

Re: Microsoft FTP Server problem on W2K?

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2003-12/0348.html>

From: DavidM (*scandal_123_at_cox.net*)

Date: 12/12/03

Date: Fri, 12 Dec 2003 11:27:37 -0600

Please note that both the Mainframe and Microsoft FTP Server is on same subnet.

--

...david

<http://www.micro-mess.com>

<http://www.va-mustang.com>

If you wish to reply to me personally, please remove the "underline" from scandal_123@cox.net. The is done to avoid SPAM!

"DavidM" <scandal_123@cox.net> wrote in message

news:O2PGLCNwDHA.2000@TK2MSFTNGP11.phx.gbl...

> We have a mainframe at work that FTPs file to a Microsoft W2K FTP server
> using SP4. Since the mainframe appears to be bogged down at times and
> doesn't seem to respond to FTP requests on its server nor respond quickly
> enough when it sends files out, I made a request to have all outgoing FTP
> files coming from mainframe to use PASSIVE instead of ACTIVE. This way,
> Microsoft FTP server can create both teh control and data ports for the
> connection; rather than requiring the mainframe to create the data port.

>

> As a result, things hit the fan.

>

> After myself and another technical engineer reviewed the network analysis,
> it was determined that since the mainframe was multi-home and performing
> load balancing across two network cards, the following was happening:

>

> 1) Mainframe would FTP from 10.246.1.12 to FTP server to port 21 (control
> connection).

> 2) Mainframe would sign in to FTP server and then issue the PASV command

> 3) Mainframe would then try to connect from 10.246.1.11 to FTP server on
> port 20 (data connection).

> 4) Microsoft FTP server reports error #426 and drops the connection.

> 5) Mainframe also drops connection after successive "I/O" errors trying to
> send the STORE command.

>

> The below excerpts are what the mainframe vendor is telling us:

>

> Email #1 from us to vendor:

> The windows FTP server does not like the mainframe sending packets from
> multiple IP addresses. When we restricted the packets to come from only
> one

> IP address, passive mode worked.

>

> So the question is, should packets be allowed to come from multiple IP
> addresses when using Passive Mode. Bug or feature. A good question for
> engineering. Can you follow up on this??

>

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

> Email #2 from vendor to us:
>
> The following is from engineering:
> 1. Any given FTP connection - in fact, any TCP/IP connection - will
involve
> packets being sent from a single IP address and to a single IP address.
The
> TCP/IP connection is identified by source and destination port numbers and
> source and destination IP addresses.
>
> 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.
>
> 3. The mainframe FTP behaves in this way:
>
> In PORT mode, where the data connection establishment is FROM server TO
> client, our client establishes the data connection from the same IP
address
> as the data connection.
>
> In PASV mode, where the data connection establishment is FROM client TO
> server, 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.
>
> I would still like to see FTP diagnostics. If the customer's analysis is
> correct, TCP/IP tracing isn't required at this stage.
>
> Email #3 from vendor to us:
>
> The following is the result of the analysis of the information you
provided:
> We analyzed the trace that was provided and it shows, we initiated the
> control connection from 10.246.1.12, and the data connection from
> 10.246.1.11. The data connection opened successfully, which suggests that
> the remote FTP server was, at least at a TCP level, prepared to accept the
> connection initiation from the second IP address. The server returned a
426
> error response when we sent the STOR command over the control connection,
> and immediately closed the data connection.
>
> As I said previously, I believe that the behavior of our client is in
> accordance with the FTP protocol standard.
>
> We still believe the problem is on the remote FTP server side.
>
> ---
>
> 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.

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

>
> Any comments, feedback, etc. appreciated.
>
> Perhaps THIS IS A Microsoft bug???
>
>
> --
> ...david
> <http://www.micro-mess.com>
> <http://www.va-mustang.com>
> If you wish to reply to me personally, please remove
> the "underline" from scandal_123@cox.net. The is done to avoid SPAM!
>
>