

60001324104.txt

I'm a career professional in computer and network security and I strongly oppose the FCC plan to require access controls in FCC-certified wireless network devices that would prevent the installation and use of third-party and open-source firmware. My comment specifically is in regards to the rules in Part 15 that permit U-NII devices in the 5 GHz Band.

The weakest point in the security of small networks is often the commodity SOHO (small office / home office) router that has an unpatched security vulnerability in its firmware. Often these unpatched vulnerabilities persist even after they are publicized, because fixing security bugs is not profitable for the vendors, and these vendors abandon update support their products long before the end of their service life. Users **must** have the option of taking control of their security by installing a community-supported firmware such as DD-WRT.

This may not seem like a matter of national security, but it is that as well. Poorly secured default/stock firmware in commodity routers allows for a kind of Distributed Denial of Service attack (DDoS) in which routers improperly respond to spoofed requests, and an attacker can use many thousands of them to bounce high volumes of traffic at a target. This is currently a popular way to shut down internet sites and services in the commercial world and government.

Additionally, for the security and trust of our own networks, we must be able to verify the integrity and provenance of the firmware in our network devices. This can only be done with open-source software/firmware and open platforms.

So I ask you to reconsider the proposed requirement for security reasons, at least. There are many other valid reasons to oppose the requirement but I want to emphasize this one with my comment. I suggest perhaps narrowing the requirement to only apply to the subset of the firmware that controls RF transmission, if that was the actual intent.

Sincerely,
Michael Myers