

Re: Auto-Updates for production servers

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.general/2007-10/msg01380.html>

- *From:* Brian Kitt <BrianKitt@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 29 Oct 2007 19:50:01 -0700
-

Sorry Anthony, you misunderstand the problem. I totally agree with keeping the servers up to date. Every Friday night, or whatever, is perfect.

HOWEVER, that is not what I am asking about.

They have the actual Windows Auto-Update on which applies all updates on an 'as released basis' from Microsoft. In other words, updates go on production servers, and nobody, not even them, have any idea which updates went on or when. Since auto-updates are on, the 'you need to reboot your server now' function keeps trying to reboot servers. For example, every time we log on to terminal services, we are prompted to reboot because of auto-updates. However, we don't have authority to reboot, so the box is grayed out. We just have to cancel the prompt. This prompt comes up every 10 or 15 minutes. There are days when I will work for 10 hours through terminal services, for every day of the week, so there are times, that for 40 or 50 hour work week, I am canceling that dang prompt every 10 minutes. It is not unusual that I may have to tunnel through 2 or 3 levels of terminal services, so take the every 10 or 15 minutes times 2 or 3.

To me, this is down and out wreckless to just apply updates to production without any knowledge whatsoever of what is being applied.

"Anthony" wrote:

Hi Brian,

I hope you won't mind advice that contradicts your presumed views.

When Microsoft or any software vendor discovers a flaw that can be exploited, they need to fix it.

If you don't apply the fix, you are vulnerable from that time on because everyone knows what the flaw is.

You can test the fix to see if it breaks anything, but you still need to apply it even if it does.

So really it could be a responsibility of the developers to be aware of fixes, maintain a testing environment and identify what to do if a fix breaks their software. They would then need to deploy their own patch within a week or two. If they object to having to test, it demonstrates that it is really an argument about who should do the work rather than whether it

Re: Auto-Updates for production servers

should be done.

The only way to avoid patching, or to postpone it till the developers are ready, is to maintain a sealed environment. You can do this as follows:

- run the