Security Bulletin

Microsoft Security Bulletin MS06-057 - Critical

Vulnerability in Windows Explorer Could Allow Remote Execution (923191)

Published: October 10, 2006

Version: 1.0

Summary

Who Should Read this Document: Customers who use Microsoft Windows

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: Critical

Recommendation: Customers should apply the update immediately.

Security Update Replacement: This bulletin replaces a prior security update. See the frequently asked questions (FAQ) section of this bulletin for the complete list.

Caveats: None

Tested Software and Security Update Download Locations:

Affected Software:

- Microsoft Windows 2000 Service Pack 4 — Download the update
- Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2 — Download the update
- Microsoft Windows XP Professional x64 Edition — Download the update
- Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1 — Download the update
- Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems — Download the update
- Microsoft Windows Server 2003 x64 Edition — Download the update

The software in this list has been tested to determine whether the versions are affected. Other versions either no longer include security update support or may not be affected. To determine the support life cycle for your product and version, visit the Microsoft Support Lifecycle Web site.

Note The security updates for Microsoft Windows Server 2003, Windows Server 2003 Service Pack 1, and Windows Server 2003 x64 Edition also apply to Windows Server 2003 R2.

General Information

Executive Summary

Executive Summary:

This update resolves a newly discovered, publicly reported vulnerability. The vulnerability is documented in the "Vulnerability Details" section of this bulletin.

An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

We recommend that customers apply the update immediately.

Severity Ratings and Vulnerability Identifiers:

Expand table

Vulnerability Identifiers	Impact of Vulnerability	Windows 2000 Service Pack 4	Windows XP Service Pack 1 and Windows XP Service Pack 2	Windows Server 2003	Windows Server 2003 Service Pack 1
Windows Shell Remote Code Execution Vulnerability - CVE-2006-3730	Remote Code Execution\	Critical\	Critical\	Moderate\	Moderate\

This assessment is based on the types of systems that are affected by the vulnerability, their typical deployment patterns, and the effect that exploiting the vulnerability would have on them.

NoteThe severity ratings for non-x86 operating system versions map to the x86 operating systems versions as follows:

- The Microsoft Windows XP Professional x64 Edition severity rating is the same as the Microsoft Windows XP Service Pack 2 severity rating.
- The Microsoft Windows Server 2003 for Itanium-based Systems severity rating is the same as the Microsoft Windows Server 2003 severity rating.
- The Microsoft Windows Server 2003 with SP1 for Itanium-based Systems severity rating is the same as the Microsoft Windows Server 2003 Service Pack 1 severity rating.
- The Microsoft Windows Server 2003 x64 Edition severity rating is the same as the Microsoft Windows Server 2003 Service Pack 1 severity rating.

Note The security updates for Windows Server 2003, Windows Server 2003 Service Pack 1, and Windows Server 2003 x64 Edition also apply to Windows Server 2003 R2.

Frequently Asked Questions (FAQ) Related to This Security Update

Extended security update support for Microsoft Windows 98, Windows 98 Second Edition, or Windows Millennium Edition ended on July 11, 2006. I am still using one of these operating systems; what should I do?
Windows 98, Windows 98 Second Edition, and Windows Millennium Edition have reached the end of their support life cycles. It should be a priority for customers who have these operating system versions to migrate to supported versions to prevent potential exposure to vulnerabilities. For more information about the Windows Product Lifecycle, visit the following Microsoft Support Lifecycle Web site. For more information about the extended security update support period for these operating system versions, visit the .

Extended security update support for Microsoft Windows NT Workstation 4.0 Service Pack 6a and Windows 2000 Service Pack 2 ended on June 30, 2004. Extended security update support for Microsoft Windows NT Server 4.0 Service Pack 6a ended on December 31, 2004. Extended security update support for Microsoft Windows 2000 Service Pack 3 ended on June 30, 2005. I am still using one of these operating systems; what should I do?

