

microsoft.public.windowsxp.perform\_maintain: lsass.exe takes cpu times for a few minutes

## Isass.exe takes cpu times for a few minutes

**Source:**

[http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.perform\\_maintain/2004-07/2096.html](http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.perform_maintain/2004-07/2096.html)

---

**From:** tomoseki ([tomoseki\\_at\\_discussions.microsoft.com](mailto:tomoseki_at_discussions.microsoft.com))

**Date:** 07/14/04

Date: Wed, 14 Jul 2004 02:04:01 -0700

Hi,

I posted this to security and administration group, but I had only one response so far.

Any advice are welcome.

Thanks,  
Tomoki

-----

When I logon to my XP Pro box, the logon process runs very slowly. Taskmgr shows that lsass.exe takes up a lot of cpu cycle like 70-80% for a few minutes. During this, everything goes very slowly. After that, everything works fine.

Windows XP Pro SP1, all updates are applied.  
The box is not in a domain.

NAV2003 is installed on the box, and scans the PC everyday. So, I don't think that it is affected by any viruses.

I looked into eventlog, but there is nothing special in application log and system log.

And when I logon to the box with other local accounts, it doesn't happen. Everything looks normal. Only my account seems affected.

I suspect that it's kind of a spyware or something like that, but I can't find any thing saying that how to fix this.

I was advised to install and scan spyware, so I did it.

I installed spybot and the latest rule, and scanned the box.  
It found some tracing cookies, and registry settings (DSO Exploit and Alexa related).  
I removed those things, but it doesn't change the situation.

I looked into task list again, and I found that one svchost.exe also take some cpu time. It looks like the svchost and lsass working together for something.

lsass.exe takes cpu times for a few minutes

microsoft.public.windowsxp.perform\_maintain: lsass.exe takes cpu times for a few minutes

below is the output from tasklist.exe /svc :

```
svchost.exe 952 AudioSrv, Browser, CryptSvc, Dhcp, dmserver,  
            ERSvc, EventSystem,  
            FastUserSwitchingCompatibility, helpsvc,  
            HidServ, lanmanserver, lanmanworkstation,  
            Messenger, Netman, Nla, RasMan, Schedule,  
            seclogon, SENS, ShellHWDetection, srservice,  
            TapiSrv, TermService, Themes, TrkWks,  
            uploadmgr, W32Time, winmgmt, wuauaserv, WZCSVC
```

Again, it only affects my local account.

Some more information.

I recently write some codes that use com+, com+ catalog, com+ events, com+ instruments, msmq, event tracing for windows.

Also, I applied group policy setting to disable windows messenger.

I don't remember anything else that likely affects the system behavior..

Any comments are welcome.

-----

Thanks,  
tomoki