

SVC host problem

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2008-05/msg01622.html>

- *From:* Mike <Mike@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 6 May 2008 02:17:00 -0700
-

Help!

I'm currently having intermittent problems with SVC host, in that it comes up with some error and I have an option to continue or debug.

Following some of the other posts on this problem, I've ran Hijackthis and the log file is posted below.

Can anyone advise what the problem is and more importantly – what the solution is to fix this?

Logfile of HijackThis v1.99.1
Scan saved at 10:11:52, on 06/05/2008
Platform: Windows XP SP2 (WinNT 5.01.2600)
MSIE: Internet Explorer v7.00 (7.00.6000.16640)

Running processes:

C:\WINDOWS\System32\smss.exe
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\system32\services.exe
C:\WINDOWS\system32\lsass.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\System32\svchost.exe
C:\WINDOWS\system32\svchost.exe
C:\Program Files\Intel\Wireless\Bin\EvtEng.exe
C:\Program Files\Intel\Wireless\Bin\S24EvMon.exe
C:\WINDOWS\system32\ZoneLabs\vsmon.exe
C:\WINDOWS\system32\spoolsv.exe
C:\Program Files\ThinkPad\ConnectUtilities\AcPrfMgrSvc.exe
C:\WINDOWS\system32\agrsmsvc.exe
C:\PROGRA~1\Grisoft\AVG7\avgamsvr.exe
C:\PROGRA~1\Grisoft\AVG7\avgupsvc.exe
C:\Program Files\LENOVO\HOTKEY\FNF5SVC.exe
C:\WINDOWS\System32\svchost.exe
C:\Program Files\Common Files\Microsoft Shared\VS7DEBUG\MDM.EXE
C:\WINDOWS\system32\HPZipm12.exe
C:\Program Files\Lenovo\PM Driver\PMSveH.exe
C:\Program Files\Intel\Wireless\Bin\RegSrvc.exe

SVC host problem

C:\WINDOWS\System32\rpcnetp.exe
C:\Program Files\Common Files\Lenovo\vtv_reg_monitor_svc.exe
C:\Program Files\Lenovo\Rescue and Recovery\rrservice.exe
C:\Program Files\Common Files\Lenovo\Scheduler\tvtsched.exe
C:\Program Files\Webroot\Washer\WasherSvc.exe
C:\Program Files\ThinkPad\ConnectUtilities\AcSvc.exe
c:\program files\lenovo\system update\suservice.exe
C:\Program Files\Common Files\Lenovo\Logger\logmon.exe
C:\Program Files\Lenovo\Client Security Solution\cssauth.exe
C:\WINDOWS\Explorer.EXE
C:\Program Files\Synaptics\SynTP\SynTPEnh.exe
C:\Program Files\Lenovo\HOTKEY\TpWAudAp.exe
C:\WINDOWS\AGRSMMMSG.exe
C:\Program Files\Lenovo\Client Security Solution\tvtpwm_tray.exe
C:\Program Files\ThinkPad\ConnectUtilities\SvcGuiHlpr.exe
C:\WINDOWS\system32\igfxtray.exe
C:\WINDOWS\system32\hkcmd.exe
C:\WINDOWS\system32\igfxpers.exe
C:\Program Files\Java\jre1.6.0_05\bin\jusched.exe
C:\Program Files\ThinkPad\ConnectUtilities\ACTray.exe
C:\Program Files\ThinkPad\ConnectUtilities\ACWLIcon.exe
C:\Program Files\Intel\Wireless\Bin\Dot1XCfg.exe
C:\PROGRA~1\BILLPS~1\WINPAT~1\winpatrol.exe
C:\WINDOWS\RTHDCPL.EXE
C:\PROGRA~1\Grisoft\AVG7\avgcc.exe
C:\Program Files\Adobe\Acrobat 8.0\Acrobat\Acrotray.exe
C:\Program Files\Zone Labs\ZoneAlarm\zlclient.exe
C:\Program Files\Hewlett-Packard\HP Software Update\HPWuSchd.exe
C:\Program Files\HP\hpcoretech\hpcmpmgr.exe
C:\Program Files\Webroot\Washer\wwDisp.exe
C:\WINDOWS\system32\ctfmon.exe
C:\Program Files\Common Files Ahead\Lib\NMBgMonitor.exe
C:\Program Files\Windows Media Player\WMPNSCFG.exe
C:\Program Files\Common Files Ahead\Lib\NMIndexingService.exe
C:\Program Files\Common Files Ahead\Lib\NMIndexStoreSvr.exe
C:\Program Files\Common Files\Macrovision Shared\FLEXnet
Publisher\FNPLicensingService.exe
C:\Program Files\Microsoft Office\Office12\OUTLOOK.EXE
C:\Program Files\Internet Explorer\iexplore.exe
C:\Program Files\Common Files\Microsoft Shared\Windows Live\WLLoginProxy.exe
C:\Documents and Settings\Mike\Desktop\HijackThis.exe