Windows NT Workstation 4.0 Service Pack 6a, Windows NT Server 4.0 Service Pack 6a, Windows 2000 Service Pack 2, and Windows 2000 Service Pack 3 have reached the end of their support life cycles. It should be a priority for customers who have these operating system versions to migrate to supported versions to prevent potential exposure to vulnerabilities. For more information about the Windows Product Lifecycle, visit the following Microsoft Support Lifecycle Web site. For more information about the extended security update support period for these operating system versions, visit the Microsoft Product Support Services Web site.

Customers who require custom support for these products must contact their Microsoft account team representative, their Technical Account Manager, or the appropriate Microsoft partner representative for custom support options. Customers without an Alliance, Premier, or Authorized Contract can contact their local Microsoft sales office. For contact information, visit the Microsoft Worldwide Information Web site, select the country, and then click **Go** to see a list of telephone numbers. When you call, ask to speak with the local Premier Support sales manager. For more information, see the Windows Operating System Product Support Lifecycle FAQ.

What updates does this release replace?

This security update replaces a prior security update. The security bulletin ID and affected operating systems are listed in the following table.

Expand table

Bulletin ID	Windows 2000 Service Pack 4	Windows XP Service Pack 1	Windows XP Service Pack 2	Windows Server 2003	Windows Server 2003 Service Pack 1
MS06-045	Not replaced	Replaced	Not replaced	Not replaced	Not replaced

Can I use the Microsoft Baseline Security Analyzer (MBSA) to determine whether this update is required?

The following table provides the MBSA detection summary for this security update.

Expand table

Product	MBSA 1.2.1	MBSA 2.0
Microsoft Windows 2000 Service Pack 4	Yes	Yes
Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2	Yes	Yes
Microsoft Windows XP Professional x64 Edition	No	Yes
Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1	Yes	Yes
Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with Service Pack 1 for Itanium-based Systems	No	Yes
Microsoft Windows Server 2003 x64 Edition family	No	Yes

For more information about MBSA, visit the MBSA Web site. For more information about the programs that Microsoft Update and MBSA 2.0 currently do not detect, see Microsoft Knowledge Base Article 895660.

For more detailed information, see Microsoft Knowledge Base Article 910723.

Can I use Systems Management Server (SMS) to determine whether this update is required?
The following table provides the SMS detection summary for this security update.

Expand table

Product	SMS 2.0	SMS 2003
Microsoft Windows 2000 Service Pack 4	Yes	Yes
Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2	Yes	Yes
Microsoft Windows XP Professional x64 Edition	No	Yes
Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1	Yes	Yes
Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with Service Pack 1 for Itanium-based Systems	No	Yes
Microsoft Windows Server 2003 x64 Edition family	No	Yes

SMS 2.0 and SMS 2003 Software Update Services (SUS) Feature Pack can use MBSA 1.2.1 for detection and therefore have the same limitation that is listed earlier in this bulletin related to programs that MBSA 1.2.1 does not detect.

For more information about SMS, visit the SMS Web site.

For more detailed information, see Microsoft Knowledge Base Article 910723.

Vulnerability Details

Windows Shell Remote Code Execution Vulnerability - CVE-2006-3730:

A remote code execution vulnerability exists in Windows Shell due to improper validation of input parameters when invoked by the WebViewFolderIcon ActiveX control (Web View). This vulnerability could potentially allow remote code execution if a user visited a specially crafted Web site or viewed a specially crafted e-mail message. An attacker could exploit the vulnerability by hosting a web site that contained a web page that was used to exploit this vulnerability. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Mitigating Factors for Windows Shell Remote Code Execution Vulnerability - CVE-2006-3730:

- In a Web-based attack scenario, an attacker would have to host a Web site that contained a Web page that was used to exploit this vulnerability. An attacker would have no way to force users to visit a specially crafted Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's Web site
- An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

- By default, Internet Explorer on Windows Server 2003 runs in a restricted mode that is known as Enhanced Security Configuration. This mode mitigates this vulnerability. See the FAQ section of this security update for more information about Internet Explorer Enhanced Security Configuration.

