

Internal security problem with RPCSS

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2005-07/0955.html

From: needlove (*needlove_at_aw.ave*)

Date: 07/18/05

Date: Sun, 17 Jul 2005 22:17:10 -0600

My computer is not part of a network! I am the ADMINISTRATOR. I installed Windows XP home sp1 OEM CD I got off ebay. I installed it on a WD raptor serial ATA hard drive using an ATA CD drive and installed the unsigned Sil3112 SATA drivers when prompted. I installed SP2 before accessing the internet to download the latest updates. The repair installations, one from the recovery console, one from an active windows session, were done using a "slipstream CD" (merging sp2 with my original sp1 version).

This is my sceRoot log for all installations:

Saturday, February 19, 2005 9:29:26 PM

C:\ is a NTFS volume.

Security for C:\ is not changed because it is not the default set by Windows. The current security is

D:(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICIIO;GA;;;CO)(A;OICI;0x1200a9;;;BU)(A;CI;LC;;;BU)(A;CIIO;DC;;;E

First attempted repair!

Thursday, July 07, 2005 2:36:55 PM

C:\ is a NTFS volume.

Security for C:\ is not changed because it is not the default set by Windows. The current security is

D:(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICIIO;GA;;;CO)(A;OICI;0x1200a9;;;BU)(A;CI;LC;;;BU)(A;CIIO;DC;;;E

Second attempted repair!

Sunday, July 17, 2005 5:51:32 PM

C:\ is a NTFS volume.

Security for C:\ is not changed because it is not the default set by Windows. The current security is

D:(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICIIO;GA;;;CO)(A;OICI;0x1200a9;;;BU)(A;CI;LC;;;BU)(A;CIIO;DC;;;E

Do you see anything wrong with this? Compare it to your sceRoot log please.

microsoft.public.windowsxp.security_admin: Internal security problem with RPCSS

I cannot make changes to RPCSS! I tried from CMD.exe, safe mode administrator account and unable to access it through MMC or component services. I can't even access the help file to editing security templates! RPCSS is run by NTAUTHORITY/SYSTEM and when I tried to change it to local account it locked itself up. WMI, DTC, Help and Support, to name a few, can't communicate with it but its running by golly!

Here is my most recent setuperr log:

Error:

Setup encountered an error while trying to set system security.

An extended error has occurred.

Error:

Setup could not register the OLE Control C:\WINDOWS\system32\swprv.dll because of the following error:

DllInstall returned error 2147549183 (8000ffff).

I ran regsvr32 swprv.dll (VSCs) and it registered ok.

I have tons of log files which ones would you need to make a diagnosis?