

Agnitum Security Insight Monthly Newsletter

Software updating as a security measure: Not a universal solution, but definitely an important element

Preface

We're all aware of the need for timely updates and patching for our computers, but how can we be sure it's really making our systems more secure? What would happen if we skipped one or more patches? In this issue of Security Insight, we'll give you all the information you need to help you decide if patching is worth the time and effort, and whether your system will be more vulnerable to hacker attacks if you don't patch.

What updating is intended to do:

By updating and patching programs on your PC, you achieve two goals:

1. Your software is more up-to-date, which should improve both performance and stability.
2. Your software is less vulnerable to attack and therefore more secure.

The first goal is quite straightforward: you get updates that are designed for your computer's current hardware and software configurations, so the updated programs will run more effectively and smoothly on your PC. This approach ensures fewer errors and malfunctions, and at the same time lessens the time it takes to execute a particular task—for example, a game update that is designed to increase the frame refresh rate.

The second goal is easy to understand but harder to measure. The theory is that the update plugs existing holes in your software, removing vulnerabilities so the software becomes safer and more resistant to intrusions and hijackings. But, unless you are a security professional, it's difficult to gauge the effectiveness and reliability of those security updates. Many people are starting to ask: "Do I really benefit by installing these security updates?"

Below, we'll try to answer this very reasonable question, concentrating on security updates but always keeping in mind that performance and stability updates are almost as important to the overall health and reliability of your system.

Types of security updates

Security updates can be broken out into four main types:

- 1) Operating System (OS) updates
- 2) Updates to software embedded into the OS
- 3) Device driver updates
- 4) Application and other third-party software updates

Let's address each of these areas in turn, as the risks and rewards for updating or not updating each is somewhat different.

1) Operating System (OS) updates

The most widespread operating system in use today is Windows in its XP interpretation. Every month, multiple updates to its internal services, engine design, embedded components, proprietary drivers and small utilities are issued on so-called "Patch Tuesday." These updates fix problems with connection protocols, repair the kernel to reflect the latest security standards and apply adjustments to existing security settings and environment configurations—all with the intention of increasing the security of the core software, the PC's operating system.

All too often, we've seen a spike in the number of virus and worm epidemics that can be directly linked to people's complacency and disregard for prompt updates to their operating system. Such complacency is

the trigger for computers all over the world becoming compromised. The examples are wide-ranging, and the results, unfortunately, can be quite drastic. You probably remember the Windows Metafile (WMF) episode at the end of last year: a flaw in the way Windows processes some graphics file formats was uncovered, which led to attackers being able to create special, exploitable graphics that remotely executed arbitrary code on unpatched systems.

The vulnerability affected not only Microsoft-made products (e.g., Outlook and Internet Explorer), but also third-party applications that relied on shared Windows Metafile (WMF) and Enhanced Metafile (EMF) graphics-rendering engines to display images. The net result was that any infected image opened up on a computer (either by unwittingly visiting a website hosting the malicious graphics or by viewing an email containing it) would automatically cause a malware download to take place.

Although Microsoft was quick to remedy this problem, people were slow to update their systems and close down this vulnerability. So a large number of viruses and other malware programs appeared that exploited the flaw and infected many hundreds of thousands of computers. Only then did people realize that applying security patches might be a good idea.

Windows is such a complex and all-encompassing piece of software that it has many services (complementary small programs) purposely left running in the background by default. These programs serve the requirements of people who use sophisticated software configurations in their work (most commonly for multi-user, domain controller environments). Most home PC users will never need these services, so it's quite safe for home users to disable them. Plenty of valuable information on running and often unneeded services can be obtained from these renowned Internet sources: PC Flank (direct link http://www.pcfank.com/art52_3.htm) and Black Viper (temporarily unavailable, archive contents available at <http://web.archive.org/web/20041128084144/www.blackviper.com/WinXP/servicecfg.htm>)

Some of these services use the network to communicate, so they open up their own connection ports and listen to commands from a remote machine, communicating data over those channels whenever a legitimate link is established. When such services are found to have flaws or vulnerabilities (either through an in-house investigation or as a result of the work of an independent security researcher), all those communication channels present a very tempting target for hackers to take over vulnerable machines and invade networks. This avenue has been used for exploits many times in the past and will no doubt continue to be used until Microsoft takes action to prevent it.

