

Using Windows Update for Windows NT

Contents

Introduction	1
Before You Begin	2
Downloading and Installing the Windows Update Components	2
Maintaining a Secure Computing Environment	6

Introduction

This document provides instructions on updating Windows NT with the necessary patches. It is very important to update your operating system software in order to plug up any existing vulnerabilities and help protect your system from computer virus attacks. This is especially the case if you just bought a new computer or recently reinstalled your operating system.

You need to perform this procedure regardless of whether or not you have been infected with a virus or worm.

How the Procedure Works

- You will be installing components from Windows Update in a specified order. The reason for this is that some components will overwrite the other components if they are installed in the incorrect order.
- If “Already Installed” appears to the right of any of these components, then that component is already installed on your computer and you will not need to install it again. (You can display the installed updates by clicking **Show Installed Updates** from Microsoft’s **Windows Update** Web page.)
- After you perform each install, you will need to reboot your computer.
- Toward the end of this procedure, you will be given the opportunity to install optional components. If you decide not to install these components, you will not affect the vulnerability of your computer.

Before You Begin

The following are required before you can perform this procedure:

- High-speed Internet connection (e.g., Ethernet connection)
- Internet Explorer (IE) 5.x

If you do not have IE 5.x or have an older version of IE, you will first need to install IE 5.0 Service Pack (SP) 2 or higher. However, many versions of Windows come with earlier versions of IE that may not be able to view the Microsoft Web site.

The alternate way to install IE 5.0SP2 is to do the following:

1. Install Netscape 4.77, which comes with the AcIS Internet Software CD (more information at <http://www.columbia.edu/acis/software/cd>).
 2. From Netscape, go to <http://www.microsoft.com/windows/ie> and then download and install either IE 5.0SP2, IE 5.5SP2, or IE 6.0.
- 70 MB of free disk space
 - Windows NT CD
 - Microsoft Office CD (If you are updating Microsoft Office, versions XP and 2000 require the CD)

Downloading and Installing the Windows Update Components

Important: Do not install the following updates:

- Outlook Express 5.0 or 6.0
- Visual Basic Scripting Support

These tools seem harmless; however, they expose your system, and leave your system vulnerable, to possible attacks. Or, to put it another way, each tool is a “wolf in sheep’s clothing.”

Step 1: Install the Service Pack

A service pack is a downloadable update to your software (e.g., Windows NT) that fixes existing problems (e.g., vulnerability to computer viruses) or provides product enhancements. Microsoft’s **Windows Update** Web page explains the product updates that are available as well as how to download and install the updates.

There are many patches that are not supplied as part of Service Pack 6a (the service pack that you will need to install). Microsoft has stated that they will not issue further service packs for Windows NT 4.0. Nevertheless, you will need to make sure that the service pack is installed.

1. Go to the **Windows Update** Web page at <http://windowsupdate.microsoft.com>.
2. Click **Product Updates**. You will need to accept an Active X control here, which allows Microsoft's web site to check your version of Windows and which updates you need to install.



Windows Update scans your system to see what you have installed and provides you with a list of suggested components.



3. From the **Select Software** Web page, choose the following (located under **Recommended Updates**):

- *Windows NT 4.0 Service Pack 6a (128-bit strong encryption)*

4. Click **Download**.

RECOMMENDED UPDATES

- Windows NT 4.0 Service Pack 6a (128-bit strong encryption)**
454 KB/ Download Time: < 1 min
Windows NT 4.0 Service Pack 6a includes the most recent updates and enhancements to Windows NT Server 4.0 and Windows NT Workstation 4.0. Service Pack releases are cumulative, so Service Pack 6a contains all previous Service Pack fixes and any new fixes created after Service Pack 5. Note that the actual download will be anywhere from 11-32Mb depending on the actual files on your current machine. **WARNING:** To avoid problems, including possible data loss, if you use both Microsoft Outlook and Computer Associates Inoculan, you should verify that you are using the latest version of the Inoculan drivers before installing SP6a. **NOTE:** The 128-bit release of SP6a is eligible for export from the U.S. to all customers worldwide, except to US embargoed destinations. Please see the Read This First page for further details. [Read this first](#)

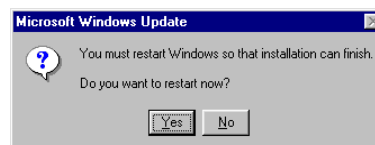
5. Verify that you have selected the correct components.
6. Click **Start Download** to begin the download and install process.
7. Click **Yes** to accept the license agreement.



Download and install the software shown above.

Note: You may be prompted to perform the installation. (If you are not prompted, Windows Update will perform the installation automatically.)

8. If this message appears, click **Yes** to restart your computer.



9. When your computer has rebooted, open an IE browser window and return to the **Windows Update** Web site.

Step 2: Install the Critical Updates

The updates listed below are the latest ones currently available at the time of writing this document.

Keep in mind that you will need to regularly install the latest Critical Updates. You can choose to be notified automatically of any new critical updates by installing **Windows Critical Update Notification** from the **Recommended Updates** section. (**Note:** You can install the notification update at any point in this procedure.)

1. If not already installed, choose the following from the **Windows Update** Web site (located under Critical Updates):
 - *Security Update, August 2, 2001*
 - *Security Update, May 24, 2001 (Internet Explorer 5.5, Service Pack 1)*
 - *Security Update, April 2, 2001*
 - *Security Update, January 17, 2000*
 - *Critical Update, September 10, 1999*
 - Any other items listed in the **Critical Updates** section.
2. Download and install the components.
3. Shut down and then restart your computer.

