

## Re: PID 1212 slowly maxing out?

---

*Source:*

[http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help\\_and\\_support/2007-07/msg01624.htm](http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.help_and_support/2007-07/msg01624.htm)

---

- *From:* Stephen McGrath <Stephen\_McGrath@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
  - *Date:* Fri, 20 Jul 2007 07:54:03 -0700
- 

Hi

I too am experiencing the slow memory leak in SVCHOST.EXE, although I wouldn't call it slow. I have to reboot at least every two days. I run WinXP Pro with SP2, AVG for virus protection, ZoneAlarm firewall as well as the Netgear hardware firewall, and Ad-aware for spyware. RPCSS is the process in SVCHOST that is eating up my RAM. I can also tell you that it is listening on 0.0.0.0:135, whatever that means. In what may only be a coincidence, I can't install the latest .Net Windows Update (although I am halfway through a solution for that). Has anyone determined how to resolve this?

"Wesley Vogel" wrote:

I can see that SVCHOST.EXE that hosts RPSCC.DLL can cause a memory leak on Windows 2003 servers, but could it affect Windows XP as well? I couldn't find any information, or a hotfix for this.

Honestly, it beats me.

I presume the Blaster Worm would show up on either Symantec Antivirus or the Malicious Removal Tool?

I would assume that also.

—  
Hope this helps. Let us know.

Wes  
MS-MVP Windows Shell/User

In <news:eeUK8FnjHHA.4772@xxxxxxxxxxxxxxxxxxxxxxxxxx>,  
Trond Svendsen <trond@xxxxxxxxxxxxxx> hunted and pecked:

Re: PID 1212 slowly maxing out?

I can see that SVCHOST.EXE that hosts RPSCC.DLL can cause a memory leak on Windows 2003 servers, but could it affect Windows XP as well? I couldn't find any information, or a hotfix for this.

I presume the Blaster Worm would show up on either Symantec Antivirus or the Malicious Removal Tool?

Trond

"Wesley Vogel" <123WVogel955@xxxxxxxxxxxx> wrote in message [news:eWZ%23xYmjHHA.3472@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:eWZ%23xYmjHHA.3472@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Hi Trond,

RpcSS.dll is Distributed COM Services. RpcSS.dll is related to DcomLaunch (DCOM Server Process Launcher service) and RpcSs (Remote Procedure Call (RPC) service). Both are necessary services.

RpcSS.dll is also related to the Blaster worm.

Search the Support Knowledge Base (KB)

Search Product: Windows XP

For: RpcSS.dll

<http://support.microsoft.com/search/default.aspx?catalog=LCID%3d1033&1033comm=1&qu>

--

Hope this helps. Let us know.

Wes

MS-MVP Windows Shell/User

In [news:OYrXmqhjHHA.3708@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:OYrXmqhjHHA.3708@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx),

Trond Svendsen <trond@xxxxxxxxxxxx> hunted and pecked:

Wes,

Yes, I'm on a home network running on wireless. I have two computers running, and they both connect to inet using a wireless accesspoint. I also have RDP enabled on both on them.

I've been monitoring the services, and it seems like it's RpcSS.dll that is slowly but shurely increasing with 4K at a time, until the OS is left useless.

Re: PID 1212 slowly maxing out?

Best regards  
Trond Svendsen

Hi Trond,

I question why you have  
these services running.  
Maybe you need them.  
Are you on a network? On  
dialup?

TermService = Terminal  
Services  
Browser = Computer  
Browser service  
FastUserSwitchingCompatibility  
= Fast User Switching  
Compatibility  
service lanmanserver =  
Server service  
lanmanworkstation =  
Workstation service  
Nla = Network Location  
Awareness service  
RasMan = Remote Access  
Connection Manager service  
seclogon = RunAs Service /  
Secondary Logon service  
ShellHWDetection = Shell  
Hardware Detection service  
TapiSrv = Telephony  
service  
dmserver = Logical Disk  
Manager service  
ERSvc = Error Reporting  
Service  
TrkWks = Distributed Link  
Tracking Client service  
WZCSVC = Wireless Zero  
Configuration service  
LmHosts = TCP/IP  
NetBIOS Helper service  
RemoteRegistry = Remote  
Registry service  
SSDPSRV = SSDP  
Discovery Service  
WebClient = WebClient  
service

Re: PID 1212 slowly maxing out?

If not on a network, I would  
disable the following  
services:

Terminal Services

Disabled, for security  
measures.

Manual, if using Remote  
Desktop (Remote  
Administration), Remote  
Assistance, Fast User  
Switching.

<http://smallvoid.com/tweak/winnt/service/stuv.html#TERMSERVICE>

Computer Browser service  
Automatic, if on a network  
and there is no dedicated  
master browser.

Disabled, if not browsing  
Network Neighborhood for  
shares/printers.