R0 – HKCU\Software\Microsoft\Internet Explorer\Main,Start Page =

<http://www.yahoo.co.uk>

R1 – HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL =

<http://go.microsoft.com/fwlink/?LinkId=69157>

R1 – HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL =

<http://go.microsoft.com/fwlink/?LinkId=54896>

R1 – HKLM\Software\Microsoft\Internet Explorer\Main,Search Page =

<http://go.microsoft.com/fwlink/?LinkId=54896>

R0 – HKLM\Software\Microsoft\Internet Explorer\Main,Start Page =

SVC host problem

<http://go.microsoft.com/fwlink/?LinkId=69157>

R0 – HKLM\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =

R1 – HKCU\Software\Microsoft\Internet Connection Wizard,ShellNext =

<http://go.microsoft.com/fwlink/?LinkId=74005>

O2 – BHO: Adobe PDF Reader Link Helper –

{06849E9F-C8D7-4D59-B87D-784B7D6BE0B3} – C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll

O2 – BHO: Skype add-on (mastermind) – {22BF413B-C6D2-4d91-82A9-A0F997BA588C} – C:\Program Files\Skype\Toolbars\Internet Explorer\SkypeIEPlugin.dll

O2 – BHO: Groove GFS Browser Helper – {72853161-30C5-4D22-B7F9-0BBC1D38A37E} – C:\PROGRA~1\MICROS~2\Office12\GRA8E1~1.DLL

O2 – BHO: SSVHelper Class – {761497BB-D6F0-462C-B6EB-D4DAF1D92D43} – C:\Program Files\Java\jre1.6.0_05\bin\ssv.dll

O2 – BHO: Windows Live Sign-in Helper – {9030D464-4C02-4ABF-8ECC-5164760863C6} – C:\Program Files\Common Files\Microsoft Shared\Windows Live\WindowsLiveLogin.dll

O2 – BHO: Adobe PDF Conversion Toolbar Helper – {AE7CD045-E861-484f-8273-0445EE161910} – C:\Program Files\Adobe\Acrobat 8.0\Acrobat\AcroIEFavClient.dll

O2 – BHO: ThinkVantage Password Manager – {F040E541-A427-4CF7-85D8-75E3E0F476C5} – C:\Program Files\Lenovo\Client Security Solution\tvtpwm_ie_com.dll

O3 – Toolbar: Adobe PDF – {47833539-D0C5-4125-9FA8-0819E2EAAC93} – C:\Program Files\Adobe\Acrobat 8.0\Acrobat\AcroIEFavClient.dll

O4 – HKLM\..\Run: [SynTPEnh] "C:\Program Files\Synaptics\SynTP\SynTPEnh.exe"

O4 – HKLM\..\Run: [TPWAUDAP] "C:\Program Files\Lenovo\HOTKEY\TpWAudAp.exe"

O4 – HKLM\..\Run: [AGRSMMMSG] AGRSMMMSG.exe

O4 – HKLM\..\Run: [SkyTel] SkyTel.EXE

O4 – HKLM\..\Run: [AzMixerSel] "C:\Program Files\Realtek\InstallShield\AzMixerSel.exe"

O4 – HKLM\..\Run: [igfxtray] C:\WINDOWS\system32\igfxtray.exe

O4 – HKLM\..\Run: [igfxhkcmd] C:\WINDOWS\system32\hkcmd.exe

O4 – HKLM\..\Run: [igfxpers] C:\WINDOWS\system32\igfxpers.exe

O4 – HKLM\..\Run: [SunJavaUpdateSched] "C:\Program Files\Java\jre1.6.0_05\bin\jusched.exe"

O4 – HKLM\..\Run: [ACTray] "C:\Program Files\ThinkPad\ConnectUtilities\ACTray.exe"