Workarounds for Windows Shell Remote Code Execution Vulnerability - CVE-2006-3730:

- **Prevent the WebViewFolderIcon ActiveX object from running in Internet Explorer.**
  You can disable attempts to instantiate an ActiveX control in Internet Explorer by setting the kill bit for the control in the registry.

  Warning If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

  For detailed steps that you can use to prevent a control from running in Internet Explorer, see Microsoft Knowledge Base Article 240797. Follow these steps in this article to create a Compatibility Flags value in the registry to prevent a COM object from being instantiated in Internet Explorer.

  To set the kill bits for CLSIDs with values of {e5df9d10-3b52-11d1-83e8-00a0c90dc849} and {844F4806-E8A8-11d2-9652-00C04FC30871}, paste the following text in a text editor such as Notepad. Then, save the file by using the .reg file name extension.

  Windows Registry Editor Version 5.00 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{e5df9d10-3b52-11d1-83e8-00a0c90dc849}] "Compatibility Flags"=dword:00000400 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{844F4806-E8A8-11d2-9652-00C04FC30871}] "Compatibility Flags"=dword:00000400

  You can apply this .reg file to individual systems by double-clicking it. You can also apply it across domains by using Group Policy. For more information about Group Policy, visit the following Microsoft Web sites:

  Group Policy Collection

  What is Group Policy Object Editor

  Core Group Policy Tools and Settings

  Note You must restart Internet Explorer for your changes to take effect.

  Note The compatibility flag for CLSID {e5df9d10-3b52-11d1-83e8-00a0c90dc849} has an original DWORD value of 0x20000. If you deploy this workaround you should reset the DWORD value to 0x20000 rather than delete the key after you have installed the security update. For more information of various values that determine the behavior of registered Microsoft ActiveX controls see the following product documentation.

  Impact of Workaround: Web sites that use the WebViewFolderIcon ActiveX Control may no longer display or function correctly.

- **Set Internet and Local Intranet security zone settings to "High" to prompt before running ActiveX controls and Active Scripting in these zones,**
  You can help protect against this vulnerability by changing your settings for the Internet security zone to prompt before running ActiveX controls and Active Scripting. You can do this by setting your security browser to **High**.

To raise the browsing security level in Microsoft Internet Explorer, follow these steps:

1. On the **Internet Explorer Tools** menu, click **Internet Options**.
2. In the **Internet Options** dialog box, click the **Security** tab, and then click the **Internet** icon.
3. Under **Security level for that zone**, move the slider to **High**. This sets the security level for all Web sites you visit to **High**.

Note If no slider is visible, click **Default Level**, and then move the slider to **High**.

Note Setting the level to **High** may cause some Web sites to work incorrectly. If you have difficulty using a Web site after you change this setting and you are sure the site is safe to use, you can add that site to your list of trusted sites. This will allow the site to work correctly even with the high security setting.

Impact of Workaround: There are side effects to prompting before running ActiveX controls. Many Web sites that are on the Internet or on an intranet use ActiveX to provide additional functionality. For example, an online e-commerce site or banking site may use ActiveX controls to provide menus, ordering forms, or even account statements. Prompting before running ActiveX controls is a global setting that affects all Internet and intranet sites. You will be prompted frequently when you enable this workaround. For each prompt, if you feel you trust the site that you are visiting, click **Yes** to run ActiveX controls. If you do not want to be prompted for all these sites, use the "Restrict Web sites to only your trusted Web sites" workaround.