<http://smallvoid.com/tweak/winnt/service/abc.html#BROWSER>

Fast User Switching

Compatibility

Manual, and it will only be  
activated when a fast user  
switch is  
requested. Otherwise  
disabled.

<http://smallvoid.com/tweak/winnt/service/def.html#FUS>

Server service

Automatic, if wanting to  
share files and printers.

Disabled, if no files to share.

<http://smallvoid.com/tweak/winnt/service/stuv.html#SERVER>

Workstation service

Automatic, when in a simple  
home network.

Disabled, if not needing  
access to network-shares

<http://smallvoid.com/tweak/winnt/service/wxyz.html#WORKSTATION>

Network Location

Awareness

Disabled if not on a  
network.

<http://smallvoid.com/tweak/winnt/service/mno.html#NLA>

Re: PID 1212 slowly maxing out?

Remote Access Connection  
Manager

Disabled, if not using  
Modem, Virtual Private  
Networking(VPN) or  
Internet

Connection Sharing.  
Manual, if wanting the  
ability to create such  
connections when  
required.

<http://smallvoid.com/tweak/winnt/service/pqr.html#RASMAN>

RunAs Service / Secondary  
Logon

Disabled, if not needing to  
start applications under  
another accounts  
credentials.

Manual, if once in awhile  
need to start an application  
as another user  
(Like Administrator).

Automatic, if constantly  
starting applications as  
another user, as it  
will avoid slow application  
launch.

<http://smallvoid.com/tweak/winnt/service/pqr.html#SECLOGON>

Shell Hardware Detection

Disabled, unless having  
problems configuring your  
Autoplay.

<http://smallvoid.com/tweak/winnt/service/stuv.html#SHELLHWDETECTION>

Telephony

Disabled if not on a dialup  
modem.

<http://smallvoid.com/tweak/winnt/service/stuv.html#TAPISRV>

Logical Disk Manager  
service

Logical Disk Manager  
Watchdog Service that  
detects the  
appearance/disappearance of  
hard drives and the  
partitions they  
contains.

Re: PID 1212 slowly maxing out?

Note if this service is stopped, then dynamic disk status and configuration information might become outdated. Therefore if one is considering to change this service state to Manual, then make sure that none of the disks in the system are configured as dynamic disks.

<http://smallvoid.com/tweak/winnt/service/jkl.html#DMSEVER>

If you have none of the above, Logical Disk Manager service doesn't need to run.

Error Reporting Service if don't want to give detailed information about your computer to Microsoft every time an application crashes.

<http://smallvoid.com/tweak/winnt/service/def.html#ERSVC>

Distributed Link Tracking Client service Disabled, if on a simple home network. Automatic, if connected to a domain and uses a NTFS file system.

<http://smallvoid.com/tweak/winnt/service/def.html#TRKWKS>

Wireless Zero Configuration Disabled, if not using wireless network with a 802.11 network device. Automatic, if using wireless network AND manufacture of the netcard haven't provided software of their own.

<http://smallvoid.com/tweak/winnt/service/wxyz.html#WZCSVC>

TCP/IP NetBIOS Helper service Disabled, if on a simple home network (Even if

Re: PID 1212 slowly maxing out?

using Netbios over  
TcpIp).

Automatic, if needing to  
login on to a domain using  
Netbios/WINS or  
using  
the LmHosts-file.

<http://smallvoid.com/tweak/winnt/service/stuv.html#LMHOSTS>

Remote Registry service  
Disabled, for security  
measures.

<http://smallvoid.com/tweak/winnt/service/pqr.html#REMOTEREGISTRY>

SSDP Discovery Service  
Disabled, unless working  
with networked Universal  
Plug and Play devices  
or using Internet Connection  
Sharing.

<http://smallvoid.com/tweak/winnt/service/stuv.html#SSDPSRV>

WebClient  
Disabled.

<http://smallvoid.com/tweak/winnt/service/wxyz.html#WEBCLIENT>

You can look up  
recommendations for  
services here...

<http://smallvoid.com/tweak/winnt/services.html>

<http://www.blackviper.com/WinXP/servicecfg.htm>

--

Hope this helps. Let us  
know.

Wes  
MS-MVP Windows  
Shell/User

In  
[news:ehTO0UZjHHA.3940@xxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:ehTO0UZjHHA.3940@xxxxxxxxxxxxxxxxxxxxxxxxx),  
Trond Svendsen  
<trond@xxxxxxxxxxxxxxxxx>  
hunted and pecked:

Background;  
while  
installing

Re: PID 1212 slowly maxing out?

WinXP  
recently, I  
installed  
Symantec  
Antivirus  
Corp  
Edition  
10.1.6.6000  
/SAV)  
before  
installing  
any network  
drivers.  
Then I  
started  
Windows  
Update, and  
installed the  
rest of my  
software.  
Just now I  
booted into  
safe mode,  
and ran a  
deep scan  
using SAV.  
No  
risks,  
or viruses  
found.