O4 – HKLM\..\Run: [ACWLIcon] "C:\Program Files\ThinkPad\ConnectUtilities\ACWLIcon.exe"

O4 – HKLM\..\Run: [cssauth] "C:\Program Files\Lenovo\Client Security Solution\cssauth.exe" silent

O4 – HKLM\..\Run: [WinPatrol] C:\PROGRA~1\BILLPS~1\WINPAT~1\winpatrol.exe

O4 – HKLM\..\Run: [IBM Warranty Notification] "C:\Program Files\IBM\acp\ERTS0749\ERTS0749.exe /nointro"

O4 – HKLM\..\Run: [RTHDCPL] RTHDCPL.EXE

O4 – HKLM\..\Run: [Alcmtr] ALCMTR.EXE

O4 – HKLM\..\Run: [AVG7_CC] "C:\PROGRA~1\Grisoft\AVG7\avgcc.exe" /STARTUP

O4 – HKLM\..\Run: [Acrobat Assistant 8.0] "C:\Program Files\Adobe\Acrobat 8.0\Acrobat\Acrotray.exe"

O4 – HKLM\..\Run: [ZoneAlarm Client] "C:\Program Files\Zone Labs\ZoneAlarm\zlclient.exe"

SVC host problem

O4 – HKLM\..\Run: [HP Software Update] "C:\Program Files\Hewlett-Packard\HP Software Update\HPWuSchd.exe"
O4 – HKLM\..\Run: [HP Component Manager] "C:\Program Files\HP\hpcoretech\hpcmpmgr.exe"
O4 – HKLM\..\Run: [HPDJ Taskbar Utility]
C:\WINDOWS\system32\spool\drivers\w32x86\3\hpztsb09.exe
O4 – HKCU\..\Run: [Window Washer] "C:\Program Files\Webroot\Washer\wwDisp.exe"
O4 – HKCU\..\Run: [ctfmon.exe] C:\WINDOWS\system32\ctfmon.exe
O4 – HKCU\..\Run: [BgMonitor_{79662E04-7C6C-4d9f-84C7-88D8A56B10AA}]
"C:\Program Files\Common Files Ahead\Lib\NMBgMonitor.exe"
O4 – HKCU\..\Run: [WMPNSCFG] C:\Program Files\Windows Media Player\WMPNSCFG.exe
O8 – Extra context menu item: Append to existing PDF – res://C:\Program Files\Adobe\Acrobat 8.0\Acrobat\AcroIEFavClient.dll/AcroIEAppend.html
O8 – Extra context menu item: Convert link target to Adobe PDF –
res://C:\Program Files\Adobe\Acrobat
8.0\Acrobat\AcroIEFavClient.dll/AcroIECapture.html
O8 – Extra context menu item: Convert link target to existing PDF –
res://C:\Program Files\Adobe\Acrobat
8.0\Acrobat\AcroIEFavClient.dll/AcroIEAppend.html
O8 – Extra context menu item: Convert selected links to Adobe PDF –
res://C:\Program Files\Adobe\Acrobat
8.0\Acrobat\AcroIEFavClient.dll/AcroIECaptureSelLinks.html
O8 – Extra context menu item: Convert selected links to existing PDF –
res://C:\Program Files\Adobe\Acrobat
8.0\Acrobat\AcroIEFavClient.dll/AcroIEAppendSelLinks.html
O8 – Extra context menu item: Convert selection to Adobe PDF –
res://C:\Program Files\Adobe\Acrobat
8.0\Acrobat\AcroIEFavClient.dll/AcroIECapture.html
O8 – Extra context menu item: Convert selection to existing PDF –
res://C:\Program Files\Adobe\Acrobat
8.0\Acrobat\AcroIEFavClient.dll/AcroIEAppend.html
O8 – Extra context menu item: Convert to Adobe PDF – res://C:\Program
Files\Adobe\Acrobat 8.0\Acrobat\AcroIEFavClient.dll/AcroIECapture.html
O8 – Extra context menu item: E&xport to Microsoft Excel –
res://C:\PROGRA~1\MICROS~2\Office12\EXCEL.EXE/3000
O9 – Extra button: (no name) – {0045D4BC-5189-4b67-969C-83BB1906C421} –
C:\Program Files\Lenovo\Client Security Solution\tvtpwm_ie_com.dll
O9 – Extra 'Tools' menuitem: ThinkVantage Password Manager... –
{0045D4BC-5189-4b67-969C-83BB1906C421} – C:\Program Files\Lenovo\Client
Security Solution\tvtpwm_ie_com.dll
O9 – Extra button: (no name) – {08B0E5C0-4FCB-11CF-AAA5-00401C608501} –
C:\Program Files\Java\jre1.6.0_05\bin\ssv.dll
O9 – Extra 'Tools' menuitem: Sun Java Console –
{08B0E5C0-4FCB-11CF-AAA5-00401C608501} – C:\Program
Files\Java\jre1.6.0_05\bin\ssv.dll
O9 – Extra button: Send to OneNote – {2670000A-7350-4f3c-8081-5663EE0C6C49}
– C:\PROGRA~1\MICROS~2\Office12\ONBttNIE.dll
O9 – Extra 'Tools' menuitem: S&end to OneNote –
{2670000A-7350-4f3c-8081-5663EE0C6C49} –
C:\PROGRA~1\MICROS~2\Office12\ONBttNIE.dll

