

Patch Management

In this chapter:

Types of Patches	550
Development of a Security Update	552
Patch Management in Six Steps	554
Best Practices	565
Additional Information	566

Patch management is required in a Microsoft network because software is not bug free. Security update and software updates must be periodically applied to the Microsoft Windows Server 2003, Windows 2000, and Windows XP operating systems to address security and functionality issues. Typically, updates are developed to resolve one of the following issues:

- **Testing for all the design possibilities is difficult.** As network designs become more complex, it is increasingly problematic to test every use of a Windows operating system component during initial testing and development of the operating system by Microsoft.
- **More legacy versions must be supported.** Although Windows XP is Microsoft's latest client operating system, not all customers will deploy it immediately. Customers will continue to use their common base operating systems, and these versions must be patched to protect against newer vulnerabilities.
- **Customers demand higher quality.** The quality bar rises as customers' network infrastructures change. More companies are connected to the Internet and are vulnerable to Internet attacks. This awareness drives higher the quality requirements for Internet-related components of Windows Server 2003.
- **Critical security issues must be fixed before the next product release.** Many issues cannot wait for a new version of the product to ship. Security issues, memory leaks, and other problems must be addressed immediately, especially if the vulnerabilities can lead to the compromise of a Windows 2000- or Windows Server 2003-based computer.

This chapter examines the following topics:

- **Types of patches** Not all patches are the same. This section looks at update formats and how Microsoft rates security patches.
- **Development of a security update** The development cycle of a security update illustrates what happens after a security vulnerability or bug is reported to Microsoft, before the security update is released to the public.
- **Patch management in six steps** The last section of this chapter proposes a methodology for patch management that will enable you to deploy patches successfully.

Types of Patches

Microsoft releases patches to provide updates to the Windows operating system and Microsoft applications. These patches fix known problems, or bugs, in an operating system or application and are shipped in the following formats:

- **Hotfixes** These updates address a single problem or bug encountered by a customer. They are developed in a short period of time and are released with less testing than other update types. Some hotfixes are referred to as *security fixes*. Security fixes differ from hotfixes in that the issues related to hotfixes are identified by the Microsoft Security Response Center (MSRC), rather than by Microsoft Product Support Services (PSS). Hotfixes are sometimes referred to as *Quick Fix Engineering (QFE) fixes*.
- **Emergency releases** These updates are designed to address issues that demand immediate attention, which include fast-moving virus attacks spreading throughout the Internet. An emergency release is tested to ensure it is suitable for broad distribution. These updates are placed on the Microsoft Windows Update site, which pushes updates quickly and automatically to millions of machines.
- **Monthly security updates** These updates provide fixes for recently discovered security vulnerabilities. Monthly security updates are released on the first Tuesday of every month. A notification of the upcoming updates is released a few days before the release of the update so that customers are aware of the upcoming month's updates. This process ensures that there is the smallest possible time between announcements of vulnerabilities and fixes being available, but also limits the amount of testing that can be performed by customers and partners because of the risk of information leaking to hackers.

- **Roll-ups** As the name suggests, a roll-up fix combines the updates of several security updates and software updates into a single update file. Roll-up fixes are run through more testing than single security updates or software updates, but are released more frequently than service packs (discussed next).
- **Software updates** These are any update, update roll-up, service pack, feature pack, critical update, security update, or hotfix that is used to improve or to fix a software product that is released by Microsoft Corporation.
- **Service packs** At fairly regular intervals, Microsoft produces a collection of all software updates released since the operating system's or application's release, including software updates released in previous service pack versions. These collections include fixes not previously released and can introduce new functionality. Service packs undergo extensive testing before their release to ensure no deployment issues exist. Microsoft might issue several beta releases of a service pack before the service pack is ready for the public.

When a security fix is released, MSRC issues a security bulletin that identifies the addressed vulnerability. In addition, a severity rating is applied to the security bulletin. If a security fix is a roll-up fix, the highest security rating of the individual security updates in the roll-up is applied.

