

# Re: Windows XP auto updates stinks!!

---

*Source:*

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2006-10/msg05610.html>

---

- *From:* "cquirke (MVP Windows shell/user)" <[cquirkenews@xxxxxxxxxxxxxxxxx](mailto:cquirkenews@xxxxxxxxxxxxxxxxx)>
  - *Date:* Tue, 17 Oct 2006 01:12:33 +0200
- 

On Sun, 15 Oct 2006 11:49:29 GMT, kojaks43@xxxxxxxxxxxxxxxxx wrote:

On 11-Oct-2006, Bruce Chambers <[bchambers@xxxxxxxxxxxxxxxxx](mailto:bchambers@xxxxxxxxxxxxxxxxx)> wrote:

Well, as it was never a good idea to let updates install automatically

True – it breaks the rule that you should be aware of every code change, and be the only entity that initiates such changes.

All "Critical" updates should be installed. These address serious issues that can affect a large number of computers. There will be only rare occasions when a Critical update will not apply. Of special importance are those that address security vulnerabilities.

The problem is that we are forced to choose the least worst of two bad practices; blindly applying patches as soon as possible, and not allowing any code changes we haven't personally tested and found to be safe. A malware can be created and released to exploit a new hole in less time than it takes to verify a new patch, and the malware has to just use one exploit whereas you have to test all patches.

If people had installed the available critical updates in July of 2003, the Blaster and Welchia worms would not have spread throughout the Internet the following month.

If the original code had been defect-free, we wouldn't have been running with that vulnerability for all the years from NT through to XP SP1. No-one ever mentions that bit of chronology, and we like to assume that because we only learned about the exploitability when MS told us about it when the patch came out, that no-one else could possibly have found and used in in the years past.

## Re: Windows XP auto updates stinks!!

In fact, until recently, many of us may have assumed all malware use of exploits could only start after an alert drew attention to the opportunity, and/or a patch provided the reverse-engineering required to figure out how exploits could be coded.

In the unlikely event that problems do develop, you can always use the Control Panel's Add/Remove Programs applet or a System Restore Point to uninstall the troublesome hotfix.

If your system can boot, and stay booted, that is...

For the "Recommended" updates, simply study the information provided to see if these updates apply in your specific situation. If they don't apply, or you're not experiencing the problem(s) addressed, you needn't install them. For instance, I have no use for WinXP's MovieMaker, so I ignore any updates to it.

That can be dangerous, as just because you don't use something, doesn't mean nothing else does. It would be OK if you could rip out what you don't need, but every new Windows version gives you less and less ability to do this. If you try, File Protection (or some update) may put the unwanted code back, and/or re-uhfault your settings.

There is an anti-competitive aspect to this, when you are forced to lose disk space and have to patch something you don't use because you'd rather use something else. You may decide that as you're forced to suffer the downside of having the bundled feature in the system, you might as well just use it... after all, everyone else does, right?

In general, though, I've found it best not to download the "Driver" updates from Windows Update

Absolutely. I'm not in favor of gratuitously changing low-level code that can prang the system (drivers) and/or cause the system not to boot (BIOS) unless I have a very good and very specific reason.

System code should be for keeps.

If you can't code for keeps, you should not be writing system code.

As I seem to be closer in ability to "Home User" I feel compelled to respond to your point of view. While I agree with all that you have said, AND I will no longer allow Automatic Updates to happen to my machine, I must point

## Re: Windows XP auto updates stinks!!

out that Microsoft's own policy is to recommend Automatic Updates.

Microsoft's other policies have in the past included...

- auto-running scripts in email "message text"
  - auto-running macros in "documents"
  - hiding file name extensions by default, including in Safe Mode
  - acting on hidden type info even if riskier than file .ext
  - automatically rebooting on system errors, even during boot
  - kill, bury, deny irreversible "fixing" of file system corruption
- ....so I don't feel obliged to trust their judgement.

What I want to do, is:

- download patches as soon as they are available
- install them when or if I choose to do so

There's an option that looks as if it does this, called "download updates automatically, but let me choose when to install them" - but the ones you UNcheck to NOT install, get automatically installed when you shut down XP SP2. The logic seems to be: "Why would you not want to install these brand new bits of code that we need to foist on you because the last time we tried to write this code, we screwed up?"

My logic is as follows: By not installing patches immediately, I run the risk of being unable to safely connect to the Internet for fear of being exploited through the defect I would now want to patch.

So I want to be able to cut off Internet access, install the mothballed patch I had already downloaded before the attacks started, and then I can connect once I'm patched.

I can select those updates I wish installed, and I probably would IF, the description of the update was written using language even closely approximating my native one. I am not an Alpha Geek.

MS update documentation comes in two speeds: 3rd gear, and Neutral.

You either get such generic info as to be useless ("an attacker could run code on your system") or you get the kind of info that may leave me wanting top gear, while you wish you could take off in 1st :-)

Yes, you are correct, I should learn more.

How much can any of us learn?

"we'll patch it later" is simply not a tenable system, and it scales very poorly indeed. We now have more new patches a month than we may

Re: Windows XP auto updates stinks!!

Re: Windows XP auto updates stinks!!

have had new malware per month, and that means MS have the same sort of ongoing event-driven urgent development load that av vendors face (at the very least... as patches have to work when retrofitted into production PCs that diverge from the fresh-install state).

Consider:

- you install the OS
- you install an incompatible app
- the app breaks
- you uninstall the app
- you cuss the app vendor for not working with the OS

Now, consider:

- you install the OS
- you install an app, and it works
- the OS patches itself
- out of the BlueSoD, the app breaks
- you have no idea why
- by now, you have crucial data that needs the app
- can you blame the app vendor this time?

Specifically, can you blame the app vendor for being incompatible with OS code that did not exist when the app was written, tested and sold?

...it is easier to follow the recommendation of the company that made the operating system. Would they intentionally want to harm me or my machine?

Intention is only part of it. Are they compitent to be trusted not to harm you by accident, when the only reason you have to allow automatic patching in the first place is because they fail this trust so often that you simply can't keep up with testing all the fixes?

We trust computing because we can't trust computing. Great.

The chilling thing is, it doesn't get better when you change software vendors or development models. At best, you may get a temporary respite while small market share means fewer and slower malware uptake of generally the same number of exploit opportunities.

-----  
Drugs are usually safe. Inject? (Y/n)  
-----

Re: Windows XP auto updates stinks!!