

# RE: Serious Security Issue in Windows XP SP2's Firewall

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2004-09/0166.html>

---

**From:** Langston, Fred (*flangston\_at\_verisign.com*)

**Date:** 09/26/04

To: "'Laura A. Robinson'" <laurarobinson@earthlink.net>, "'Thor'" <thor@hammerofgod.com>, focus-m  
Date: Sun, 26 Sep 2004 13:34:37 -0400

Hi All,

Let's see if we can reduce this problem. Is this the sequence of cause and effect described in the bulletin?

1. Start with XP SP1 with ICF off and ICS on (a home user using dialup and bridging to the rest of their home network comes to mind and is still common, I believe)
2. Upgrade to SP2
3. "As soon as you install SP2 on a Windows XP PC with a certain configuration, your file and printer sharing data are visible worldwide, despite an activated Firewall."

I think = Ports 137, 138,139, 445 are open and unfiltered on any interface, file and printer sharing is available for network login from any network (I guess)

4. "This also applies to all other services." Now, all ports and running services are available on all interfaces?
5. "The PC only has to provide sharing for an internal local network and connect to the Internet via dial-up or ISDN" Now, ICS is enabled?? On the dial-up of ISDN??? Or do they mean have file and print sharing enabled on an interface (trusted interface = internal)? Wha?
6. "Additionally, Internet Connection Sharing of the PC has to be disabled." OK, must mean no ICS.

So, without building a default XP build adding SP1 and then doing the above upgrade to verify, I think the bulletin is saying that SP2 upgrades with ICF off and ICS enabled, that this setup will not propagate a 'secure by default' configuration upon upgrade. Certainly, the configuration can easily be fixed and the risk mitigated, but unsophisticated users will never

SecurityFocus Microsoft: RE: Serious Security Issue in Windows XP SP2's Firewall

know to fix this on their own (or not 'secure by default').

To speculate, maybe the starting configuration, which bridges interfaces and therefore doesn't allow access control in the default MS implementation, has the interface objects in a state that passes object properties to all objects in the upgrade rather than just the SP2's expected object set.

Fred Langston, CISSP  
Principal Consultant  
VeriSign, Inc. Global Security Consulting  
M: 425.765.3330 O: 206.903.8147 x223

-----Original Message-----

From: Laura A. Robinson [mailto:laurarobinson@earthlink.net]  
Sent: Wednesday, September 22, 2004 5:14 PM  
To: 'Thor'; focus-ms@securityfocus.com  
Subject: RE: Serious Security Issue in Windows XP SP2's Firewall

Inline with snippage... (but in a nutshell, your instincts are correct, Tim)

> > *In other words, this caused the service to be released*  
> *worldwide through*  
> > *the dial-up connection as soon as you were connected to the*  
> *Internet.*

Um, what are these people smoking? They're saying that when you establish a point-to-point dial-up connection and have F&P Sharing enabled, you're somehow magically exposing your machine to the planet?? Am I misunderstanding their claim?

> > *Microsoft at that time issued an update to patch the bug.*  
> *The fact that*  
> > *file and printer sharing since then is not connected to the dial-up*  
> > *connection anymore, can easily be seen on your system:*  
> *Right-click on the*  
> > *symbol "My Network Places" and select "Properties". Repeat*  
> *the right-click*  
> > *and selection with the icon of your dial-up connection and*  
> *select the tab*  
> > *"Settings". If there is no check at "File and Printer Sharing", it*  
> > *indicates that this service should not be made available*  
> *through your*  
> > *dial-up connection.*

I cannot confirm or deny that this is a default setting as I have FPS disabled on all of my connections and do not recall what the default settings were.

> >  
> > *This in fact is true for Windows XP without Service Pack.*  
> *Since SP1, this*

RE: Serious Security Issue in Windows XP SP2's Firewall

## SecurityFocus Microsoft: RE: Serious Security Issue in Windows XP SP2's Firewall

> > *configuration is hardly more than cosmetics and does not  
> serve any purpose  
> > anymore. This means, the file and printer sharing service  
> > is connected in  
> > general, also to the dial-up network adapter.*

Okay, call me thick or confused, but what does this mean? What are they talking about— A dial-up adapter, or a network adapter? Is this a translation thing? I have absolutely no idea what the above is supposed to say.

>> *This in  
> itself is a serious  
> > bug, since your shared data potentially could be seen on  
> the Internet.*

Gee, now it's not "the world" and it's only "potentially"?

> > *However, there are no catastrophic effects, as every  
> dial-up connection is  
> > configured with an activated firewall by default.  
> >  
> > If you intended to deactivate this firewall, Windows  
> displayed an easily  
> > recognizable dialog, that this choice would allow access to  
> your computer.  
> > Despite the bug in SP1, the configuration of the firewall  
> was worked out  
> > in a clean way: You were able to run the dial-up connection with a  
> > firewall and the internal network card without, because the  
> latter was  
> > supposed to enable access through the Windows network.*

Okay, fine, whatever. I have some of my connections firewalled and others not. That didn't change with SP2.