Following is the ratings system implemented by the MSRC in November 2002:

- **Critical** A vulnerability that might enable an attacker to gain control of your computer through elevation of privilege or by allowing access to sensitive data. You should always apply critical-rating updates after testing. It is recommended that you apply a critical update within 24 hours of the update's release. If your organization is testing the update before deploying it on your network, it is recommended you deploy the tested update within two weeks of release.
- **Important** A vulnerability that might compromise the confidentiality, integrity, or availability of user data, as well as the integrity or availability of processing resources. You should always apply important-rating updates after testing. It is recommended that you apply an important update within one month of the update's release. If your organization is testing the update before deploying it on your network, it is recommended you take no longer than two months to apply the important update.

- **Moderate** A vulnerability that might be mitigated by good security measures, such as implementing a security baseline configuration or performing regular network auditing. This rating can also be applied to vulnerabilities that are difficult to exploit. You should evaluate a moderate update to determine whether the vulnerability addressed is relevant to your company before testing and deployment. It is recommended that you apply a moderate update within four months of the update's release or wait until the next service pack or roll-up that includes the patch. If your organization is performing extensive testing of the update before deploying it on your network, it is recommended you deploy the tested update within six months of release.
- **Low** A vulnerability that is extremely difficult to exploit or whose impact is minimal. You should determine whether a low-rating update is necessary before testing and deployment. It is recommended that you wait for the next service pack or roll-up that includes the low update. In some cases, you might decide not to deploy the update at all because it is not relevant to your organization.

Development of a Security Update

Once product support or the MSRC identifies the need for a security update, the development process begins. This process differs for operating systems and applications, but the same general method is used:

1. The vulnerability identified by MSRC or the bug identified by product support is escalated to the Microsoft sustained engineering team.
2. The sustained engineering team investigates the bug and assigns it to a developer. The developer might be on the sustained engineering team or might be the core team developer responsible for the operating system or application component.
3. The developer creates an initial security update. This security update addresses the vulnerability or bug but does not undergo testing other than that performed by the developer. This version of the security update is referred to as a *private*.
4. The private is sent to the customer who reported the problem to MSRC or to product support. The customer deploys the private to determine whether it corrects the problem.
5. If the customer reports that the bug is fixed, the sustained engineering team registers the bug against the next version of the operating system or application. This ensures that the next release does not include the same bug.

6. The private is provided to the core team developer responsible for the operating system or application component affected by the vulnerability. The developer reviews the security update to ensure no other issues exist.
7. When the developer completes her analysis, the security update is submitted to the build lab, which creates the security update and runs it through several build verification tests.
8. The security update is then passed through testers. The testers ensure that the security update works as expected. Because of time constraints, testing is not as extensive as the testing performed on service packs.
9. Localization teams review the security update to determine whether localized versions are required for different language versions of the operating system or application. If required, localized versions are developed.
10. The completed security update is released to customers. In addition, Microsoft releases a related security bulletin that applies a vulnerability rating and provides further descriptions of the vulnerability.

Once the security update is released to customers, the race begins between the organizations applying the patch and attackers attempting to create an attack that takes advantage of the vulnerability. An attacker will typically reverse engineer the patch to figure out what changes it made to the operating system or application to determine what is being fixed. Once determined, the attacker creates worm or virus code that takes advantage of the vulnerability. The attacker then releases the worm or virus—no testing is necessary because he has the entire Internet to test the worm or virus. Table 26-1 shows the time between when a security and an associated exploit were released for some of the more recognizable attacks in recent years.