SVC host problem

O9 – Extra button: Skype – {77BF5300-1474-4EC7-9980-D32B190E9B07} –
C:\Program Files\Skype\Toolbars\Internet Explorer\SkypeIEPlugin.dll

O9 – Extra button: Research – {92780B25-18CC-41C8-B9BE-3C9C571A8263} –
C:\PROGRA~1\MICROS~2\Office12\REFIEBAR.DLL

O9 – Extra button: (no name) – {e2e2dd38-d088-4134-82b7-f2ba38496583} –
%windir%\Network Diagnostic\xpnetdiag.exe (file missing)

O9 – Extra 'Tools' menuitem: @xpsp3res.dll,-20001 –
{e2e2dd38-d088-4134-82b7-f2ba38496583} – %windir%\Network
Diagnostic\xpnetdiag.exe (file missing)

O9 – Extra button: Messenger – {FB5F1910-F110-11d2-BB9E-00C04F795683} –
C:\Program Files\Messenger\msmsgs.exe

O9 – Extra 'Tools' menuitem: Windows Messenger –
{FB5F1910-F110-11d2-BB9E-00C04F795683} – C:\Program Files\Messenger\msmsgs.exe

O11 – Options group: [INTERNATIONAL] International*

O16 – DPF: {1C3DE665-D259-4C72-9D7D-C51FCB4CCFB9} (Panasonic Network Camera)
– <http://217.155.209.14:2220/SysCamInst.cab>

O16 – DPF: {2DAD3559-2923-4935-AD49-B673D2539944} (IASRunner Class) –
<http://www-307.ibm.com/pc/support/acpir.cab>

O16 – DPF: {54BE6B6F-3056-470B-97E1-BB92E051B6C4} (DeviceEnum Class) –
<http://h20264.www2.hp.com/ediags/dd/install/HPDriverDiagnosticsxp2k.cab>

O16 – DPF: {6E32070A-766D-4EE6-879C-DC1FA91D2FC3} (MUWebControl Class) –
http://www.update.microsoft.com/microsoftupdate/v6/V5Controls/en/x86/client/muweb_site.cab?1197018878546

O16 – DPF: {8AD9C840-044E-11D1-B3E9-00805F499D93} (Java Runtime Environment
1.6.0) –
<http://javadl-esd.sun.com/update/1.6.0/jinstall-6u5-windows-i586-jc.cab>

O18 – Protocol: grooveLocalGWS – {88FED34C-F0CA-4636-A375-3CB6248B04CD} –
C:\PROGRA~1\MICROS~2\Office12\GR99D3~1.DLL

O18 – Protocol: ms-help – {314111C7-A502-11D2-BBCA-00C04F8EC294} –
C:\Program Files\Common Files\Microsoft Shared\Help\hxds.dll

O18 – Protocol: skype4com – {FFC8B962-9B40-4DFF-9458-1830C7DD7F5D} –
C:\PROGRA~1\COMMON~1\Skype\SKYPE4~1.DLL

O18 – Filter hijack: text/xml – {807563E5-5146-11D5-A672-00B0D022E945} –
C:\PROGRA~1\COMMON~1\MICROS~1\OFFICE12\MSOXMLMF.DLL

