Patch Windows 2003 Terminal Server to allow more than 2 concurrent sessions

WP1 SAT

As you might know Windows 2003 Server accepts at most 2 concurrent Terminal Server sessions (and 1 console session) in Remote Administration mode (which is the default). Of course if you switch to Application Mode you can have an unlimited number of sessions but this requires licenses and a license server.

When Terminal Server creates a new session it checks if the new session is either a console session or a help assistant session and if not it allocates a license. The function that performs this check is called CRAPolicy::Logon

```
.text:7656B494
.text:7656B494 ; =============== S U B R O U T I N E ==============================
.text:7656B494
.text:7656B494 ; Attributes: bp-based frame
.text:7656B494
.text:7656B494 ; public: virtual long __thiscall CRAPolicy::Logon(class CSession &)
.text:7656B494 ?Logon@CRAPolicy@@UAEJAAVCSession@@@Z proc near ; DATA XREF: .text:7
.text:7656B494
.text:7656B494 arg_0 = dword ptr 8
.text:7656B494
.text:7656B494 mov edi, edi
.text:7656B496 push ebp
.text:7656B497 mov ebp, esp
.text:7656B499 push esi
.text:7656B49A mov esi, [ebp+arg_0]
.text:7656B49D push edi
.text:7656B49E mov edi, ecx
.text:7656B4A0 mov ecx, esi
.text:7656B4A2 call ?IsSessionZero@CSession@@QBEEXZ ; CSession::IsSessionZero(void)
.text:7656B4A7 test al, al
.text:7656B4A9 jnz short loc_7656B4C2
.text:7656B4AB push 0
.text:7656B4AD push dword ptr [esi]
.text:7656B4AF call _TSIsSessionHelpSession@8 ; TSIsSessionHelpSession(x,x)
.text:7656B4B4 test eax, eax
.text:7656B4B6 jnz short loc_7656B4C2
.text:7656B4B8 push esi
.text:7656B4B9 mov ecx, edi
.text:7656B4BB call ?UseLicense@CRAPolicy@@AAEJAAVCSession@@@Z ; CRAPolicy::UseLice
.text:7656B4C0 jmp short loc_7656B4C4
.text:7656B4C2 ; ---------------------------
.text:7656B4C2
.text:7656B4C2 loc_7656B4C2: ; CODE XREF: CRAPolicy::Logon(CSession &)+15j
.text:7656B4C2 ; CRAPolicy::Logon(CSession &)+22j
.text:7656B4C2 xor eax, eax
```

```
.text:7656B4C4
.text:7656B4C4 loc_7656B4C4: ; CODE XREF: CRAPolicy::Logon(CSession &)+2Cj
.text:7656B4C4 pop edi
.text:7656B4C5 pop esi
.text:7656B4C6 pop ebp
.text:7656B4C7 retn 4
.text:7656B4C7 ?Logon@CRAPolicy@@UAEJAAVCSession@@@Z endp

So if we want to bypass this license allocation we simple change it to:

.text:7656B494 ; public: virtual long __thiscall CRAPolicy::Logon(class CSession &)
.text:7656B494 ?Logon@CRAPolicy@@UAEJAAVCSession@@@Z proc near ; DATA XREF: .text:7
.text:7656B494 xor eax, eax
.text:7656B496 retn 4
.text:7656B496 ?Logon@CRAPolicy@@UAEJAAVCSession@@@Z endp
```

the binary diff is:

```
0002A894: 8B 31
0002A895: FF C0
0002A896: 55 C2
0002A897: 8B 04
0002A898: EC 00
```

If you are going to replace termsrv.dll please note that it's protected by Windows File Protection so you need to replace it in the following order:

- Replace termsrv.dll in c:\windows\system32\dllcache
- If you have the installation cd/dvd (i386) folder copied to your harddrive replace (use the compress command) or remove it there as well
- Now rename the original file in your system32 folder and place the patched version
- Reboot

VPatch file: Windows Server 2003 VPatch file (2003tspatch.zip) (of termsrv.dll build 5.2.3790.3959 English language)

How to use the pat file:

1. install v-patch: vpatch32.zip
2. from the vpatch directory launch vpatchprompt.exe
3. vpatchprompt will ask you for the following files:
   – Patch file (the .pat file).
   – Source file (termsrv.dll).
   – Destination file (the patched termsrv.dll).
4. now replace termsrv.dll as instructed in the post & reboot