Table 26-1 Time Between Security Update Release and Exploit Release

Attack	Patch Release Date	Attack Date	Number of days patch was available before the attack
Trojan.Kaht	March 17, 2003	May 5, 2003	49
SQL Slammer	July 24, 2002	January 24, 2003	184
Klez-E	March 29, 2001	January 17, 2002	294
Nimda	October 17, 2000	September 18, 2001	336
Code Red	June 18, 2001	July 16, 2001	28

Patch Management in Six Steps

It is recommended you use a six-step process for patch management. This process ensures that you apply the patches in an organized manner that prevents other applications on the network from failing. This is the recommended six-step process for patch management:

1. **Notification** You must be aware of new security updates or service packs to ensure that the updates or service packs are installed in a timely manner.
2. **Assessment** You must identify which computers on the network require the security update or service pack.
3. **Obtainment** You must acquire the security update or service pack installation files from Microsoft.
4. **Testing** You must test the security update or service pack before you apply it to all affected computers on your network to ensure that undesired effects do not occur.
5. **Deployment** You must deploy the security update or service pack to the affected computers in a timely manner, taking advantage of tools to assist in the deployment.
6. **Validation** You must ensure that the security update or service pack is successfully installed on all affected computers.



Note Other methodologies will work for patch management as long as they follow a systematic, repeatable process.

Step 1. Notification

The first step in patch management is being aware of when Microsoft releases security patches. When a security patch is released, Microsoft issues a security bulletin that details the vulnerability fixed by the security patch as well as a vulnerability rating so that you can assess whether to deploy the security patch immediately after testing.

One way to stay on top of releases is to subscribe to the Microsoft Security Notification Service, which you access at <http://register.microsoft.com/subscription/subscribeme.asp?ID=135>. The notification service sends you an e-mail message when a new security bulletin is released. If you desire even more timely information, consider subscribing to the Microsoft Security Bulletin Advance Notification announcement,

available at <http://www.microsoft.com/technet/security/news/bulletinadvance.aspx>. The advance notification provides e-mail notification of upcoming security bulletins and timely notification of any minor changes to previously released Microsoft security bulletins.



Note All e-mail messages from the Microsoft Security Notification Service are signed with a Pretty Good Privacy (PGP) key. The Microsoft PGP key is available at <http://www.microsoft.com/technet/security/bulletin/pgp.aspx>. You can verify the Microsoft PGP key by inspecting its fingerprint, which is 9502 BE22 B497 5112 FBEO BFC9 8ADE 1206 AA55 BC66.

In addition to the Microsoft Security Notification Service, several other notification services can inform you when new security issues arise for Microsoft Windows NT 4.0, Windows Server 2003, Windows 2000, and Windows XP:

- **NTBugtraq** The <http://www.ntbugtraq.com> Web site, hosted by Russ Cooper, maintains a mailing list that discusses security bugs and exploits in Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003.
- **United States Computer Emergency Readiness Team (US-CERT) Cyber Security Alerts and Bulletins** The National Cyber Alert System maintains its own mailing list that notifies participants when computer-related security problems arise. You can subscribe to the US-CERT Security Alerts (sent whenever a security alert is released) at <http://www.us-cert.gov/cas/signup.html#ta> or to the US-CERT Security Bulletins (weekly summaries of security issues) at <http://www.us-cert.gov/cas/signup.html#tb>.

Step 2. Assessment

Once you identify the release of a security patch, you must determine whether the vulnerability affects your company and whether your computers require the patch. As mentioned earlier, you can utilize the Microsoft security bulletin rating system to assist in this decision. If a security bulletin is rated as critical or important, you should consider immediately applying the patch once you have tested it.

After testing, you must identify which computers require patch application. In many ways, this is the most difficult part of patch management. Keeping manual records of which patches and service packs are applied to every network computer is not possible if you have a large number of computers. Sometimes just determining which operating system a computer is running is a challenge, never mind which service packs and security patches are applied.

Keeping an inventory of your systems assists you in planning patch deployment. By categorizing your computer systems, you can quickly identify how many computers are affected by a reported vulnerability. For example, if Microsoft releases a new security bulletin relating to a bug in Microsoft Exchange Server 2003, it will be useful to know how many instances of Exchange Server 2003 are on the network, as well as their physical location and which service packs and software updates are current.

