

Re: Big hole??

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.basics/2004-09/3324.html>

From: David H. Lipman (*DLipman~nospam~_at_Verizon.Net*)

Date: 09/19/04

Date: Sun, 19 Sep 2004 11:17:27 -0400

Think what you want.

That ***IS*** my name and those who know me know I don't steer people wrong. I do make mistakes, and I'll admit it, but I don't deliberately mislead.

Dave

"Ted Grumbull" <pappy73@email.com> wrote in message
news:ek6rk0djgq0vlbn7e41i2888s8788bmnvi@4ax.com...

| On Sat, 18 Sep 2004 22:42:34 -0400, "David H. Lipman"
| <DLipman~nospam~@Verizon.Net> wrote:

|
|>Care to corroborate that info with a URL from a LEGITIMATE CERT or Security Organization
|?

|>

|>So far this information remains uncorroborated !

|>

|>But what do you expect from an anonymous poster posting in HTML.

|>

|>Dave

|>

|>

|>

|

|

| Yeah, and we *****ALL***** know your name really is "David H. Lipman",
| because this is USENET and you say so.....

|

|>

|>

|>"User1" <user1@msn.net> wrote in message news:uwD88BfnEHA.392@tk2msftngp13.phx.gbl...

|>"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.

|>

microsoft.public.windowsxp.basics: Re: Big hole??

|>
|>
|>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

Re: Big hole??

microsoft.public.windowsxp.basics: Re: Big hole??

|>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.

Re: Big hole??

microsoft.public.windowsxp.basics: Re: Big hole??

|>

|>

|>

|>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 SP1. Great, don't
you

|>think?

|>

|