> >  
> > *SP1 + SP2 leads to a catastrophic error  
> >  
> > Due to the bug carried over from SP1 as well as a new bug,  
> the firewall  
> > configuration with SP2 has a catastrophic effect. The SP2  
> installation  
> > simply uses the previous configuration of the firewall: If  
> it was active  
> > for the dial-up connection, now it also has been activated  
> for the network  
> > adapter.*

Are they talking about the enabling of the firewall? If so, they're wrong. Are they talking about the enabling of FPS system-wide? If so, they're

## SecurityFocus Microsoft: RE: Serious Security Issue in Windows XP SP2's Firewall

wrong. Are they saying that \*if\* a user, er, user were to do something like go and enable FPS on a dial-up connection but not on a LAN connection, that installing SP2 would then enable FPS on the network connection, as well? If so, I have no idea if it's true as I'd not do something like that. However, I see nothing on my system to indicate that this is true.

> >  
> > *At the same time, an exception is determined for file and printer sharing:*  
> > *For the internal network card – and astonishingly also for all adapters.*

Not on my machine. At all.

> >  
> > *With the first use of the dial-up connection after installing SP2, all of your shared data are available on the Internet.*

Okay, this is just a stupid statement.

> *Now, other users can start guessing your passwords for administrator and guest and you basically are no more secure than the first Windows 95 users with an Internet connection – thanks to Service Pack 2.*

See above.

> >  
> > *How to correct the problem*  
> >  
> > *It is not advisable to keep this defective default configuration. However, the previous environment cannot be restored: The configuration for the firewall was changed, which does not allow the setting of active or inactive conditions or exceptions for each network adapter anymore. Now this only works for network areas.*

BZZZZZZT! Wrong again, kiddies. They need to investigate the Advanced tab in the Windows firewall better. I just allowed 3389 on one and only one of my connectoids. In \*fact\*, on that Advanced tab, the very first chunk of text reads:

"Windows firewall is enabled for the selected connections below. To add exceptions for an individual connection, select it, and then click Settings."

## SecurityFocus Microsoft: RE: Serious Security Issue in Windows XP SP2's Firewall

You can even <gasp!> \*pre\*–set exceptions for connections on which the firewall is not currently enabled! Neat–OH!

> >  
> > *Choose "Windows Firewall" in the in the Windows Control  
> Panel and the  
> > there the tab "Exceptions". Select "File and Print  
> Services" and click on  
> > "Edit". Now you can see four ports which are used by the  
> file and print  
> > sharing service.*  
> >  
> > *To lock the service to the outside and keep it open for the  
> internal LAN,  
> > you have to individually select and change its area with  
> the respective  
> > button.*

And the point is?

> > *Our reader Yves Jerschov notified us of another  
> > bug: The value for  
> > the area set by default "Only for own network (Subnet)"  
> > only works, if the  
> > Internet Connection Sharing is activated.*

My apparently magic computer disagrees with Yves. I do not have ICS on any of my connections. I do, however, have "Only for own network (subnet)" available for each exception. I click the little radio button and SHAZAM! It works.

This is ridiculously easy to test. (even when it involves hobbling on crutches from one room to another– only for you, T., do I do these things. ;-))

1. Make sure that the XPSP2 box has Remote Desktop enabled.
2. In the Windows Firewall exceptions, ensure that your connection (I recommend having only one active connection during this testing for obvious reasons) allows Remote Desktop (TCP 3389) from "the world".
3. Go to a machine on another subnet and remote in to the XP box. Verify success.
4. Okay, now the fun part. Since you're already remoted into the XP box, change the firewall setting to (subnet) for TCP 3389.
5. Disconnect your session.
6. Attempt to reconnect. Oh, my goodness, it doesn't work anymore. Must be that there firewall thingie that don't werk unless you use ICS on one of your connections. Puhleeze.

> > *If this is not  
> > the case, your  
> > shared data are visible worldwide.*

SecurityFocus Microsoft: RE: Serious Security Issue in Windows XP SP2's Firewall

Aside from the fact that their premise is incorrect, this is not quite the case even if it *\*were\** correct.

- > > *This error can be*
- > *corrected by choosing*
- > > *"User defined List" and entering the IP addresses that are*
- > *supposed to*
- > > *have access – the IP addresses of your LAN. A whole range*
- > *of an IP area*
- > > *can be entered as "192.168.x.0/255.255.255.0", if the*
- > *respective addresses*
- > > *start with 192.168.x.*

See above.

- > >
- > > *After these measures, you can be sure to be as safe as you*
- > *were with SP1.*
- > > *Great, don't you think?*

I think I'd really like to know what these guys consider a testing methodology.

I call bullpucky.

Laura

---

---

---

---