By utilizing software, such as Microsoft Systems Management Server (SMS), you can create a detailed inventory of network computers. The inventory information should help you determine which service packs and software updates are applied to each computer.

Based on the inventory, you can categorize computers into common collections for deploying service packs and software updates. For example, creating a collection of all Windows 2000–based computers will assist in the deployment of the latest Windows 2000 service pack.

Step 3. Obtainment

Once you identify the computers you must patch, you must obtain the patches or service pack files. The online location you choose to download from will depend on several factors, including which application or operating system is affected by the patch, whether all network computers are connected to the Internet, and whether you have a service pack or software update deployment solution in operation.

The following locations are available for downloading service packs and software updates:

- Microsoft Windows Update (<http://windowsupdate.microsoft.com>)
- Microsoft Office Product Updates (<http://officeupdate.microsoft.com/>)
- Microsoft Download Center (<http://www.microsoft.com/downloads/>)

Microsoft Windows Update

The Microsoft Windows Update site is available for the download and application of Windows security updates, software updates, and service packs. In addition to downloading and installing patches, you can also use the Windows Update Catalog to download patches for future application. The Windows Update Catalog provides a searchable collection of updates that can be installed on Windows-based computers across your home network or corporate network. The Windows Update Catalog enables you to download service packs, security updates, and driver updates with-

out installing them on the local computer. Instead, the files are downloaded into a folder containing instructions for future application to one or more computers on your network.

Enabling the Windows Update Catalog By default, the Windows Update Catalog is not enabled when you connect to the Microsoft Windows Update Web site. To enable the Windows Update Catalog in Windows 2000 or Windows Server 2003, you must use the following procedure:

1. Open Microsoft Internet Explorer.
2. Open *http://windowsupdate.microsoft.com*.
3. In the leftmost pane of the Microsoft Windows Update site, click Personalize Windows Update.
4. In the details pane, enable the Display The Link To The Windows Update Catalog Under See Also option.
5. In the details pane, click the Save Settings button.

This procedure adds a link to the Windows Update Catalog in the left-hand pane of the Microsoft Windows Update site under the heading See Also.

For Windows XP, the process is slightly different:

1. Open Internet Explorer.
2. Open *http://windowsupdate.microsoft.com*.
3. In the leftmost pane of the Microsoft Windows Update site, click Administrator Options.
4. In the Update Multiple Operating Systems section of the Web page, click the Windows Update Catalog link.

Using the Windows Update Catalog The Windows Update Catalog enables you to find patches for Windows operating systems and hardware device drivers. You can download updates for specific operating systems, including the following:

- The 64-bit version of the Windows Server 2003 family
- Windows Server 2003 family
- The 64-bit version of Windows XP
- Windows XP family
- Windows 2000 family
- Microsoft Windows Millennium Edition (Me)
- Microsoft Windows 98

In addition to selecting the operating system version, you can choose to download localized versions of the updates by indicating the preferred language for the updates. You can search for updates based on the date they were posted to the Microsoft Windows Update Web site, the keywords in the update descriptions, and the type of update (such as critical updates, service packs, and recommended updates).

As mentioned, you can also use the Windows Update Catalog to download updated device drivers. You can select these device drivers based upon the type of hardware. For example, you can select network drivers by manufacturer, operating system, language, date posted, and specific keywords.

Once you select the operating system and device driver updates, you can download updates to your download basket. The Windows Update Catalog allows you to designate a local folder for downloads. The files are stored in the folder structure shown in Figure 26-1.