O20 – Winlogon Notify: ACNotify – ACNotify.dll (file missing)

O20 – Winlogon Notify: igfxcui – C:\WINDOWS\SYSTEM32\igfxdev.dll

O20 – Winlogon Notify: tphotkey – C:\Program Files\Lenovo\HOTKEY\tphklock.dll

O21 – SSODL: WPDShServiceObj – {AAA288BA-9A4C-45B0-95D7-94D524869DB5} –
C:\WINDOWS\system32\WPDShServiceObj.dll

O23 – Service: Ac Profile Manager Service (AcPrfMgrSvc) – Lenovo –
C:\Program Files\ThinkPad\ConnectUtilities\AcPrfMgrSvc.exe

O23 – Service: Access Connections Main Service (AcSvc) – Lenovo –
C:\Program Files\ThinkPad\ConnectUtilities\AcSvc.exe

O23 – Service: Agere Modem Call Progress Audio (AgereModemAudio) – Agere
Systems – C:\WINDOWS\system32\agrsmSvc.exe

O23 – Service: AVG7 Alert Manager Server (Avg7Alrt) – GRISOFT, s.r.o. –
C:\PROGRA~1\Grisoft\AVG7\avgamsvr.exe

O23 – Service: AVG7 Update Service (Avg7UpdSvc) – GRISOFT, s.r.o. –
C:\PROGRA~1\Grisoft\AVG7\avgupsvc.exe

O23 – Service: Intel(R) PROSet/Wireless Event Log (EvtEng) – Intel
Corporation – C:\Program Files\Intel\Wireless\Bin\EvtEng.exe

O23 – Service: FLEXnet Licensing Service – Macrovision Europe Ltd. –

SVC host problem

C:\Program Files\Common Files\Macrovision Shared\FLEXnet
Publisher\FNPLicensingService.exe
O23 – Service: Fn+F5 Service (FNF5SVC) – Lenovo. – C:\Program
Files\LENOVO\HOTKEY\FNF5SVC.exe
O23 – Service: InstallDriver Table Manager (IDriverT) – Macrovision
Corporation – C:\Program Files\Common Files\InstallShield\Driver\1150\Intel
32\IDriverT.exe
O23 – Service: NBService – Nero AG – C:\Program Files\Nero\Nero 7\Nero
BackItUp\NBService.exe
O23 – Service: NMIndexingService – Nero AG – C:\Program Files\Common
Files\Ahead\Lib\NMIndexingService.exe
O23 – Service: Pml Driver HPZ12 – HP – C:\WINDOWS\system32\HPZipm12.exe
O23 – Service: PMSveH – Lenovo – C:\Program Files\Lenovo\PM Driver\PMSveH.exe
O23 – Service: IBM PSA Access Driver Control (PsaSrv) – Unknown owner –
C:\WINDOWS\system32\PsaSrv.exe (file missing)
O23 – Service: Intel(R) PROSet/Wireless Registry Service (RegSrv) – Intel
Corporation – C:\Program Files\Intel\Wireless\Bin\RegSrv.exe
O23 – Service: Intel(R) PROSet/Wireless Service (S24EventMonitor) – Intel
Corporation – C:\Program Files\Intel\Wireless\Bin\S24EvMon.exe
O23 – Service: ServiceLayer – Nokia. – C:\Program Files\PC Connectivity
Solution\ServiceLayer.exe
O23 – Service: System Update (SUService) – Lenovo Group Limited – c:\program
files\lenovo\system update\suservice.exe
O23 – Service: ThinkVantage Registry Monitor Service – Lenovo Group Limited
– C:\Program Files\Common Files\Lenovo\tvt_reg_monitor_svc.exe
O23 – Service: TVT Backup Service – Lenovo Group Limited – C:\Program
Files\Lenovo\Rescue and Recovery\rrservice.exe
O23 – Service: TVT Scheduler – Lenovo Group Limited – C:\Program
Files\Common Files\Lenovo\Scheduler\tvtsched.exe
O23 – Service: TrueVector Internet Monitor (vsmon) – Zone Labs, LLC –
C:\WINDOWS\system32\ZoneLabs\vsmon.exe
O23 – Service: Window Washer Engine (wwEngineSvc) – Webroot Software, Inc. –
C:\Program Files\Webroot\Washer\WasherSvc.exe

Thanks in advance.

Mike

HijackThis log file
