

Re: TS/3389 risk on Internet

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2004-11/0022.html>

From: Tim (tim-pentest_at_sentinelchicken.org)

Date: 11/02/04

Date: Mon, 1 Nov 2004 22:43:03 -0500

To: "Peadro, Jeff (AIS)" <jpeaa@allstate.com>

- > *If you choose to do this you need to enable high encryption which uses*
- > *128 bit and change the port TS listens on.*
- > <http://support.microsoft.com/default.aspx?scid=187623>

I think the originator of this thread is aware of this problem, but based on many of the other posts, it appears others aren't, so I'll post it here:

<http://seclists.org/lists/bugtraq/2003/Apr/0038.html>

AFAIK, M\$ has changed nothing to fix this major design flaw. My point here is, no amount of encryption will do any good if you aren't authenticating who you are sending it to, as a client. If you can masquerade as the server, then you should be able to inject your own session keys, and read any data coming from the client, which would include any login passwords.

(If there have been any recent changes by M\$ in newer versions which correct this, please, do tell.)

Come to think of it, perhaps using an alternative client (rdesktop?) one could authenticate and store server keys/fingerprints, fixing this user-interface flaw. I haven't touched Windoze in a while, does anyone know if this feature is available in alternative clients?

thanks,
tim