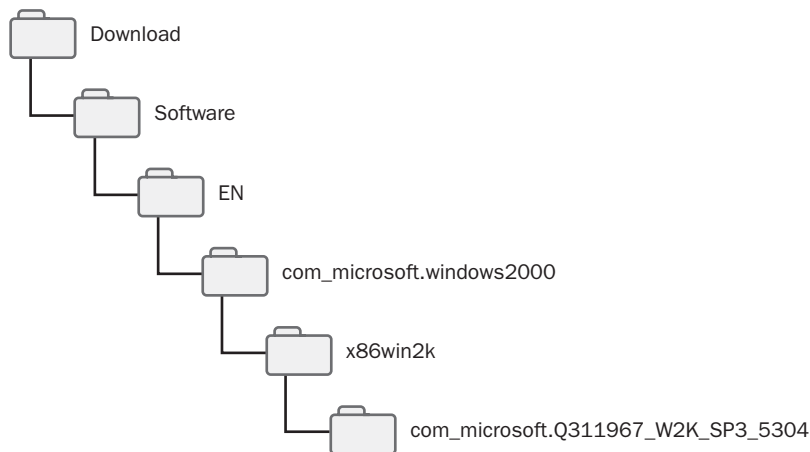


Figure 26-1 The folder structure created for the Windows Update Catalog

The folder structure created by the Windows Update Catalog depends upon whether you download a Windows operating system or device driver update. Below the folder you select as the download location—in this example, \Download—the Windows Update Catalog creates one of two folders. For operating system updates, a folder named Software is created, as shown in Figure 26-1. For device driver updates, a folder named Drivers is created.

Below this top-level folder, the next level of folders is based on the language selected. As Figure 26-1 shows, the English (EN) version of the update was downloaded. The next two levels of folders designate the update's operating system version. The example shown in Figure 26-1 is a Windows 2000 update designated by two folders: `com_microsoft.windows2000` and `x86win2k`.

The final folder designates the actual downloaded update. The update's name indicates the related Microsoft Knowledge Base article, the update's intended operating system, the update's service pack version, and a unique identifier number. As shown in Figure 26-1, the update relates to Knowledge Base article 311967, "Unchecked Buffer in the Multiple UNC Provider." The update is intended for computers running Windows 2000 and is included in Windows 2000 Service Pack 3. If the update is an updated device driver, the final folder's name is assigned by the updated device driver's manufacturer.

Microsoft Office Product Updates

The Microsoft Office Product Updates site provides updates, add-ins, extras, converters, viewers, and downloads for Microsoft Office 97/98, Office 2000, Office 2002, and Office 2003. The updates can be selected by individual Office software components or for all Office applications.

To download Office updates to your computer, use the following procedure:

1. Open Internet Explorer.
2. Open <http://officeupdate.microsoft.com>.
3. Select the Office product and version updates you want to download.
4. Select whether to download updates, add-ins, and extras or converters and viewers for the selected Office component.
5. Select the individual updates from the list of available downloads.



Note You also have the option to view downloads from other providers. The Microsoft Office Product Updates site also displays a list of third-party updates for the Office suite components.

The Microsoft Office Product Updates site does not download the update files into any specific folder structure. You must designate a custom location for the download.

Microsoft Download Center

The Microsoft Download Center enables you to search for other software and updates from Microsoft. As with Microsoft Office Product Updates, you must manually designate a download location.

The following update categories are available from the Microsoft Download Center:

- **Games** Includes trial versions and updates for games from Microsoft.
- **DirectX** Includes updates and the latest versions of DirectX. DirectX provides innovations in graphics, sound, music, and 3-D animation for gaming and graphics.
- **Internet** Includes updates for all Internet-based applications, such as Windows Messenger and Internet Explorer.
- **Windows (Security & Updates)** Includes security updates for any components of the Windows operating system. This includes service packs, Internet Explorer updates, and security updates.
- **Windows Media** Includes updates and codecs for Windows Media Player for various operating systems.
- **Drivers** Includes updated drivers for Microsoft hardware, as well as updates for common operating system components, such as Microsoft Data Access Components (MDAC).
- **Office and Home Applications** Includes updates for Office and other home applications, such as Microsoft MapPoint.
- **Mobile Devices** Includes updates for the Palm PC, Microsoft ActiveSync, and Microsoft Windows CE.
- **Macintosh & Other Platforms** Includes updates of software for Macintosh, Solaris, and Unix computers.
- **Server Applications** Includes updates for Microsoft BackOffice components, such as Microsoft SQL Server, Exchange Server, Microsoft Systems Management Server (SMS), and Microsoft SharePoint Portal Server.
- **System Management Tools** Includes updates for Windows management, including Windows Installer, the Microsoft Internet Information Services (IIS) Lockdown Tool, and Sysprep.
- **Development Resources** Includes updates for Microsoft Visual Basic, the Microsoft .NET Framework, and Microsoft Visual Studio.

