-set FCC Region Code in OTP (one-time programmable memory) and the RF parameter settings are restricted to be compliant with FCC rules in the Wi-Fi firmware.*

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.

[MRVL]

The RF-related software/firmware is the Wi-Fi firmware.

The Wi-Fi connectivity chip is a specialized ASIC (application-specific-integrated-circuit) which contains specialized hardware and software to optimize performance. The radio is integrated into the Wi-Fi chip. For the device to operate properly, thousands of registers need to be programmed in the correct sequence by the Wi-Fi firmware. All design documents are Marvell trade secrets and are well controlled within the company. For customers of Kinoma Create, datasheet and register information are not shared.

Only compiled Wi-Fi firmware binary code is available for download, not source code.

A CRC32 based integrity check is built into the Wi-Fi firmware loading procedure to ensure that the source has not been tampered with. The CRC32 is calculated across each downloaded firmware section. This CRC check is a non-standard procedure and not shared with customers, so it is not easily reproducible by developers unfamiliar with the internal design of the Wi-Fi chip.

A version flag is programmed into the OTP of the Wi-Fi chip. This flag ensures that older versions of the Wi-Fi firmware, which did not respect the Region Code, will not be recognized by the Wi-Fi chip and therefore will not run. This prevents an attacker from rolling back to an older version of the Wi-Fi firmware which did not limit RF parameters based on the Region Code.

To date, there is no known case of our Wi-Fi firmware being modified or replaced.

Any other attempts, i.e. through device driver, to operate outside the authorized range will be disqualified by Wi-Fi firmware and will not take effect on the Wi-Fi radio.

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

[MRVL]

The Wi-Fi firmware is not encrypted. As described in the response to Question 3, the nature of the device and the built-in firmware download and verification process make it difficult for a 3rd party to create a new Wi-Fi firmware or modify an existing firmware, to successfully download it onto the device, and to make it operable.

	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? *[MRVL]* *Kinoma Create is configured only as a client device by default and through user interface.* *The Wi-Fi chip and firmware support both master and client modes. In order to configure the device as an access point (AP), a user would need to change the kernel software and device driver to enable AP mode and recompile the host software.* *The Wi-Fi firmware, with fixed FCC Region Code, restricts RF parameters to be FCC compliant for both master and client modes. More specifically, without DFS master mode certification from FCC, the DFS channels (U-NII-2A and U-NII-2C) are excluded from the channel list in master mode. Thus, even if the Kinoma Create were reconfigured to act as a mini-access point, the device would still operate in compliance with the FCC requirements. Any attempt to program RF settings outside of these authorized ranges will be disqualified by the Wi-Fi firmware.*

Third-Party Access Control	1. <u>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.</u> *[MRVL]* *For U.S.-sold devices, the FCC Region Code is factory-set in the OTP of the device. The Wi-Fi firmware either uses fixed FCC Region Code or uses Region Code set in the OTP of the device, and restricts RF settings accordingly.* *A third party may load a non-U.S. version of the Wi-Fi firmware; however, at runtime, the Wi-Fi firmware uses FCC Region Code in the OTP and restricts RF settings to FCC authorized range.* *This helps to ensure FCC compliance for US-sold devices.*

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.

[MRVL]
Kinoma Create is a device designed to be used by hardware and software developers to prototype new products. To fulfill this goal, the device allows developers to modify, update, and install software/firmware, including the Wi-Fi firmware that controls the device's underlying RF parameters. However, only authorized Wi-Fi firmware can be run on the Wi-Fi chip. All authorized Wi-Fi firmware for Kinoma Create restricts RF parameters to be within the FCC authorized range. Any attempts to operate outside the FCC authorized range will be disqualified by the Wi-Fi firmware and will not take effect on the Wi-Fi radio.

As described in the response to Question 3 in the General Description section, it is difficult to create an un-authorized Wi-Fi firmware, to successfully download it onto the device, and to make it operable:

a) *The Wi-Fi connectivity chip is an ASIC with integrated radio. For the device to operate properly, thousands of registers need to be programmed in the correct sequence by the Wi-Fi firmware. Datasheet and register information are well controlled within the company and not shared with Kinoma Create customers. This makes it difficult for a third-party to create a functioning Wi-Fi firmware from scratch.*

b) *Only compiled Wi-Fi firmware image is available for download, not the source code. This makes it difficult for a third-party to modify the Wi-Fi firmware.*

c) *The proprietary CRC32 based integrity check during Wi-Fi firmware downloading procedure prevents a third party from successfully downloading a modified Wi-Fi firmware onto the device. This makes it difficult to run a modified Wi-Fi firmware on the device.*

d) *Older versions of the Wi-Fi firmware, which does not respect the FCC Region Code, will be invalidated by an OTP flag on the device and made in-operable. This prevents an attacker from rolling back to an older version of the Wi-Fi firmware which did not limit RF parameters based on the Region Code.*

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.

[MRVL]
Not applicable. There is no user detachable radio module in this system.

SOFTWARE CONFIGURATION DESCRIPTION	
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. *[MRVL]* *The user interface of Kinoma Create is only for end users. There is no professional installer or system integrator user interface. Wi-Fi configuration is limited to selecting an access point to connect to and providing the password for the access point, if needed.*
	a) What parameters are viewable and configurable by different parties? *[MRVL] None.*
	b) What parameters are accessible or modifiable by the professional installer or system integrators *[MRVL] None.*
	i) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? *[MRVL]* *The installer will not be able to change parameters that exceed the authorized limits, as restricted by the Wi-Fi firmware.*
	ii) What controls exist that the user cannot operate the device outside its authorization in the U.S.? *[MRVL]* *The Wi-Fi firmware has fixed FCC Region Code and accordingly the Wi-Fi firmware restricts the RF parameters to be FCC compliant. Any user attempts to operate outside the authorized range will be disqualified by Wi-Fi firmware and will not take effect on the Wi-Fi radio.*

Sincerely,

Kinoma Team
Marvell Semiconductor