I consider  
myself an  
experienced  
user, and  
I've  
(re)installed  
WinXP  
many  
times, but  
this is the  
first time  
I've  
experienced  
this issue.

Here are a  
list of the  
SVCHOST.EXE  
running:

Re: PID 1212 slowly maxing out?

svchost.exe  
952  
DcomLaunch,  
TermService  
svchost.exe  
1020 RpcSs  
svchost.exe  
1060  
AudioSrv,  
Browser,  
CryptSvc,  
Dhcp,  
dmserver,  
ERSvc,  
EventSystem,  
FastUserSwitchingCompatibility,  
helpsvc,  
lanmanserver,  
lanmanworkstation,  
Netman,  
Nla,  
RasMan,  
Schedule,  
seclogon,  
SENS,  
SharedAccess,  
ShellHWDetection,  
TapiSrv,  
Themes,  
TrkWks,  
W32Time,  
winmgmt,  
wscsvc,  
wuauserv,  
WZCSVC  
svchost.exe  
1156  
Dnscache  
svchost.exe  
1232  
LmHosts,  
RemoteRegistry,  
SSDPSRV,  
WebClient  
Best regards  
Trond  
Svendsen

PID,  
process

Re: PID 1212 slowly maxing out?

identifier,  
numbers  
change  
every  
time  
that  
you  
boot  
and  
PID  
numbers  
are  
not  
necessarily  
the  
same  
from  
one  
machine  
to  
the  
next.  
PIDs  
can  
be  
used  
with  
the  
netstat  
-ano  
command,  
for  
example,  
to  
see  
what  
PID  
is  
what  
process  
in  
the  
Task  
Manager.

process  
identifier  
(PID)  
[[A  
numerical  
identifier

Re: PID 1212 slowly maxing out?

that  
uniquely  
distinguishes  
a  
process  
while  
it  
runs.  
Use  
Task  
Manager  
to  
view  
PIDs.]]

The  
Network  
Service  
account  
is  
a  
special  
built-in  
account  
that  
has  
reduced  
privileges  
similar  
to  
an  
authenticated  
user  
account.  
The  
actual  
name  
of  
the  
account  
is  
NT  
AUTHORITY\NetworkService.

Network  
Service  
uses  
this...  
C:\WINDOWS\System32\svchost.exe  
-k  
NetworkService

Re: PID 1212 slowly maxing out?

to  
start  
svchost.exe  
to  
load  
DnsCache,  
the  
DNS  
Client  
service,  
which  
is  
dnsrslvr.dll.

UPDATE  
your  
antivirus  
software  
and  
run  
a  
full  
system  
scan.

UPDATE  
whatever  
anti-spyware  
applications  
that  
you  
have  
and  
run  
a  
full  
system  
scan  
with  
each  
one.

You  
might  
want  
to  
start  
in  
Safe  
Mode  
to

Re: PID 1212 slowly maxing out?

run  
your  
antivirus  
and  
anti-spyware  
software.

Running  
a  
full  
system  
antivirus  
scan  
or  
anti-spyware  
scan  
in  
Safe  
Mode  
can  
be  
a  
good  
idea.  
Some  
viruses  
and  
other  
malware  
like  
to  
conceal  
themselves  
in  
areas  
Windows  
protects  
while  
using  
them.  
Safe  
mode  
can  
prevent  
those  
applications  
access  
and  
therefore  
unprotect  
the

Re: PID 1212 slowly maxing out?

viruses  
or  
other  
malware  
allowing  
for  
easier  
removal.

"In  
safe  
mode,  
you  
have  
access  
to  
only  
basic  
files  
and  
drivers  
(mouse,  
monitor,  
keyboard,  
mass  
storage,  
base  
video,  
default  
system  
services),  
just  
the  
minimum  
device  
drivers  
required  
to  
start  
Windows."

Because  
of  
that  
some  
malware  
does  
not  
load  
in  
Safe

Re: PID 1212 slowly maxing out?

Mode  
and  
is  
easier  
to  
get  
rid  
of.

How  
to  
start  
Windows  
in  
Safe  
Mode  
Windows  
XP

<http://www.bleepingcomputer.com/forums/index.php?showtu>

--  
Hope  
this  
helps.  
Let  
us  
know.

Wes  
MS-MVP  
Windows  
Shell/User

In  
[news:uyfwK5MjHHA.4772@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:uyfwK5MjHHA.4772@xxxxxxxxxxxxxxxxxxxxxxxx),  
Trond  
Svendsen  
<trond@xxxxxxxxxxxxxxxx>  
hunted  
and  
pecked:

It's  
SVCHOST.EXE  
(PID  
1212)