Because Windows is so complex, it is almost impossible for Microsoft to consistently issue patches quickly; a great deal of testing and QA must be done to ensure that the patches don't break any other programs. So users can never be sure how many security vulnerabilities have **not** been addressed in any particular patch issue (and are open to exploit by the hacker community). Beyond this, there is also a black market for Microsoft vulnerabilities, where unscrupulous individuals sell their discoveries to gangs of cybercriminals—without, of course, Microsoft's knowledge.

You can access the Automatic Updates tab to configure how you want to receive your Windows XP updates through the My Computer | Properties window. MacOS and Linux updates also can be retrieved and applied automatically—for instructions on updating these operating systems, see the appropriate Help file entry on your computer.

2) Updates to software embedded into the OS

OS-embedded software encompasses programs that are included in the package alongside the operating system itself. For Windows, most of these programs are designed by Microsoft, so it's Microsoft's responsibility to keep them secure and update them when necessary.

Microsoft has made great strides in that direction, but nothing is 100 percent in the software business. Microsoft's programs are not the exception (but rather the rule), and security defects are often found. Stories of new vulnerabilities in its browser software (Internet Explorer), built-in email client (Outlook Express) and multimedia player (Windows Media Player) pop up in the news almost every month. So it's important to update all those Internet-enabled Microsoft applications using the Automatic Updates

procedure noted above.

3) Device driver updates

Device drivers are small programs that control how your installed hardware (network adapter, graphics card, sound card, etc.) works. By installing the most recent drivers, you not only enhance performance and remove stability issues, but also have the opportunity to plug any security holes.

Not long ago, a [case](#) was reported in which Intel Centrino platform drivers were found to have a flaw that opened up access to the affected computer's wireless LAN, enabling attackers to remotely execute code on Centrino-based notebooks. Users of such computers were advised to quickly apply the corrective patch. These types of flaws are appearing more often. As wireless connectivity and high-speed Internet access continue to expand, users of telecom devices such as modems, WiFi adapters and routers should stay alert and consult the device manufacturers' sites once in a while to ensure they have the latest device drivers installed.

4) Third-party software updates

Third-party applications are those whose developers differ from the host operating system developer. While most people use a central core of Windows applications, programs like Adobe Acrobat Reader, Firefox browser, Skype VoIP software or Google Toolbar can be found on many Internet-enabled home computers. These and other programs, because they are popular and in wide use, have experienced vulnerability issues just as Microsoft has, prompting the developers to issue patches.

The general rule with any third-party programs, especially since most of them are using the Internet to operate, is to leave the automatic updating enabled and run those programs only when they are needed.

The downside of security updates

Along with the positive effects of updating, some downsides do exist. Some programs, for example, may temporarily lose Internet accessibility or have part of their functionality switched off. But these occurrences are quite rare and the developer of the application in question will usually provide users with a fix. It's also another good reason to register your software with the developer—so they know where to find you when they need to send you important information.

Useful things to do and have along with updating

Even if you're closely following update recommendations and you regularly update your software, there are a few additional steps you need to follow:

1. *Install a quality personal firewall*, such as Outpost Firewall Pro, that can close your computer's connection channels and protect your data from the initiators of unauthorized or otherwise unnecessary Internet connections;
2. *Do not run unknown programs*—if you don't recognize the program or do not trust its creators, use Internet search tools to do a little research on the company and the program before you allow the program to run on your system;
3. *Do not open suspicious file attachments* from unknown senders, and don't browse disreputable web sites.

Software most prone to security issues

1. All Windows services that use remote access functionality (Server Service, Telnet, Remote Desktop and others)
2. All programs bundled with Windows that access the Internet (IE, Windows Messenger, others)
3. Any third-party software that relies on Internet access functionality (browsers, players of remote multimedia content, etc.)

Conclusion

Security updating is one of the key maintenance procedures you should undertake regularly on your computer. The benefits of having an updated, well-configured system far outweigh the time it takes to run the updates. Considering that you can do most updates automatically in the background, there's really no excuse for not having a properly patched and smoothly running PC.

Useful Links:

- Secunia vulnerability reporting service — <http://secunia.com>
- Microsoft Security Bulletin (<http://www.microsoft.com/technet/security/current.aspx>) — one-stop information on the latest Microsoft security developments
- Windows Update service — <http://windowsupdate.microsoft.com>
- Software updates for Microsoft Office products — <http://www.officeupdate.com/>

by Igor Pankov,
Agnitum Ltd.
www.agnitum.com

Press contacts:
pr@agnitum.com

To sign up for the free Security Insight monthly newsletter
Please go to www.agnitum.com

[Read all Security Insight Articles](#)