Each download category presents a list of the 10 most popular downloads. You can also search for a download by specific products, technologies, and keywords.

Step 4. Testing

In an enterprise network, you cannot take the risk of deploying service packs or software updates without testing them in your environment. Testing ensures that the application of a service pack or software update does not create any undesired side effects.

To ensure that the testing is valid, consider implementing the following measures:

- **Deploy a test network.** A test network contains computers with the standard configuration used on your network. This allows you to determine if a security update or service pack causes issues with other applications installed on a standard desktop computer.
- **Implement a pilot project.** Service packs should be tested by a subset of your network computers. The subset will determine whether the service pack causes any issues on the corporate network for the affected computers.



Note Typically, you would perform pilot projects only for service packs, not for security updates or security roll-ups. But the decision is typically based on the security policies and previous experience of the organization applying the updates.

Once this initial testing is completed, you can start the deployment of the service pack or software update to all affected computers.

Step 5. Deployment

Once you download and test the necessary software update or service pack, you must install it on the affected computers. As mentioned earlier, you can determine the affected computers on your network by reviewing your computer inventory. The method you use to deploy a software update or service pack will depend on whether your company uses manual or automated distribution.



More Info This chapter discusses only the manual deployment of service packs or software updates. For detailed information on automating service pack or software update distribution, see Chapter 27, "Using Patch Management Tools."

Installing Service Packs

The easiest way to obtain the latest service packs for Windows Server 2003, Windows 2000, and Windows XP is to use the Microsoft Windows Update site at <http://windowsupdate.microsoft.com/> to download them. The available updates will include the latest service pack for your operating system.

If you are deploying a service pack to a large segment of your network, it might be better to download the Network Installation version of the service pack to reduce the amount of bandwidth consumed while downloading.



Note If you implement a patch management system, you might be able to download the network version of the service pack and deploy the service pack using only internal network bandwidth after the initial download.

The Network Installation download of a service pack includes all updated files for the selected operating system. You can extract the service pack files from the downloaded executable by running ***ServicePackName.exe -x*** (where *ServicePackName* is the name of the service pack file). Once you extract the service pack files, you can run **`\download folder\i386\Update\Update.exe`** to install. If you have not extracted the service pack files, run **`\download folder\ServicePackName.exe`**.

Alternatively, you can use the packaged `\download folder\i386\Update\Update.msi` file to deploy the service pack to computer accounts in a software installation Group Policy object (GPO). By assigning the Update.msi package to a GPO applied to an OU with computer accounts running the targeted operating system, you can deploy the service pack through Group Policy.

Installing Software Updates

All Windows Server 2003, Windows 2000, or Windows XP software updates—whether released prior to or since Windows 2000 Service Pack 3—are packaged in a format that automatically installs the service pack when you run the downloaded software update executable. The executable automatically extracts all files related to the software update and installs them. The following two subsections discuss the manual installation of software updates on computers.