- **Configure Internet Explorer to prompt before running ActiveX controls or disable ActiveX controls in the Internet and local intranet security zone.**
  You can help protect against this vulnerability by changing your settings to prompt before running ActiveX controls only. To do this, follow these steps:

  1. In Internet Explorer, click **Internet Options** on the **Tools** menu.
  2. Click the **Security** tab.
  3. **Click Internet**, and then click **Custom Level.**
  4. Under **Settings**, in the **ActiveX controls and plug-ins** section, under **Run ActiveX controls and plug-ins**, click **Prompt**.
  5. In the **Scripting** section, under **Active Scripting**, click **Prompt** and then click **OK.**
  6. Click **Local intranet** and then click **Custom Level**.
  7. Under **Settings**, in the **ActiveX controls and plug-ins** section, under **Run ActiveX controls and plug-ins**, click **Prompt**.
  8. In the **Scripting** section under **Active Scripting**, click **Prompt**.
  9. Click **OK** two times to return to Internet Explorer.

  Impact of Workaround: There are side effects to prompting before running ActiveX controls. Many Web sites that are on the Internet or on an intranet use ActiveX to provide additional functionality. For example, an online e-commerce site or banking site may use ActiveX controls to provide menus, ordering forms, or even account statements. Prompting before running ActiveX controls is a global setting that affects all Internet and intranet sites. You will be prompted frequently when you enable this workaround. For each prompt, if you feel you trust the site that you are visiting, click **Yes** to run ActiveX controls. If you do not want to be prompted for all these sites, use the "Restrict Web sites to only your trusted Web sites" workaround.

- **Restrict Web sites to only your trusted Web sites**
  After you set Internet Explorer to require a prompt before it runs ActiveX controls and Active Scripting in the Internet zone and in the Local intranet zone, you can add sites that you trust to Internet Explorer's Trusted sites zone. This will

allow you to continue to use trusted Web sites exactly as you do today, while helping to protect you from this attack on untrusted sites. We recommend that you add only sites that you trust to the Trusted sites zone.

To do this, follow these steps:

1. In Internet Explorer, click the **Tools** menu, click **Internet Options**, and then click the **Security** tab.
2. In the **Select a Web content zone to specify its current security settings** box, click **Trusted Sites** and then click **Sites**.
3. If you want to add sites that do not require an encrypted channel, click to clear the **Require server verification (https:) for all sites in this zone** check box.
4. In the **Add this Web site to the zone** box, type the URL of a site that you trust and then click **Add**.
5. Repeat these steps for each site that you want to add to the zone.
6. Click **OK** two times to accept the changes and return to Internet Explorer.

Add any sites that you trust not to take malicious action on your computer. One in particular that you may want to add is "*.windowsupdate.microsoft.com" (without the quotation marks). This is the site that will host the update, and it requires an ActiveX control to install the update.

FAQ for Windows Shell Remote Code Execution Vulnerability - CVE-2006-3730:

What is the scope of the vulnerability?
This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

What causes the vulnerability?
The vulnerability is caused by improper validation of input parameters to the Windows Shell when invoked by the WebViewFolderIcon ActiveX object.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could take complete control of the affected system.

How could an attacker exploit the vulnerability?
While the vulnerability exists in Windows Explorer the attack vector is exposed through the use of Internet Explorer. As a result, exploitation of the vulnerability is through a Web-based attack scenario. In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to attempt to exploit this vulnerability. An attacker would have no way to force users to visit a specially crafted Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's site. It could also be possible to display specially crafted Web content by using banner advertisements or by using other methods to deliver Web content to affected systems.

What systems are primarily at risk from the vulnerability?
Workstations and terminal servers are primarily at risk. Servers could be at more risk if administrators allow users to log on to servers and to run programs. However, best practices strongly discourage allowing this.

I am running Internet Explorer on Windows Server 2003. Does this mitigate this vulnerability?
Yes. By default, Internet Explorer on Windows Server 2003 runs in a restricted mode that is known as Enhanced Security Configuration. This mode mitigates this vulnerability.

