

Re: Svchost.exe & Wuauctl.exe Cannibalizing My CPU Usage on Internet ?

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windowsupdate/2007-08/msg01354.html>

- *From:* "MowGreen [MVP]" <mowgreen@xxxxxxxxxxxxxx>
 - *Date:* Fri, 24 Aug 2007 12:03:40 -0700
-

When you use Automatic Updates to scan for updates or to apply updates to applications that use Windows Installer, you experience issues that involve the Svchost.exe process
<http://support.microsoft.com/kb/932494>

MowGreen [MVP 2003-2007]

=====
-343- FDNY
Never Forgotten
=====

Flex wrote:

i spoke with a microsoft technician yesterday and he gave me this link to run
<http://www.spywareinfo.com/xscan.php> good luck

"teknowbabble@xxxxxxxx" wrote:

Ive been pretty happy with WinXP for the most part until recently.

When I get on the internet the CPU usage goes to 100% Usage and does not stop until I de-activate the Windows Update Client using the NET STOP WUAUSERV system command.

When I use Sysinternals Process Explorer I notice the following;

SVCHOST.exe is the process using the most CPU cycles. There are 2 wuauctl.exe processes that are running as a children under SVCHOST.exe. The first wuauctl.exe is present after I bootup. The second wuauctl.exe process appears when I get on the Internet.

To temporarily resolve the problem I do a ...

```
c:>net stop wuauserv
```

Re: Svchost.exe & Wuauctl.exe Cannibalizing My CPU Usage on Internet ?

.... after serveral minutes wuauctl.exe disappears
.... and then wmiprvse.exe disappears.

It takes several minutes for this to occur which I find unusual.

Then my CPU Usage returns to Normal.

My Windows Update System is setup on a NOTIFY ME BUT DO NOT
DOWNLOAD
setting.

Im not sure whats going on. Any help is appreciated.

If you have any ideas plz let me know.

Ive provided additional information below.

Thanks
Teknowbabble

My System

Pentium 1 166mhz system
128 MB RAM
Windows XP SP1 (WinNT 5.01.2600)
Internet Explorer v6.00 SP1 (6.00.2800.1106)
2 HDD: 40 Gig & 80 Gig

This system has worked fine with no problems. Im running Office Pro
2003 with no problems.

List of WUAUCLT* FILES RUNNING WHEN CPU AT 100%

wuauctl.exe 113,944 8/3/2004 2:02 PM a
C:\windows\LastGood\System32\
wuauctl.exe 124,184 5/26/2005 4:16 AM a
C:\windows\SYSTEM32\dlcache\
wuauctl.exe 124,184 5/26/2005 4:16 AM a
C:\windows\SYSTEM32\
WUAUCLT.EXE-399A8E72.pf 23,256 10/21/2005 11:06 PM a
C:\windows\Prefetch\
wuauctl1.exe 167,704 8/3/2004 2:01 PM a
C:\windows\LastGood\System32\
wuauctl1.exe 172,312 5/26/2005 4:16 AM a
C:\windows\SYSTEM32\

CHECKED FOR SPYWARE & VIRUS'

Re: Svchost.exe & Wuauctl.exe Cannibalizing My CPU Usage on Internet ?

- 1 Ran CWS shredder 2.15 (Found nothing)
2. Run Spybot 1.3 (Found a couple tracking cookies)
3. Ran Adaware 6.181 (Found a couple tracking cookies)
4. Ran AVG 7.0.338 (Found No Virus')

Ran System File Checker with No Changes

c:>Sfc /scannow

—> I thought I might have Corrupted DLL cache files.

c:/windows/system32/dllcache/

HijackThis Log File When System at CPU @ 100%

Logfile of HijackThis v1.99.1

Scan saved at 3:17:51 AM, on 10/23/2005

Platform: Windows XP SP1 (WinNT 5.01.2600)

MSIE: Internet Explorer v6.00 SP1 (6.00.2800.1106)

