

Re: How is dangerous connect to server over internet with remote d

Re: How is dangerous connect to server over internet with remote d

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-08/msg00039.html>

- *From:* "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx>
 - *Date:* Sat, 22 Jul 2006 10:38:57 -0700
-

There is or was also a man in the middle vulnerability, at least if it has not yet been fixed (and I have not noticed MS mentioning this). The XP SP2 era changes raised the bar on this but did not eliminate all possibilities.

Note however that a man in the middle attack is not the most simple thing to accomplish, depending on network topologies, so the poster should probably not be too concerned if their server is not a high profile site and they can trust their provider/collocation.

ref:

www.oxid.it/downloads/rdp-gbu.pdf

www.networksecurityarchive.org/html/Exploits-HackingTools/2005-06/msg00002.html

"Miha Pihler [MVP]" <mihap-news@xxxxxxxxxxxx> wrote in message news:uZPeoVNrGHA.4864@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hi,

I did a search and I found one DoS vulnerability from the past:

Microsoft Security Advisory (904797)

Vulnerability in Remote Desktop Protocol (RDP) Could Lead to Denial of Service

<http://www.microsoft.com/technet/security/advisory/904797.msp>

—

Mike

Microsoft MVP – Windows Security

"Miha Pihler [MVP]" <mihap-news@xxxxxxxxxxxx> wrote in message news:ehewxSNrGHA.2464@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hi,

I can't recall any critical vulnerabilities in the past in Terminal Services. I consider it a very good solution for remote access and administration even without IP filtering. As mentioned the only concern

Re: How is dangerous connect to server over internet with remote d
is how strong and protected your passwords are.

--

Mike
Microsoft MVP – Windows Security

"Massimo" <Massimo@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:AC61C683-818C-4FEF-A912-73767BB69894@xxxxxxxxxxxxxxxxxxxx

Thank'you very much for you answer. I want know if there
are in the
past..
bug or vulenability in the terminal service (remote desktop).
If i use
encryption and if i connect to server with the same ip (i
configure
firewall
to accept only my remote fixed ip for 3389 port) can i
consider this
solution
a good solution for manage the server?

"Miha Pihler [MVP]" wrote:

Hi,

There are few things you can do to make
these connections (more)
secure:
– On the server set the encryption to high
– On Windows Server 2003 with SP1
installed on it you can use
certificates
to prevent MITM (Man In The Middle)
attacks.

Now the only thing that I usually worry
about when considering RDP are
key
loggers that might be installed on a computer
from which you are trying
to
connect to your server (e.g. if you are trying
to connect to your
server
from cyber café). Still this is not only the
problem with RDP
connection but
with any remote connection using static
username and password.

Re: How is dangerous connect to server over internet with remote d

So if you decide for this option pay attention to username and password (use strong username and password and change passwords frequently). Don't use domain administrator account for connection – use ordinary user account. Whenever possible this user account should not even be local administrator on the server. Once you are connected to the server you can raise your permissions using another RDP to the server or options such as "run as" etc.

Another thing to consider is to limit IP address from which you can connect to your server over RDP (e.g. limit it to your home IP address only).

--
Mike
Microsoft MVP – Windows Security

"Massimo"
<Massimo@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote in message
news:0E85C1B9-1460-4EF8-8EFC-7FF4FD983C45@xxxxxxxxxxxxxxxxxxxx

I have installed windows server 2003 enterprise edition. I have to manage my server from remote site. A solution with remote desktop only is very dangerous? Terminal service of windows server 2003 with encryption is not secure?

Thank's

Re: How is dangerous connect to server over internet with remote d