What is the Internet Explorer Enhanced Security Configuration?
Internet Explorer Enhanced Security Configuration is a group of preconfigured Internet Explorer settings that reduce the

likelihood of a user or of an administrator downloading and running specially crafted Web content on a server. Internet Explorer Enhanced Security Configuration reduces this risk by modifying many security-related settings. This includes the settings on the **Security** tab and the **Advanced** tab in the **Internet Options** dialog box. Some of the important modifications include the following:

- Security level for the Internet zone is set to **High**. This setting disables scripts, ActiveX controls, Microsoft Java Virtual Machine (MSJVM), and file downloads.
- Automatic detection of intranet sites is disabled. This setting assigns all intranet Web sites and all Universal Naming Convention (UNC) paths that are not explicitly listed in the Local intranet zone to the Internet zone.
- Install On Demand and non-Microsoft browser extensions are disabled. This setting prevents Web pages from automatically installing components and prevents non-Microsoft extensions from running.
- Multimedia content is disabled. This setting prevents music, animations, and video clips from running.

What does the update do?
The update removes the vulnerability by correcting the parameter validation done in the Windows Shell when invoked by the WebViewFolderIcon ActiveX object.

When this security bulletin was issued, had this vulnerability been publicly disclosed?
Yes. This vulnerability has been publicly disclosed. It has been assigned Common Vulnerability and Exposure number CVE-2006-3730. It also has been named WebViewFolderIcon setSlice by the larger security community. This security bulletin addresses the publicly disclosed vulnerability.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?
Yes. When the security bulletin was released, Microsoft had received information that this vulnerability was being exploited.

Does applying this security update help protect customers from the code that has been published publicly that attempts to exploit this vulnerability?
Yes. This security update addresses the vulnerability that is currently being exploited. The vulnerability that has been addressed has been assigned the Common Vulnerability and Exposure number CVE-2006-3730.

Security Update Information

Affected Software:

For information about the specific security update for your affected software, click the appropriate link:

Windows 2000 (all versions)

Prerequisites For Windows 2000, this security update requires Service Pack 4 (SP4). For Small Business Server 2000, this security update requires Small Business Server 2000 Service Pack 1a (SP1a) or Small Business Server 2000 running with Windows 2000 Server Service Pack 4 (SP4).

The software that is listed has been tested to determine whether the versions are affected. Other versions either no longer include security update support or may not be affected. To determine the support life cycle for your product and version, visit the Microsoft Support Lifecycle Web site.

For more information about how to obtain the latest service pack, see Microsoft Knowledge Base Article 260910.

Inclusion in Future Service Packs The update for this issue may be included in a future Update Rollup.

Installation Information

This security update supports the following setup switches.

Expand table

Switch	Description
/help	Displays the command-line options.
Setup Modes	
/passive	Unattended Setup mode. No user interaction is required, but installation status is displayed. If a restart is required at the end of setup, a dialog box will be presented to the user with a timer warning that the computer will restart in 30 seconds.
/quiet	Quiet mode. This is the same as unattended mode, but no status or error messages are displayed.
Restart Options	
/norestart	Does not restart when installation has completed.
/forcerestart	Restarts the computer after installation and forces other applications to close at shutdown without saving open files first.
/warnrestart[:x]	Displays a dialog box with a timer warning the user that the computer will restart in *x* seconds. (The default setting is 30 seconds.) Intended for use with the **/quiet** switch or the **/passive** switch.
/promptrestart	Display a dialog box prompting the local user to allow a restart.
Special Options	
/overwriteoem	Overwrites OEM files without prompting.
/nobackup	Does not back up files needed for uninstallation.
/forceappsclose	Forces other programs to close when the computer shuts down.
/log:path	Allows the redirection of installation log files.
/integrate:path	Integrates the update into the Windows source files. These files are located at the path that is specified in the switch.
/extract[:path]	Extracts files without starting the Setup program.
/ER	Enables extended error reporting.
/verbose	Enables verbose logging. During installation, creates %Windir%\CabBuild.log. This log details the files that are copied. Using this switch may cause the installation to proceed more slowly.