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\spoolsv.exe
- C:\WINDOWS\Microsoft.NET\Framework\v2.0.40607\aspnet_admin.exe
- C:\PROGRA~1\Grisoft\AVGFRE~1\avgamsvr.exe
- C:\PROGRA~1\Grisoft\AVGFRE~1\avgupsvc.exe
- C:\WINDOWS\system32\cisvc.exe
- C:\Program Files\Common Files\Microsoft Shared\VS7Debug\mdm.exe
- C:\WINDOWS\System32\svchost.exe
- C:\WINDOWS\SYSTEM32\ZONELABS\VSMON.EXE
- C:\WINDOWS\Explorer.EXE
- C:\Program Files\Hewlett-Packard\HP Share-to-Web\hpgs2wnd.exe
- C:\Program Files\Zone Labs\ZoneAlarm\zlclient.exe
- C:\WINDOWS\System32\wuauctl.exe
- C:\PROGRA~1\Grisoft\AVGFRE~1\avgcc.exe
- C:\Program Files\Microsoft ActiveSync\WCESCOMM.EXE
- C:\PROGRA~1\HEWLET~1\HPSHAR~1\hpgs2wnf.exe
- C:\WINDOWS\System32\ctfmon.exe
- C:\WINDOWS\system32\cidaemon.exe
- C:\WINDOWS\system32\cidaemon.exe
- C:\ALEXS-FILES\Computer\Diagnostics\procexp.exe
- C:\WINDOWS\System32\taskmgr.exe
- C:\Program Files\Internet Explorer\iexplore.exe
- C:\WINDOWS\System32\CMMON32.EXE

Re: Svchost.exe & Wuaucit.exe Cannibalizing My CPU Usage on Internet ?

C:\WINDOWS\System32\wuaucit.exe

C:\Documents and Settings\freewil\Desktop\HijackThis-V1-99-1.exe

O2 – BHO: AcroIEHlprObj Class –

{06849E9F-C8D7-4D59-B87D-784B7D6BE0B3}

– C:\Program Files\Adobe\Acrobat 5.0\Reader\ActiveX\AcroIEHelper.ocx

O2 – BHO: (no name) – {53707962-6F74-2D53-2644-206D7942484F} –

C:\PROGRA~1\SPYBOT~1\SDHelper.dll

O3 – Toolbar: &Radio – {8E718888-423F-11D2-876E-00A0C9082467} –

C:\WINDOWS\System32\msdxm.ocx

O4 – HKLM\..\Run: [SystemTray] SysTray.Exe

O4 – HKLM\..\Run: [Share-to-Web Namespace Daemon] C:\Program

Files\Hewlett-Packard\HP Share-to-Web\hpgs2wnd.exe

O4 – HKLM\..\Run: [Zone Labs Client] C:\Program Files\Zone

Labs\ZoneAlarm\zlclient.exe

O4 – HKLM\..\Run: [AVG7_CC]

C:\PROGRA~1\Grisoft\AVGFRE~1\avgcc.exe

/STARTUP

O4 – HKCU\..\Run: [H/PC Connection Agent] "C:\Program Files\Microsoft

ActiveSync\WCESCOMM.EXE"

O4 – HKCU\..\Run: [ctfmon.exe] C:\WINDOWS\System32\ctfmon.exe

O8 – Extra context menu item: E&xport to Microsoft Excel –

res://C:\PROGRA~1\MICROS~3\OFFICE11\EXCEL.EXE/3000

O9 – Extra button: Create Mobile Favorite –

{2EAF5BB1-070F-11D3-9307-00C04FAE2D4F} – C:\Program

Files\Microsoft

ActiveSync\inetrepl.dll

O9 – Extra button: (no name) –

{2EAF5BB2-070F-11D3-9307-00C04FAE2D4F} –

C:\Program Files\Microsoft ActiveSync\inetrepl.dll

O9 – Extra 'Tools' menuitem: Create Mobile Favorite... –

{2EAF5BB2-070F-11D3-9307-00C04FAE2D4F} – C:\Program

Files\Microsoft

ActiveSync\inetrepl.dll

O9 – Extra button: Research –

{92780B25-18CC-41C8-B9BE-3C9C571A8263} –

C:\PROGRA~1\MICROS~3\OFFICE11\REFIEBAR.DLL

O9 – Extra button: (no name) –

{CD67F990-D8E9-11d2-98FE-00C0F0318AFE} –

(no file)

O9 – Extra button: Messenger –

{FB5F1910-F110-11d2-BB9E-00C04F795683} –

C:\Program Files\Messenger\MSMSG.S.EXE

O9 – Extra 'Tools' menuitem: Messenger –

{FB5F1910-F110-11d2-BB9E-00C04F795683} – C:\Program

Files\Messenger\MSMSG.S.EXE

O12 – Plugin for .spop: C:\Program Files\Internet

Explorer\Plugins\NPDocBox.dll

O16 – DPF: Yahoo! Chat –

<http://us.chat1.yimg.com/us.yimg.com/i/chat/applet/c381/chat.cab>

O16 – DPF: {2B323CD9-50E3-11D3-9466-00A0C9700498} (Yahoo!

Re: Svchost.exe & Wuauctl.exe Cannibalizing My CPU Usage on Internet ?

