# Forced firmware lockdown?

Christian Scheele

cs@embedd.com

@ripe71 2015-11-16

# Short Information

FCC / ETSI intends to force router makers to lock down their devices to prevent users from changing RF settings to operate a device outside the allowed spectrum.

FCC affects only 5GHz Units

ETSI seem to affect ALL frequencies

Practically this leads to a complete firmware lock down preventing users from installing third party firmwares.

# USA FCC

- 2014, June 2: FCC up dated rules for U-NI I devices op erating under Part 15C
- 2015, June 1: stop approval of devices under the new rules
- 2015, August 16th: Deadline for accepting comments
- 2016, June 1: stop marketing under the old rules

FCC Document (as on November 12, 2015):

„SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES“

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.

2. Describe, if the device permits third - party software or firmware installation, what mechanisms are provided by the manufacture r to permit integrat ion 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 descri ption include what controls and/ or agreements are in place with providers of third - party functionality to ensure the d evices ' underlying RF parameters are unchanged and how the manufacturer verifies the functionality

3. For Certified Transmitter modular devices, describe how the module grantee ensures that host manufacture r s 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 .

Document link: http://shortlinks.de/24jc

Document available here:
https://ripe71.ripe.net/programme/meeting-plan/
plenary/

# European Union

DIRECTIVE 2014/53/EU becomes effective on 13. of June 2016

"on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/E"

Essential requirements

1. Radio equipment shall be constructed so as to ensure:

[...]

(i) radio equipment supports certain features in order to ensure that software can only be loaded into the radio equipment where the compliance of the combination of the radio equipment and software has been demonstrated.

Document link: http://shortlinks.de/j834

Document available here:
https://ripe71.ripe.net/programme/meeting-plan/plenary/

# Affected Devices

- WiFi Access points

Other devices which use WiFi and can use Access Point mode

- Smartphones
- Tablets

# Problems (incomplete list)

- Usually vendors only provide updates for a short time, so after a vendor stops shipping security updates the device becomes prone to attack

# Innovations

- Bufferbloat
- IPv6 development
- Open Mesh networks
- many more

# Discussion