

Re: Microsoft FTP Server problem on W2K?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2003-12/0363.html>

From: Pete Hornby (*peter.hornby_at_unisys.com*)

Date: 12/13/03

Date: Fri, 12 Dec 2003 16:44:23 -0800

"Alun Jones [MS MVP]" <alun@taxis.com> wrote in message
news:sLpCb.789\$UI.289@newssvr22.news.prodigy.com...

> *In article <O2PGLCNwDHA.2000@TK2MSFTNGP11.phx.gbl>, "DavidM"*

> *<scandal_123@cox.net> wrote:*

<<snip>>

I have technical responsibility for this FTP implementation, and I need to make some comments on what you said here. Neither here, nor in the responses quoted by David, am I trying to say that "we're right, and they're wrong". I would make the point that it's not a cut-and-dried decision, and there are arguments on both sides.

> >2. *The FTP standard (RFC 1123 section 4.1.2.12) states that, on a*
> >*multi-homed server, the data connection MUST use the same IP*
> >*address as the control connection. It is not, however, required that*
> >*the client-side data connection use the same IP address as the*
> >*client-side control connection. In fact, it's not even necessary,*
> >*according to RFC 959, that the client ends of the two connections*
> >*be in the same machine. See RFC 959 section 2.3.*

>

> *Ah, but section 3.3 of RFC 959 says that there is a default port,*
> *client-side, that must be used unless the PORT command is used to*
> *negotiate a different one. Since PASV voids PORT, the client side*
> *must use the default port (and hence, the IP address that it used to*
> *connect to the server from). As it turns out, few clients do this, but*
> *all clients should use the same IP address.*

Right. Section 3.3 tells us that the client side must use the default port, U. It says nothing about the IP address. It seems to me that your parenthetical comment "and hence, the IP address that it used to connect to the server from" isn't implied by the text of the RFC. It may be that your experience as an implementer tells you that that's what the world does, and I wouldn't argue with that, but it's not what the RFC says.

> *Also, check out section 4 of RFC 2577, "FTP Security*

- > *Considerations" – essentially, your vendor is saying that there is a*
- > *random chance that their client won't work when connecting to a*
- > *server that chooses to check for the same IP address in control*
- > *and data connections.*

RFC 2577 says that the server may find it "desirable to restrict access based on network address", citing an example of a server which might want to "restrict access to certain files from certain places". Maybe I'm wrong, but it doesn't seem to me that that's what's going on here.

<<snip>>

- > *>In PASV mode, where the data connection establishment is FROM*
- > *>client TOver, our client allows TCP/IP to assign the IP address*
- > *>of the data connection. It is possible that this could be different*
- > *>from the IP address of the control connection.*
- >
- > *This is bogus. It takes what, two, three lines of code to call*
- getsockname*
- > *and bind? The IP address used to connect to the PASV socket should*
- > *be the same as used to connect to the control connection, if it comes*
- > *from the same machine. Otherwise, the server is free to decide that "this*
- > *is not the same client", and reject the attempt to hijack the port.*

The server is free to make any decision it wants. It can do what RFC 2577 seems to suggest, which is to make some sensible configuration decisions based on knowledge of the environment in which it operates. Or it can unconditionally make the decision made by the server in use at David's site. In the case he's discussing, the two IP addresses were not only in the same network, they were in the same system. I might argue, but probably won't, that this is throwing the baby out with the bathwater.

<<snip>>

- > *>We still believe the problem is on the remote FTP server side.*
- >
- > *Bull–pucky. The FTP server is behaving slightly more securely than*
- > *RFC 959 / 1123 dictates, in a manner compliant with RFC 2577. The*
- > *FTP client is behaving like its programmers have got their heads up their*
- > *collective arses and haven't been aware of the last decade's developments*
- > *in FTP.*

We shouldn't have said this. The overall intent of the response was not to suggest that this was a problem and that it was someone else's – although I admit that this was what ended up being said. It isn't a cut-and-dried issue, and drawing inferences about the location of my head won't make it so. You yourself have said (excerpting from <http://www.securityfocus.com/archive/1/4.3.2.7.2.20021025120751.01f12818@208.55.91.110/2002-10-20/2002-10-26/0>)

>>>

The best that a server can do against PASV hijacking is to improve the

randomness of its choice of ports, and to close all connections other than the first received on the incoming port. It might also care to verify that the source address matches that of the client, but that, too, is somewhat a matter of taste.

>>>

> >Can someone please tell me what the correct answer is. I would imagine that

> >the FTP server cannot accept passive connections from two different IP
> >addresses. Otherwise, FTP transmissions would be failing for no apparent
> >reasons due to port scans, hackers, etc.

>

> The FTP server *could*, if it wanted to, accept connections to PASV
> listeners from any old IP address. But, this would open your server up to
> port hijacking attacks. See RFC 2577. This FTP server is configured or
> programmed to prevent such attacks by requiring that both control and data
> connections must come from the same port.

These weren't "any old IP addresses". These were two IP addresses on the same machine.

> This

is how our own FTP servers,

> WFTPD and WFTPD Pro, are configured by default, and it's a recommendation
> of RFC 2577, which only covers the most basic and vital of security
> considerations. [Its only concession to encryption, for instance, is to
> state "To guarantee the privacy of the information FTP transmits, a strong
> encryption scheme should be used whenever possible."]

>

> The client, and its vendor, are being stubborn-headed in insisting that
> they're RFC compliant. For that matter, so's a brick - it refuses all
> access. That doesn't make it useful. Your vendor doesn't want to add the
> few lines that it takes to make their client more useful in the days of an
> unsecured Internet. Dump your client vendor and go with one that gives
even

> the slightest damn about security.

>

> >Any comments, feedback, etc. appreciated.

>

> I like RFC 2577. It has my name in it.

Splendid.

Look, I don't mind changing this. It's a single line of code. Truth be told, I'm not entirely sure why we did it the way we did in the first place. I'm sympathetic to the issue faced by David, and those you talk about in your response. I just wanted to point out that there are things to be said on both sides. And I'm persuaded.

microsoft.public.inetsrvr.iis.security: Re: Microsoft FTP Server problem on W2K?

One more thing. David didn't point out that our client does allow you to force the two client-side IP addresses to be the same. He has verified that this works.

Enough. I'll cut a fix.

Peter Hornby
Unisys Corporation
Mission Viejo/CA