Note You can combine these switches into one command. For backward compatibility, the security update also supports the setup switches that the earlier version of the Setup program uses. For more information about the supported installation switches, see Microsoft Knowledge Base Article 262841. For more information about the Update.exe installer, visit the Microsoft TechNet Web site. For more information about the terminology that appears in this bulletin, such as *hotfix*, see Microsoft Knowledge Base Article 824684.

Deployment Information

To install the security update without any user intervention, use the following command at a command prompt for Windows 2000 Service Pack 4:

Windows2000-kb923191-x86-enu /quiet

Note Use of the **/quiet** switch will suppress all messages. This includes suppressing failure messages. Administrators should use one of the supported methods to verify the installation was successful when they use the **/quiet** switch. Administrators should also review the KB923191.log file for any failure messages when they use this switch.

To install the security update without forcing the system to restart, use the following command at a command prompt for Windows 2000 Service Pack 4:

Windows2000-kb923191-x86-enu /norestart

For more information about how to deploy this security update with Software Update Services, visit the Software Update Services Web site. For more information about how to deploy this security update using Windows Server Update Services, visit the Windows Server Update Services Web site. This security update will also be available through the Microsoft Update Web site.

Restart Requirement

You must restart your system after you apply this security update.

Removal Information

To remove this security update, use the Add or Remove Programs tool in Control Panel.

System administrators can also use the Spuninst.exe utility to remove this security update. The Spuninst.exe utility is located in the %Windir%\$NTUninstallKB923191$\Spuninst folder.

Expand table

Switch	Description
/help	Displays the command-line options.
Setup Modes	
/passive	Unattended Setup mode. No user interaction is required, but installation status is displayed. If a restart is required at the end of setup, a dialog box will be presented to the user with a timer warning that the computer will restart in 30 seconds.
/quiet	Quiet mode. This is the same as unattended mode, but no status or error messages are displayed.
Restart Options	
/norestart	Does not restart when installation has completed.
/forcerestart	Restarts the computer after installation and forces other applications to close at shutdown without saving open files first.
/warnrestart[:x]	Displays a dialog box with a timer warning the user that the computer will restart in *x* seconds. (The default setting is 30 seconds.) Intended for use with the **/quiet** switch or the **/passive** switch.
/promptrestart	Display a dialog box prompting the local user to allow a restart.
Special Options	
/forceappsclose	Forces other programs to close when the computer shuts down.
/log:path	Allows the redirection of installation log files.

File Information

The English version of this security update has the file attributes that are listed in the following table. The dates and times for these files are listed in coordinated universal time (UTC). When you view the file information, it is converted to local time. To find the difference between UTC and local time, use the **Time Zone** tab in the Date and Time tool in Control Panel.

Windows 2000 Service Pack 4 and Small Business Server 2000:

Expand table

File Name	Version	Date	Time	Size	Folder
Comctl32.dll	5.81.3900.7109	28-Aug-2006	23:33	529,680	
Comctl32.dll	5.81.4968.2500	28-Aug-2006	21:14	530,192	XPSP2_BINARYDROP

Verifying that the Update Has Been Applied

- **Microsoft Baseline Security Analyzer**
  To verify that a security update has been applied to an affected system, you may be able to use the Microsoft Baseline Security Analyzer (MBSA) tool. See the frequently asked question, "Can I use the Microsoft Baseline Security Analyzer (MBSA) to determine whether this update is required?" in the section, Frequently Asked Questions (FAQ) Related to This Security Update, earlier in this bulletin.

- **File Version Verification**
  Note Because there are several versions of Microsoft Windows, the following steps may be different on your computer. If they are, see your product documentation to complete these steps.

