

Windows XP SP2 and Windows Server 2003 SP1 TCP-IP Connections

Mark E. Donaldson

Starting with Windows XP SP2 (and Windows Server 2003 SP1 beta as well), Microsoft throttles the concurrent outbound half-open TCP connections per second -- apparently in the name of security. Pre-Windows XP SP2 systems allowed basically unlimited simultaneous outbound TCP connections, but with this new "enhancement," only 10 of those connections per second are allowed. This may be suitable for regular Windows users, but it hampers us security folks who use programs that open multiple TCP connections simultaneously, such as port scanners and vulnerability assessment tools.

Understanding the Limitation

We've known about the limitation on TCP connections for quite some time, but many security professionals (myself included) haven't paid a lot of attention to it. However, I learned about its effects the hard way not long ago while scanning a fairly large number of workstations on a client's network. The vulnerability-scanning tool I was using is normally very responsive, but it appeared to have lost its get-up-and-go that particular day.

I started my scans -- and waited. And waited, and waited. With minimal responses and no completion even after several hours, I finally stopped the tool during the process thinking perhaps it had just hung up. I rebooted and launched the vulnerability scanner again to no avail. I then started tweaking its scanning delay and query timeouts -- still the same sluggishness.

I started digging around on the Internet and stumbled across several postings about the exact problem I was experiencing. Apparently, Microsoft hard-coded this limit into the TCP/IP stack in a file called `tcpip.sys` that's located in `c:\windowssystem32\drivers`. Thankfully, a hacker by the name of LvlLord has created a hack for this very issue in a program called Event ID 4226 Patcher. This program changes the connection limit by a factor of five (from 10 to 50) by default -- likely more than enough for most tools you'll be using. You can also make the changes manually yourself by following the instructions here.

Just download the patcher and execute it. It will automatically find the windows directory and ask, if it should increase/decrease. For higher values, please check the help with parameter `/?`. After a successful patch, the new `TCPIP.SYS` will be automatically installed. After that, the computer should be restarted.

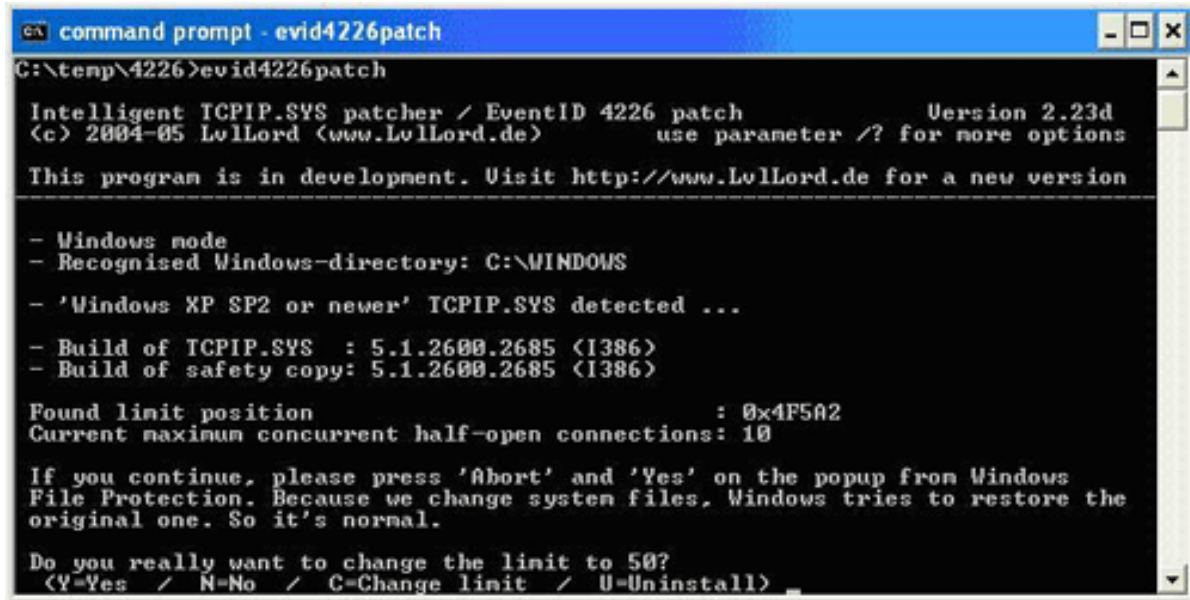
As a side note, had I looked through my event logs, I would've seen that something was going on. With this new "enhancement," Windows will record a warning in the local system event log if a local application goes over the TCP connection limit. The new log entry is Event ID 4226: *TCP/IP has reached the security limit imposed on the number of concurrent TCP connect attempts*. Check your event logs if you suspect something is going on -- you may be surprised by how often it occurs.

Making the Changes

If you don't want this Microsoft-imposed limitation on your TCP/IP stack, all you have to do is run Event ID 4226 Patcher's executable `EvID4226Patch.exe`. It's as simple as downloading it, unzipping it and running it as shown in Figure 1.

Windows XP SP2 and Windows Server 2003 SP1 TCP-IP Connections

Mark E. Donaldson



```
command prompt - evid4226patch
C:\temp\4226>evid4226patch

Intelligent TCPIP.SYS patcher / EventID 4226 patch          Version 2.23d
(c) 2004-05 LollLord (www.LollLord.de)                    use parameter /? for more options

This program is in development. Visit http://www.LollLord.de for a new version
-----
- Windows mode
- Recognised Windows-directory: C:\WINDOWS
- 'Windows XP SP2 or newer' TCPIP.SYS detected ...
- Build of TCPIP.SYS : 5.1.2600.2685 (I386)
- Build of safety copy: 5.1.2600.2685 (I386)

Found limit position : 0x4F5A2
Current maximum concurrent half-open connections: 10

If you continue, please press 'Abort' and 'Yes' on the popup from Windows
File Protection. Because we change system files, Windows tries to restore the
original one. So it's normal.

Do you really want to change the limit to 50?
(Y=Yes / N=No / C=Change limit / U=Uninstall)
```

Figure 1.
Simply download, unzip and run Event ID 4226 Patcher.

When running this program, you'll notice the default setting for maximum connections is 10. The program will prompt you to change it to 50. You have to press "Y" to proceed and "Y" again to have it rename tcpip.sys until the patching process is complete. Windows File Protection will likely throw up a warning about files being replaced by unrecognized versions, but you can simply click Cancel and ignore the message.

During the patching process, you can also press "C" to change the maximum concurrent connections to anywhere from 10 to 16,777,214. Go with the default of 50 first and see how that works for starters. Just keep an eye on your system log for 4226 warnings. I've recently experienced these warnings in my system log, so I'll likely be bumping up my setting. Just be careful, since raising it too high may cause problems with your local system or the systems you're testing.

Be Forewarned

This tcpip.sys hack doesn't come without a price -- you've got to modify a Windows system file, which Microsoft would surely frown upon when it comes time for support. Therefore, perform this hack at your own risk. Having said that, I haven't found this to be an issue since the Event ID 4226 Patcher makes a backup copy of your original tcpip.sys file and even has an uninstall feature that will reverse its actions if you need to go back. If you choose to go the manual route, be sure to make your own tcpip.sys backup.

This hack is not necessarily for the faint of heart, but if you're performing security assessments, I'm sure you understand the logic and value this offers. Enjoy that extra time you'll undoubtedly end up with. You might just buy enough time to learn another security tool you can't live without.