Software security for UNII Devices

Vorwerk Elektrowerke GmbH & Co. KG

Mühlenweg 17-37

42270 Wuppertal

Germany

To Whom It May Concern:

Product/Model/HVIN: Thermomix TM6-5

FCC ID: 2AGELTM65

IC: 20889-TM65

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES acc. to KDB 594280

SOFTWARE CONFIGURATION DESCRIPTION	
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. [ALPS 2019/4/24] Wi-Fi driver and firmware are embedded in system firmware and there is not any installation process
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? [ALPS 2019/4/24] All default parameters approved by the FCC are programmed in both driver and firmware which would be embedded in system firmware. It cannot be accessed by third parties.
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. [ALPS 2019/4/24]

	All default parameters approved by the FCC are programmed in both driver and firmware which would be embedded in system firmware. It cannot be accessed by third parties.
4	Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware. [ALPS 2019/4/24] The Wi-Fi device needs specific driver and firmware to operate; the driver and firmware would recognize some IDs to confirm if the chip is correct. The driver would read the country code regulatory parameter to limit product to operate the device under its authorization in the U.S..
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? [ALPS 2019/4/24]. This module is used for client mode only in the market.
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. [ALPS 2019/4/24]. Third parties do not have capability to operate in any manner that will allow violation of the certification in the U.S. Frequencies, power, and other essential parameter regarding to regulatory domain is programmed into OTP memory at the factory.
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. [ALPS 2019/4/24]. Essential RF parameters regarding to regulatory domain is programmed into OTP memory at the factory and cannot be modified, reprogrammed or re-flashed by third parties.
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.

	[ALPS 2019/4/24]. RF parameters in firmware cannot be modified by host and/or driver software loaded in the host. Essential RF parameters cannot be modified because it is programmed in OTP memory and third party cannot access.
	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. [ALPS 2019/4/24]. User are not able to modify any content of Wi-Fi driver and its firmware because system firmware is programmed and protected in flash memory.
1.a	What parameters are viewable and configurable by different parties? [ALPS 2019/4/24]. User could select which Access Point to connect, and input password of Access Point for connection. Others, user are not able to access and modify any content because system firmware is programmed and protected in flash memory.
1.b	What parameters are accessible or modifiable by the professional installer or system integrators? [ALPS 2019/4/24]. None.
1.b(1)	Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized? [ALPS 2019/4/24] Yes. Some parameters are programmed in Wi-Fi driver and firmware which are embedded in system firmware, installer cannot access them. The system firmware is programmed and protected in flash memory. The professional installer/end-user cannot access the flash memory.
1.b(2)	What controls exist that the user cannot operate the device outside its authorization in the U.S.? [ALPS 2019/4/24] There is a country code regulatory parameter to limit user to operate the device outside its authorization in the U.S.
1.c	What parameters are accessible or modifiable by the end-user? [ALPS 2019/4/24]

	User could select which Access Point to connect, and input password of Access Point for connection
1.c(1)	Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized? [ALPS 2019/4/24] Some parameters are programmed in Wi-Fi driver and firmware which are embedded in system firmware, installer cannot access them. The system firmware is programmed and protected in flash memory. The professional installer/third parties cannot access the flash memory.
1.c(2)	What controls exist so that the user cannot operate the device outside its authorization in the U.S.? [ALPS 2019/4/24] There is a country code regulatory parameter to limit user to operate the device outside its authorization in the U.S.
1.d	Is the country code factory set? Can it be changed in the UI? [VE 2019/5/24] The country code will be factory set and can't be changed by the end customer. There will be still a dialog in the UI configuration dialogs of the device to select countries, but this will not impact the country code that is relevant for WiFi channel or RF parameters.
1.d(1)	If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.? [VE 2019/5/24] The country code will be factory set and can't be changed by the end customer.
1.e	What are the default parameters when the device is restarted? [VE 2019/5/25] The default parameter will be the factory set country code.
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. [ALPS 2019/4/24] No, there is no control to change between bridge and 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? [ALPS 2019/4/24] This is client device
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)) [ALPS 2019/4/24] This device is not an access point.

Thomas Schwätzler, technical approvals

Vorwerk Elektrowerke GmbH & Co. KG

Mühlenweg 17 – 37, 42270 Wuppertal, Germany

+49 202 564 3955