

RE: automatic updates and firewall

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windowsupdate/2005-10/msg00267.html>

- *From:* "Qrystal" <Qrystal@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 11 Oct 2005 06:03:15 -0700
-

I too would love to hear the answer to this question. I've been trying to figure out for a few weeks now (ever since I started using XP) what to do about this.

As it stands, I have done the following:

– allowed svchost access to the IP address ranges for microsoft (207.46.0.0 to 207.46.255.255) and hotmail (64.4.0.0 to 64.4.63.255), since the updates seem to occasionally be coming through there (I do not have hotmail set up as my mail service or anything ... I hope I'm not being too trusting here.)

– denied svchost access to the IP address ranges for Level3, Savvis, Qwest, and possibly a few others, even though my research into this question seems to indicate that these sites may be being used to alleviate the strain on microsoft's own servers (something about "footprint"?). I'd really like to know if these sites are officially sanctioned by microsoft, and whether there's any possibility that a malicious dll may be using svchost to contact those sites (if I understand correctly what svchost does). I refuse to blindly open these IP ranges when I'm not entirely sure if it's windows update that is trying to contact them (even Process Explorer* doesn't show me which svchost is trying to connect unless I allow the connection to take place). It would be really nice if there was some sort of authentication required that identifies the communication as belonging to a microsoft process.

– I have my firewall ask me about other sites, and I amend the above two lists (usually adding to the "denied" addresses, unless there's something that explicitly says Microsoft on it).

I just read somewhere that windows update likes to try to update itself every 22 hours maximum, which explains why it seems to like to attempt it every morning when I turn on my PC. So if I want to allow this on a particular day, I will toggle my firewall rule for the "footprint" servers to allow connections for a few minutes, while watching via Process Explorer* to make sure it's only windows update that's going on.

With the above settings, I'm hoping I'll get notification of the crucial updates directly from Microsoft, and then if there's something to download I just have to toggle the "footprint" firewall setting before proceeding (the

RE: automatic updates and firewall

update site "hangs" unless I do this). I would prefer to let this all happen on its own, like my antivirus and antispyware programs --- but Microsoft had to make things difficult by using svchost.exe instead of something like wuauclt.exe that could be explicitly allowed to connect on its own.

But what can I do. I'm just a stubborn Windows user who is demanding to know what's going on behind my back.

* FYI: Process Explorer can be found at <http://www.sysinternals.com/Utilities/ProcessExplorer.html> --- it's free! Microsoft refers to it fairly often in its support pages, although it's quick to point out: "Except for our own products, Microsoft does not endorse or recommend this product over others in the same area." (rofl!)

"Mike Brown" wrote:

> "Marcin Barczynski" wrote:
>> I don't want to allow svchost to connect all hosts on all ports.
>>> How to configure firewall to allow automatic updates, but nothing more
>>> than really needed (I mean there are no unnecessary ports open and no
>>> unnecessary applications allowed).
>
> 4 people rated this post helpful, but there is nothing helpful in it. What's
> the answer to Marcin's question? It would be nice to be able to configure my
> personal firewall to allow Windows Update the access it needs, without
> allowing blanket access to svchost.
>
>
>

-
- Prev by Date: [**Re: Keyboard**](#)
 - Next by Date: [**Re: Windows Update and Windows 2000SP4 error**](#)
 - Previous by thread: [**Re: Windows Automatic Update Fail, After KB892130 Installed**](#)
 - Next by thread: [**Re: Windows Update and Windows 2000SP4 error**](#)
 - Index(es):
 - ◆ [**Date**](#)
 - ◆ [**Thread**](#)