  1. Click **Start**, and then click **Search**.
  2. In the **Search Results** pane, click **All files and folders** under **Search Companion**.
  3. In the **All or part of the file name** box, type a file name from the appropriate file information table, and then click **Search**.
  4. In the list of files, right-click a file name from the appropriate file information table, and then click **Properties**.

     Note Depending on the version of the operating system or programs installed, some of the files that are listed in the file information table may not be installed.
  5. On the **Version** tab, determine the version of the file that is installed on your computer by comparing it to the version that is documented in the appropriate file information table.

     Note Attributes other than the file version may change during installation. Comparing other file attributes to the information in the file information table is not a supported method of verifying that the update has been applied. Also, in certain cases, files may be renamed during installation. If the file or version information is not present, use one of the other available methods to verify update installation.

- **Registry Key Verification**
  You may also be able to verify the files that this security update has installed by reviewing the following registry key:

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows 2000\SP5\KB923191\Filelist

Note This registry key may not contain a complete list of installed files. Also, this registry key may not be created correctly when an administrator or an OEM integrates or slipstreams the security update into the Windows installation source files.

Windows XP (all versions)

Prerequisites This security update requires Microsoft Windows XP Service Pack 1 or a later version. For more information, see Microsoft Knowledge Base Article 322389.

Inclusion in Future Service Packs The update for this issue will be included in a future Service Pack or Update Rollup.

Installation Information

This security update supports the following setup switches.

Expand table

Switch	Description
/help	Displays the command-line options.
Setup Modes	
/passive	Unattended Setup mode. No user interaction is required, but installation status is displayed. If a restart is required at the end of setup, a dialog box will be presented to the user with a timer warning that the computer will restart in 30 seconds.
/quiet	Quiet mode. This is the same as unattended mode, but no status or error messages are displayed.
Restart Options	
/norestart	Does not restart when installation has completed.
/forcerestart	Restarts the computer after installation and forces other applications to close at shutdown without saving open files first.
/warnrestart[:x]	Displays a dialog box with a timer warning the user that the computer will restart in *x* seconds. (The default setting is 30 seconds.) Intended for use with the **/quiet** switch or the **/passive** switch.
/promptrestart	Display a dialog box prompting the local user to allow a restart.
Special Options	
/overwriteoem	Overwrites OEM files without prompting.
/nobackup	Does not back up files needed for uninstallation.
/forceappsclose	Forces other programs to close when the computer shuts down.
/log:path	Allows the redirection of installation log files.
/integrate:path	Integrates the update into the Windows source files. These files are located at the path that is specified in the switch.
/extract[:path]	Extracts files without starting the Setup program.
/ER	Enables extended error reporting.
/verbose	Enables verbose logging. During installation, creates %Windir%\CabBuild.log. This log details the files that are copied. Using this switch may cause the installation to proceed more slowly.

Note You can combine these switches into one command. For backward compatibility, the security update also supports the setup switches that the earlier version of the Setup program uses. For more information about the supported installation switches, see Microsoft Knowledge Base Article 262841. For more information about the Update.exe installer, visit the Microsoft TechNet Web site.

Deployment Information

To install the security update without any user intervention, use the following command at a command prompt for Microsoft Windows XP:

Windowsxp-kb923191-x86-enu /quiet

Note Use of the **/quiet** switch will suppress all messages. This includes suppressing failure messages. Administrators should use one of the supported methods to verify the installation was successful when they use the **/quiet** switch. Administrators should also review the KB923191.log file for any failure messages when they use this switch.

To install the security update without forcing the system to restart, use the following command at a command prompt for Windows XP:

Windowsxp-kb923191-x86-enu /norestart

For information about how to deploy this security update by using Software Update Services, visit the Software Update Services Web site. For more information about how to deploy this security update using Windows Server Update Services, visit the Windows Server Update Services Web site. This security update will also be available through the Microsoft Update Web site.

