

Re: Administrator rights for legacy appliations

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.terminal_services/2004-08/0256.html

From: Vera Noest [MVP] (vera.noest_at_remove-this.hem.utfors.se)

Date: 08/05/04

Date: Thu, 05 Aug 2004 14:54:27 -0700

It's not a question of highly skilled, malicious users, just innocent users running workstation applications and browsing the Internet and your filesystem.

Look at it this way: your users are all working interactively on your Domain Controller. They will surf to all kinds of malicious websites, try to download software, etc.

They will need quite some permissions to be able to run applications at all, even if you try to lock them down as best as you can.

Another problem is that a lot of applications are not 100% TS-compatible and can cause various problems on your server. If your TS hangs because of such an application, your whole DC is down as well, meaning all non-TS users are also affected.

And then there's the performance impact: when you install Terminal Services, the internal tuning of the OS changes quite a bit. If the same server also is a DC, running AD, DNS and maybe more, you could create a serious performance problem.

--
Vera Noest
MCSE, CCEA, Microsoft MVP – Terminal Server
<http://hem.fyrlistorg.com/vera/IT>
--- please respond in newsgroup, NOT by private email ---

"Graham Taylor" <gt2002@freeuk.com> wrote in
news:#sQkKzYeEHA.3028@TK2MSFTNGP12.phx.gbl:

- >
- > *Are there any links or info as to why having a DC as a multiple*
- > *user workstation is a security risk?*
- >
- > *Would the users in question need some MS networking experience*
- > *to take advantage of the situation or is it a differnet kind of*
- > *exploit vulnerability?*

>
> *Regards*
> *Graham*
>
> *"Vera Noest [MVP]" <vera.noest@remove-this.hem.utfors.se> wrote*
> *in message*
> *news:Xns953CDEA9D4C95veranoesthemutforsse@207.46.248.16...*
>> *I would download FileMon and RegMon from*
>> *<http://www.sysinternals.com/>. Run them as administrator, start*
>> *a TS session as a normal user and try to run the application.*
>>
>> *FileMon and RegMon will show you all "access denied" errors*
>> *that occur, so that you can give your users the necessary*
>> *permissions on a file-to file or Registry subkey basis.*
>>
>> *Even if you manage to have users run the application without*
>> *making them Administrators, you still have a security problem,*
>> *since you actually are using your DC as a multiple-user*
>> *workstation. I would try to purchase a second server as soon as*
>> *possible, and make that a dedicated TS (as a member server in*
>> *your domain).*
>>
>> --
>> *Vera Noest*
>> *MCSE, CCEA, Microsoft MVP – Terminal Server*
>> *<http://hem.fyristorg.com/vera/IT>*
>> *--- please respond in newsgroup, NOT by private email ---*
>>
>> *"Will G" <wgrever@crcm.edu> wrote in*
>> *news:#pssRcveEHA.708@TK2MSFTNGP09.phx.gbl:*
>>
>>> *I am running W2K3 standard server with Terminal Services in*
>>> *application mode and this box is the only server in the*
>>> *forest / domain / enterprise (my AD lingo is not what it*
>>> *should be) any way, it is the only server so it is also the*
>>> *one and only domain controller.*
>>>
>>> *My problem is that I have several applications on the*
>>> *server that require*
>>> *the user to have admin rights in order for the application to*
>>> *function properly. I do not want to give full admin right to*
>>> *the users when they log on to a TS session to run these*
>>> *applications, but I have been unable to come up with any*
>>> *other solution. My impression is that these applications are*
>>> *doing something in the registry, but I am not sure.*
>>>
>>> *Is there a way to have a TS session with the user having*
>>> *Administrator*
>>> *rights of the session but not local Admin rights on the*
>>> *server itself? And would this solve my problem?*
>>>

microsoft.public.windows.terminal_services: Re: Administrator rights for legacy applications

>> > *Thank you,*

>> > *Technet alias: wgrever@crcm.edu*