

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

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2004-09/0150.html>

From: Thor (*thor_at_hammerofgod.com*)

Date: 09/23/04

To: "Jens Mickerts" <jens@mickerts-partner.de>, <focus-ms@securityfocus.com>

Date: Thu, 23 Sep 2004 01:46:31 -0700

I have tested this many times, and cannot reproduce the behavior described here— I've gone out of my way to try to make this happen, and can't. I'm no guru, but I would hope that if this was possible, I'd be able to make it happen. Please give us detailed instructions that we can reproduce.

T

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

From: "Jens Mickerts" <jens@mickerts-partner.de>

To: "Thor" <thor@hammerofgod.com>; <focus-ms@securityfocus.com>

Sent: Wednesday, September 22, 2004 11:47 PM

Subject: AW: Serious Security Issue in Windows XP SP2's Firewall

Hi,

the report is correct. If you update a WinXP SP-1 with enabled Internet Connection Firewall (enabled for a single dial-up connection is sufficient) and no internet connection sharing enabled (I do not know what the heck is different with ICS enabled), the File and Print Sharing will be world visible on any interface after applying SP-2 and enabling the Firewall!

If there is no ICF enabled before upgrade things seem to work fine, if ICS is enabled before the upgrade things also work fine.

This is very strange and dangerous indeed.

Regards,

Jens

-----Ursprüngliche Nachricht-----

Von: Thor [mailto:thor@hammerofgod.com]

Gesendet: Dienstag, 21. September 2004 21:56

An: focus-ms@securityfocus.com

Betreff: Fw: Serious Security Issue in Windows XP SP2's Firewall

This article in pc-welt was brought to my attention yesterday, and I just

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

have no idea what they are talking about. It is like the entire piece is totally bogus— has anyone seen anything about this?

T

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

From: "Andreas Marx" <amarx@gega-it.de>

To: <bugtraq@securityfocus.com>

Sent: Sunday, September 19, 2004 2:23 AM

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

> Hello,

>

> *this might be interesting for you (see below): Please note that all
> screenshots and more details can be found in the German article only (see
> links), the English one is slightly shortened.*

>

> *cheers,*

> *Andreas Marx*

>

>

> *PC-WELT discovers and fixes serious security issue in Windows XP SP2
> by Andreas Kroschel and Thorsten Eggeling; Sep 15, 2004*

>

> *English version: <<http://www.pcwelt.de/know-how/extras/103039/>>*

> *German version: <<http://www.pcwelt.de/news/sicherheit/103013/>>*

>

>

> *Windows XP Service Pack 2 with Advanced Security Technologies helps you
> protect your PC against viruses, hackers, and worms." – this is how
> Microsoft promotes its Service Pack 2 on its website. What the company
> does not say: Instead of viruses, worms, and hackers, the supposedly safe
> SP2 for Windows XP invites any Internet user to have a look around your
> PC.*

>

> *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. This also applies to all other services.
> The PC only has to provide sharing for an internal local network and
> connect to the Internet via dial-up or ISDN. Users of DSL services are
> also affected, if a firewall is not integrated into the DSL modem or a
> common modem instead of a DSL router is used. Additionally, Internet
> Connection Sharing of the PC has to be disabled.*

>

> *A number of test scans run by PC-Welt revealed that this in fact is a
> common configuration and not a rare sight. Without great effort, we were
> able to discover private documents on easily accessible computers on the
> Internet. It must be assumed, that these users wrongly believe they are
> safe and that their sharing configurations are only visible in their
> network at home: Often, we did not even encounter password protection.*

>

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

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

- > *Already Windows 95 affected by a similar problem*
- >
- > *Experienced Windows users may remember that there was a similar problem in*
- > *the past, specifically with Windows 95. Back then, Microsoft forgot to*
- > *separate file and printer sharing from the dial-up network adapter when*
- > *such a connection was configured.*
- >
- > *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.*
- > *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.*
- >
- > *This in fact is true for Windows XP without Service Pack. Since SP1, this*
- > *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. This in itself is a serious*
- > *bug, since your shared data potentially could be seen on the Internet.*
- > *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.*
- >
- > *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.*
- >
- > *At the same time, an exception is determined for file and printer sharing:*
- > *For the internal network card – and astonishingly also for all adapters.*
- >
- > *With the first use of the dial-up connection after installing SP2, all of*
- > *your shared data are available on the Internet. 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.*
- >
- > *How to correct the problem*

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

- >
- > *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.*
- >
- > *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. 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. If this is not the case, your*
- > *shared data are visible worldwide. 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.*
- >
- > *After these measures, you can be sure to be as safe as you were with SPI.*
- > *Great, don't you think?*
- > --
- > *AV-Test GmbH, Klewitzstr. 7, 39112 Magdeburg, Germany*
- > *Phone: +49 (0)391 6075466, <<http://www.av-test.org>>*
- >
- >
- >