Step 3: Install the Internet Explorer and Internet Tools

If you have not done so already, you will need to upgrade to a secure version of IE by installing one of the updates listed in this procedure.

1. When your computer has restarted, open an IE browser window and go to <http://www.microsoft.com/windows/ie>.
2. Download and install one of the following versions of IE:
 - 5.01 SP2
 - 5.5 SP2
 - IE 6.0

If you install IE 6.0 but do not install Outlook Express 6.0, then you will also need to install the patches MS01-020 or MS01-027. You can obtain these patches from <http://www.microsoft.com/technet/security/current.asp>.

Note: AcIS recommends using Netscape 4.77 since IE contains many security vulnerabilities.

3. Install MS01-051, obtainable at <http://www.microsoft.com/technet/security/current.asp>.
4. Shut down and then restart your computer.

Step 4: Install the Microsoft Office Updates

Microsoft Office, especially Outlook, also has many security vulnerabilities.

1. When your computer has rebooted, open an IE browser window and return to the **Windows Update** Web site.

Warning: Before you install any updates, you must disable your anti-virus software. Anti-virus products may interfere with the installation in that some anti-virus programs do not allow certain types of content to be copied into the system. So if an anti-virus program is running (enabled), it may cause an installation to fail.

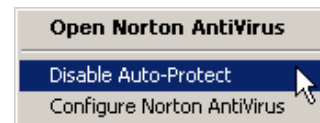
To prevent this, simply disable your anti-virus program before you install any updates.

If you have Norton AntiVirus, for example, you can disable the Auto-Protect feature by performing the following:

- a. Right click on the icon shown here, located on the far right side of the taskbar.



- b. Select **Disable Auto-Protect**.



An "X" appears over the icon.



2. If not already installed, install the following (located under **Recommended Updates**), just as you did for the Critical Updates:
 - *Non-Gregorian Calendar Update for Office 2000 SR-1*
3. Click **Product Updates** from <http://office.microsoft.com>. From the **Product Updates** Web page, install the service pack and all security updates. (You can click **Show Installed Updates** to display all the updates that are already installed on your computer.)

Note: You may be asked to insert your Microsoft Office CD to install the updates.
4. Download and install the update.
5. Shut down and then restart your computer.

Step 5: Install the Optional Updates

The following updates are not required to be installed.

Once you have installed all the above updates, you can also install the following optional updates:

- *NetMeeting 3.01*
- *Chat 2.5*

Step 7: Check to Make Sure There Are No More Critical Updates

After updating Internet Explorer, Office, and the Optional Updates, there may be more Critical Updates that only apply to systems that have installed those updates. Therefore, follow the instructions in Step 2, one more time.

Maintaining a Secure Computing Environment

The most important thing we can do to protect our computers after closing known vulnerabilities is to alter our online behaviors. When there are no vulnerabilities available to exploit via active attacks across the networks, the virus writers must wait for users to provide them an opportunity.

Behaviors You Should Adopt

It is vitally important that you adopt behaviors that will your computer if you have not been attacked by a virus, as well as be able to disinfect your computer if you have been attacked. Safe computing practices include:

- Check for software updates often and check news reports regularly for computer security issues. (See alerts links below in the Resources for Secure Computing section)
- Use virus protection software. (See <http://www.columbia.edu/acis/software/nav>)
- Make regular backups of critical data.
- Change your default settings in your network applications to disable scripting and other insecure “features” (Refer to the resources below for more information).
- Exercise extreme caution whenever receiving data from the Internet, no matter how trusted the source is. (Refer to the resources below for more information)

Resources for Secure Computing

The following list contains links to sites that help you protect your computer and keep you informed of the latest security-related news and tools.

- http://www.cert.org/tech_tips/home_networks.html
CERT’s guide to Home Network Security.
CERT is part of the Software Engineering Institute (SEI), a federally-funded research and development center operated by Carnegie Mellon University. CERT researches the causes and prevention of system security vulnerabilities and the improvement of system security, publishes information about security issues on its Web site, and develops information and training to incident response professionals and system administrators.
- <http://www.microsoft.com/technet/security/bulletin/notify.asp>
Free e-mail notification service that Microsoft uses to send information to subscribers about the security of Microsoft products. AcIS strongly recommends that you subscribe to this list.
- <http://www.microsoft.com/security>
Microsoft’s “Get Secure and Stay Secure” campaign . This site contains general information about Microsoft’s support of security issues.
- <http://www.microsoft.com/technet/security/tools/nt4exist.asp>

Provides baseline steps for securing systems using Windows NT 4.0 Enterprise Edition, Windows NT Workstation 4.0, or Windows NT Server 4.0.

- <http://www.microsoft.com/technet/security>
Microsoft's TechNet Web site. Contains links to security bulletins, the latest security news and technical information, discussion and chat groups, and troubleshooting tips and advice.
- <http://www.securityfocus.com/microsoft>
Contains security-related news, existing vulnerabilities, tools, and mailing lists.
- <http://www.microsoft.com/technet/security/current.asp>
The complete list of vulnerabilities for all Microsoft products.
- 1-866-PC SAFETY
Microsoft's toll-free security support line.
- <http://www.microsoft.com/technet/security/tools/mbrsrvcl.asp>
Windows NT 4.0 Workstation baseline security checklist
- <http://www.microsoft.com/technet/security/tools/nt4svrcl.asp>
Windows NT 4.0 Server baseline security checklist

For information on current threats and alerts:

- AcIS Alerts:
<http://www.columbia.edu/acis/>
- CERT's Advisories:
<http://www.cert.org/advisories/>

Microsoft Security Bulletins for Microsoft Products:
<http://www.microsoft.com/security/bulletins>