Installing Software Updates Released Prior to Windows 2000 Service Pack 3

Software Updates released prior to Windows 2000 Service Pack 3 are installed by using Hotfix.exe. When you install a software update, you can use several command-line switches to customize installation. The available command-line switches for hotfixes released prior to Windows 2000 Service Pack 3 include the following:

- **/f** Causes all other programs to quit when the computer is shut down.
- **/l** Displays a list of all hotfixes currently installed on the computer.
- **/m** Performs an unattended software update installation.
- **/n** Prevents the computer from archiving previous versions of files replaced by the software update. (This switch prevents the uninstallation of the software update.)
- **/q** Performs the installation in quiet mode. (Quiet mode does not require user interaction.)
- **/y** Uninstalls the software update. (This option must be used with /m or /q.)
- **/z** Prevents the computer from restarting after installation.

When performing an unattended software update installation, you typically use the following command line:

```
Hotfix.exe /m /q /z
```

This command line allows the installation of multiple software updates in a single batch file.



Warning Hotfix.exe does not perform version control when you install multiple software updates. If you create a batch process that installs multiple software updates, you must ensure that the last line of the batch file is QChain.exe. QChain.exe ensures that if a file is modified by multiple software updates, the most recent version is maintained when the computer restarts. For more information on QChain.exe, see Knowledge Base article 296861: "Use QChain.exe to Install Multiple Hotfixes with Only One Reboot" (<http://support.microsoft.com/kb/296861>).

Installing Software Updates Released Since Windows 2000 Service Pack 3

Software updates released after Windows 2000 Service Pack 3, including those for Windows XP and Windows Server 2003, are installed by using the Update.exe program. The Update.exe program includes the QChain.exe functionality, eliminating

the need to run QChain.exe if multiple software updates are installed by a batch-file method. Update.exe is also used as the software update installation method for Windows XP software updates.

The following command-line switches are available when you install a software update released since Windows 2000 Service Pack 3:

- **-u** Performs the installation in unattended mode.
- **-f** Forces all other programs to quit when the computer shuts down.
- **-n** Prevents the archiving of previous versions of files replaced by the software update. (This switch prevents the uninstallation of the software update.)
- **-o** Overwrites original equipment manufacturer (OEM) files without prompting.
- **-z** Prevents the computer from restarting after the software update installation. (This option allows the application of multiple software updates without rebooting.)
- **-q** Performs an unattended installation but does not show the user interface during the installation process.
- **-l** Lists all software updates currently installed on the computer.

Step 6. Validation

Once you complete the software update installation, verify that it was installed successfully. Numerous methods to determine whether a software update is correctly applied to a computer exist, including the following:

- **Inspect the file system** When a software update is installed so that the previous versions of replaced files are archived, the archived files are stored in the %windir%\\$NTUninstallQ#####\$ folder, where ##### is the related Knowledge Base article number. If the folder exists, you can assume the software update was applied correctly. Be aware that this does not prevent the updated version from being replaced by an incorrect version at a later time, especially with software updates released prior to Service Pack 3 that do not have QChain.exe functionality.
- **Inspect the registry** When a software update is successfully installed, the installation program registers the software update in the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Hotfix\Q##### or \KB##### registry key, where ##### is the related Knowledge Base article. As with inspecting the file system, examining the registry does not detect whether updated files are later replaced.

- **Use software update diagnosis tools** To inspect the system for currently applied software updates and determine which software updates are required for your computer, you can use software update diagnosis tools, such as the Microsoft Baseline Security Analyzer command-line version executable Mbsacli.exe, Shavlik's hotfix network checker HfNetChk.exe (found at <http://www.shavlik.com>), and those found on the Microsoft Windows Update Web site (<http://windows.update.microsoft.com>). By inspecting the checksums on the updated files, these tools can determine whether the hotfix needs reapplication.



More Info For more information on using these patch management tools, see Chapter 27, "Using Patch Management Tools."