Audio

Conferencing) –

<http://us.chat1.yimg.com/us.yimg.com/i/chat/applet/v45/yacsc.com.cab>

O16 – DPF: {4E888414–DB8F–11D1–9CD9–00C04F98436A}

(Microsoft.WinRep) –

<https://webresponse.one.microsoft.com/oas/ActiveX/winrep.cab>

O16 – DPF: {6E32070A–766D–4EE6–879C–DC1FA91D2FC3}

(MUWebControl Class)

–

http://update.microsoft.com/microsoftupdate/v6/V5Controls/en/x86/client/muweb_site.cab?11289422

O16 – DPF: {7D1E9C49–BD6A–11D3–87A8–009027A35D73} (Yahoo!

Audio UI1) –

<http://chat.yahoo.com/cab/yacsui.cab>

O16 – DPF: {9B17FE0E–51F2–4692–8B32–8EFB805FC0E7}

(HPObjctInstaller

Class) –

<http://h30155.www3.hp.com/ediags/gs/install/guidedsolutions.cab>

O16 – DPF: {A7E092C3–692A–11D0–A7E5–08002B322F3B}

(WebResponseAttachments Control) –

<https://webresponse.one.microsoft.com/oas/ActiveX/FileXfer.cab>

O16 – DPF: {F58E1CEF–A068–4C15–BA5E–587CAF3EE8C6} (MSN

Chat Control

4.5) – <http://chat.msn.com/bin/msnchat45.cab>

O17 –

HKLM\System\CCS\Services\Tcpip\..\{A338D98A–04F0–4998–81B4–E5E857BCD5B9}:

NameServer = 64.40.40.51 66.54.140.10

O17 –

HKLM\System\CS1\Services\Tcpip\..\{A338D98A–04F0–4998–81B4–E5E857BCD5B9}:

NameServer = 64.40.40.51 66.54.140.10

O18 – Protocol: ms–help –

{314111C7–A502–11D2–BBCA–00C04F8EC294} –

C:\Program Files\Common Files\Microsoft Shared\Help\hxds.dll

O23 – Service: AVG7 Alert Manager Server (Avg7Alrt) – GRISOFT, s.r.o.

–

C:\PROGRA~1\Grisoft\AVGFRE~1\avgamsvr.exe

O23 – Service: AVG7 Update Service (Avg7UpdSvc) – GRISOFT, s.r.o. –

C:\PROGRA~1\Grisoft\AVGFRE~1\avgupsvc.exe

O23 – Service: TrueVector Internet Monitor (vsmon) – Zone Labs, LLC –

C:\WINDOWS\SYSTEM32\ZONELABS\VSMON.EXE

Tasklist When CPU @ 100% Usage

C:\>tasklist /svc

Image Name PID Services

=====

=====

Re: Svchost.exe & Wuauctl.exe Cannibalizing My CPU Usage on Internet ?

System Idle Process 0 N/A
System 4 N/A
SMSS.EXE 308 N/A
CSRSS.EXE 356 N/A
WINLOGON.EXE 392 N/A
SERVICES.EXE 436 Eventlog, PlugPlay
LSASS.EXE 448 ProtectedStorage, SamSs
SVCHOST.EXE 700 RpcSs
SVCHOST.EXE 740 AudioSrv, CryptSvc, Dhcp, dmserver,
ERSvc,EventSystem, FastUserSwitchingCompatibility,
helpsvc, lanmanserver, Netman, Nla, RasMan,
Schedule, seclogon, SENS, SharedAccess,
ShellHWDetection, srservice, TapiSrv,
TermService, Themes, TrkWks, uploadmgr,
W32Time, winmgmt, WmdmPmSp, wuauclt, WZCSVC
SVCHOST.EXE 844 Dnscache
SVCHOST.EXE 868 LmHosts, RemoteRegistry, SSDPSRV,
WebClient
spoolsv.exe 968 Spooler
alg.exe 1052 ALG
aspnet_admin.exe 1072 aspnet_admin
avgamsvr.exe 1096 Avg7Alrt
avgupsvc.exe 1124 Avg7UpdSvc
cisvc.exe 1164 CiSvc
mdm.exe 1200 MDM
SVCHOST.EXE 1248 stisvc
vsmon.exe 1276 vsmon
EXPLORER.EXE 480 N/A
HPGS2WND.EXE 1400 N/A
zlclient.exe 1464 N/A
wuauctl.exe 748 N/A
avgcc.exe 1632 N/A
wcescomm.exe 1700 N/A
hpgs2wnf.exe 1732 N/A
ctfmon.exe 1600 N/A
cidaemon.exe 2108 N/A
cidaemon.exe 2120 N/A
taskmgr.exe 2620 N/A
CMMON32.EXE 2956 N/A
wuauctl.exe 3032 N/A
procexp.exe 3344 N/A
CMD.EXE 3380 N/A
tasklist.exe 3392 N/A
WMIPRVSE.EXE 3428 N/A

C:\>