

Re: Big hole??

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-09/23769.html>

From: Testy (*fraudbuster_at_canoemail.com*)

Date: 09/19/04

Date: Sun, 19 Sep 2004 08:45:03 -0400

Typical knee-jerk reaction here. You know "shoot the messenger"

Testy

"Jeff" <jeff@phony.com> wrote in message

news:%235LWgVknEHA.4056@TK2MSFTNGP09.phx.gbl...

> *I'm no expert, but it seems to me all the responses here seem to be
> attacking the sender instead of refuting the facts of what he is claiming.
> Not helpful to the rest of us.*

>

> --

>

> *Jeff Williams*

> *Email address deliberately false to avoid spam*

> *jeff@phony.com*

>

>

> *"Jone Doe" <fake@nowhere.org> wrote in message*

> *news:%23k%23bhzhnEHA.3712@TK2MSFTNGP15.phx.gbl...*

> **sniff* I smell a troll.*

> *"User1" <user1@msn.net> wrote in message*

> *news:%2306crwfnEHA.608@TK2MSFTNGP09.phx.gbl...*

> *Ya - I do. What's the point?*

> *"OMG!!" <anonymous@discussions.microsoft.com> wrote in message*

> *news:15a201c49dfa\$5d3696e0\$a501280a@phx.gbl...*

> *Uh, do you run a firewall? If so then what are ya worried*

> *about. Have your provider ping you, if they see a*

> *firewall then even they can't get in, that plus the added*

> *protection from Microsoft kinda makes you pretty*

> *invulnerable*

>>-----Original Message-----

>>*"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*

Re: Big hole??

> 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.
>>
>>
>>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*

>>

>>

>>*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?*

>>

>

>

> ---

> *Outgoing mail is certified Virus Free.
> Checked by AVG anti-virus system (<http://www.grisoft.com>).
> Version: 6.0.766 / Virus Database: 513 – Release Date: 9/17/2004*

>

>