Best Practices

- **Subscribe to security update and service pack notification services.** Notification services assist you in identifying recently released security updates and service packs, enabling you to deploy the updates or service packs in a timely manner.
- **Assess your network to determine which computers require the security update or service pack.** A security update or service pack might not be applicable to all computers on your network. You must identify which computers will require the update or service pack.
- **Obtain security update or service pack installation files from download locations.** Depending on which operating system or application is affected by the security update or service pack, you must connect to the appropriate Web site to download the installation files.
- **Test the security update or service pack on test computers before performing a full deployment.** By performing a pilot deployment, you identify any issues that might arise with the security update or service pack installation. This prevents the security update or service pack installation from causing undesired side effects on the target computers or network.
- **Use the appropriate tools to deploy the security update or service pack.** The tools that you choose for deploying the security update or service pack will determine the administrative effort required for the deployment.
- **Validate the installation of the security update or service pack.** Once you complete the installation of the security update or service pack, you must ensure that the security update or service pack is installed correctly on the target computers.
- **Always have a rollback plan.** In some cases, a security update might not interact as expected with your organization's computers. Have a plan on how to roll back the changes and return the machine to the expected operating status.

Additional Information

- Microsoft Security Notification Service (<http://www.microsoft.com/technet/security/bulletin/notify.asp>)
- Microsoft Security Bulletin Advance Notification (<http://www.microsoft.com/technet/security/bulletin/advance.mspix>)
- Microsoft Security Response Policy and Practices (<http://www.microsoft.com/technet/security/topics/policy/msrpracs.mspix>)
- Microsoft Security Guidance Center: Patch Management Index (<http://www.microsoft.com/security/guidance/topics/PatchManagement.mspix>)
- Microsoft Security Bulletin Advance Notification Announcement (<http://www.microsoft.com/technet/security/news/bulletinadvance.mspix>)
- Microsoft Windows 2000 Hotfix Installation and Deployment Guide (HFDeploy.htm) (<http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/HFDeploy.htm>)
- Microsoft Windows XP Hotfix Installation and Deployment Guide (<http://www.microsoft.com/WindowsXP/pro/downloads/servicepacks/sp1/hfdeploy.asp>)
- Guide for Installing and Deploying Updates for Microsoft Windows XP Service Pack 2 (<http://www.microsoft.com/technet/prodtechnol/winxp/pro/deploy/hfdeploy.mspix>)
- Guide for Installing and Deploying Updates for Microsoft Windows Server 2003 and Windows XP 64-Bit Edition Version 2003 (HFDeploy.htm) (<http://www.microsoft.com/technet/security/topics/patch/HFDeploy.mspix>)
- Microsoft TechNet Security Web site (<http://www.microsoft.com/technet/security/default.asp>)
- “Managing Security Hotfixes,” by Paul Niser, *Windows & .NET Magazine* (July 2002) (<http://www.microsoft.com/technet/security/tips/sechotfx.asp>)
- *Security Operations Guide for Windows 2000 Server*, Chapter 5, “Patch Management” (<http://www.microsoft.com/downloads/details.aspx?FamilyID=f0b7b4ee-201a-4b40-a0d2-cdd9775aeff8&displaylang=en>)
- NTBugtraq Web site (<http://www.ntbugtraq.com>)
- United States Computer Emergency Readiness Team—Nation Cyber Alert System Web site (<http://www.us-cert.gov/cas/index.html>)
- “Patch Management Process” (<http://www.microsoft.com/technet/security/guidance/secmod193.mspix>)

- The following Knowledge Base articles:
 - ❑ 262841: “Windows 2000 Hotfix.exe Program Description and Command-Line Switches” (<http://support.microsoft.com/kb/262841>)
 - ❑ 296861: “Use QChain.exe to Install Multiple Hotfixes with Only One Reboot” (<http://support.microsoft.com/kb/296861>)
 - ❑ 810232: “Summary of Command-Line Syntax for Software Updates” (<http://support.microsoft.com/kb/810232>)
 - ❑ 824684: “Description of the Standard Terminology That Is Used to Describe Microsoft Software Updates” (<http://support.microsoft.com/kb/824684>)
 - ❑ 824687: “Command-Line Switches for Microsoft Software Update Packages” (<http://support.microsoft.com/kb/824687>)