

Re: shared folders

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2004-11/0310.html>

From: Christo (*chris_at_juststuff.co.uk*)

Date: 11/14/04

Date: Sun, 14 Nov 2004 13:38:37 -0000

"Thore "Tocis" Schmechtig" <MAILTO:commoner@carcosa.de> wrote in message news:2vogiqF2j3t81U1@uni-berlin.de...

> *Christo wrote:*

>

>> *are these security holes, specifically the Remote admin*

>

> *These are builtin M\$ features to help the spread of malware. ;)*

>

> *Honestly:*

>

> *They are called administrative shares and are meant for the administrators*

> *of large networks to ease their work. To access them you need the*

> *machine's*

> *admin password, so if you have a good, strong one you aren't in too much*

> *danger. All those who think that admin passwords are for wimps, however,*

> *are in for a nasty surprise sooner or later.*

> *Yes they can be disabled via a certain registry key that, IIRC, you have*

> *to*

> *create yourself (it's not there by default). Unfortunately I can't tell*

> *you*

> *right away what this key is because I largely moved to SuSE Linux months*

> *ago, only starting M\$ for games and some very special multimedia apps.*

>

> *Ah, wait, I may still have the batch file here, accessible from Linux...*

>

> *(digs through his XP partition)*

>

> *...there it is. On my XP pro system, the following worked:*

>

>

>

> *in the registry branch*

>

> *HKLM\system\currentcontrolset\services\lanmanserver\parameters*

>

> *create a new DWORD key named*

>

> *autosharewks*
>
> *and give it the value 0.*
>
>
>
> *That should disable those admin shares at next reboot at the latest,*
> *though*
> *I'm not perfectly sure if IPC\$ will be affected too – it may be too*
> *important for the system as a whole to be switched off. But ADMIN\$ and the*
> *drive shares should be gone.*
>
> *You need admin privileges for that of course, so either start your regedit*
> *with "Run as..." or login as admin to do it. And if you haven't already*
> *done so, PLEASE do yourself the favor and assign a strong password to the*
> *admin account – one that can't be guessed by a dictionary attack. :)*
>
> *Hope to have helped...*
>
> --
> *Regards*
>
> *Thore "Tocis" Schmechtig*

read a bit more and found that AutoShareServer at 0 may also work