Please Do Not Reply To This Email.

Public Comments on Equipment Authorizations:========

Title: Equipment Authorizations

FR Document Number: 2015-21634

RIN:

Publish Date: 9/1/2015 12:00:00 AM

Submitter Info:

First Name: Donald

Last Name: Plotz

Mailing Address: 3530 Forest Road

City: Bethel Park

Country: United States

State or Province: PA

ZIP/Postal Code: 15102

Email Address: don.plotz@gmail.com

Organization Name: Atos Corporation

Comment: I work in the IT industry, designing and building email systems for large companies. As such, I am quite cognizant of the need for security and particularly the need to patch security holes in a timely fashion. On my home network I use three consumer-class routers, two manufactured by Buffalo Corporation - WZR600DHP and WZR600DHP2, and one manufactured by Cisco/Linksys - WRT300N. Two of these are older routers, particularly the WRT300N. Cisco/Linksys does not provide updated firmware for this model, and third party firmwares such as DD-WRT fill the gap. In the case of the two Buffalo routers, which came with a version of DD-WRT, a critical vulnerability such as POODLE took more than 6 months to fix, while the open source community had it fixed in less than a week. I use features of the router which were vulnerable to this bug, and I'm sure I'm not the only one who does - it's one of the selling points of this router.

The requirement to prevent the installation of third party firmware on new routers will not only stifle new development - the fact that Buffalo routers ship with DD-WRT firmware proves that innovations

made by the open source community are frequently "mainstreamed" back into commercial firmware - but it will decrease the security of the Internet as a whole.

I work in the IT industry, designing and building email systems for large companies. As such, I am quite cognizant of the need for security and particularly the need to patch security holes in a timely fashion. On my home network I use three consumer-class routers, two manufactured by Buffalo Corporation - WZR600DHP and WZR600DHP2, and one manufactured by Cisco/Linksys - WRT300N. Two of these are older routers, particularly the WRT300N. Cisco/Linksys does not provide updated firmware for this model, and third party firmwares such as DD-WRT fill the gap. In the case of the two Buffalo routers, which came with a version of DD-WRT, a critical vulnerability such as POODLE took more than 6 months to fix, while the open source community had it fixed in less than a week. I use features of the router which were vulnerable to this bug, and I'm sure I'm not the only one who does - it's one of the selling points of this router.

The requirement to prevent the installation of third party firmware on new routers will not only stifle new development - the fact that Buffalo routers ship with DD-WRT firmware proves that innovations made by the open source community are frequently "mainstreamed" back into commercial firmware - but it will decrease the security of the Internet as a whole.