Restart Requirement

You must restart your system after you apply this security update.

Removal Information

To remove this security update, use the Add or Remove Programs tool in Control Panel.

System administrators can also use the Spuninst.exe utility to remove this security update. The Spuninst.exe utility is located in the %Windir%\$NTUninstallKB923191$\Spuninst folder.

Expand table

Switch	Description
/help	Displays the command-line options.
Setup Modes	
/passive	Unattended Setup mode. No user interaction is required, but installation status is displayed. If a restart is required at the end of setup, a dialog box will be presented to the user with a timer warning that the computer will restart in 30 seconds.
/quiet	Quiet mode. This is the same as unattended mode, but no status or error messages are displayed.
Restart Options	
/norestart	Does not restart when installation has completed.
/forcerestart	Restarts the computer after installation and forces other applications to close at shutdown without saving open files first.

Switch	Description
/warnrestart[:x]	Displays a dialog box with a timer warning the user that the computer will restart in *x* seconds. (The default setting is 30 seconds.) Intended for use with the **/quiet** switch or the **/passive** switch.
/promptrestart	Display a dialog box prompting the local user to allow a restart.
Special Options	
/forceappsclose	Forces other programs to close when the computer shuts down.
/log:path	Allows the redirection of installation log files.

File Information

The English version of this security update has the file attributes that are listed in the following table. The dates and times for these files are listed in coordinated universal time (UTC). When you view the file information, it is converted to local time. To find the difference between UTC and local time, use the **Time Zone** tab in the Date and Time tool in Control Panel.

Windows XP Home Edition Service Pack 1, Windows XP Professional Service Pack 1, Windows XP Tablet PC Edition, Windows XP Media Center Edition, Windows XP Home Edition Service Pack 2, Windows XP Professional Service Pack 2, Windows XP Tablet PC Edition 2005, and Windows XP Media Center Edition 2005:

Expand table

File Name	Version	Date	Time	Size	Folder
Comctl32.dll	5.82.2800.1891	25-Aug-2006	15:53	561,664	SP1QFE
Fldrclnr.dll	6.0.2800.1579	20-Aug-2004	22:01	82,432	SP1QFE
Shell32.dll	6.0.2800.1873	13-Jul-2006	13:46	8,353,280	SP1QFE
Sxs.dll	5.1.2600.1579	20-Aug-2004	22:01	700,928	SP1QFE
Comctl32.dll	6.0.2800.1891	25-Aug-2006	15:53	925,184	SP1QFE\ASMS\60\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		25-Aug-2006	15:57	1,812	SP1QFE\ASMS\60\MSFT\WINDOWS\COMMON\CONTROLS
Comctl.man		25-Aug-2006	15:57	621	SP1QFE\ASMS\60\POLICY\60\COMCTL
Comctl32.dll	5.82.2900.2982	25-Aug-2006	15:45	617,472	SP2QFE
Comctl32.dll	6.0.2900.2982	25-Aug-2006	15:45	1,054,208	SP2QFE\ASMS\60\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		25-Aug-2006	15:55	1,862	SP2QFE\ASMS\60\MSFT\WINDOWS\COMMON\CONTROLS
Comctl.man		25-Aug-2006	15:55	621	SP2QFE\ASMS\60\POLICY\60\COMCTL

Windows XP Professional x64:

Expand table

File Name	Version	Date	Time	Size	CPU	Folder
Comctl32.dll	5.82.3790.2778	28-Aug-2006	09:31	956,928	x64	SP1QFE

File Name	Version	Date	Time	Size	CPU	Folder
Comctl32.dll	5.82.3790.2778	28-Aug-2006	09:31	956,928	x64	SP1QFE\ASMS\582\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:31	2,176		SP1QFE\ASMS\582\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:31	630		SP1QFE\ASMS\582\POLICY\MSFT\WINDOWS\COMMON\CONTROLS
Comctl32.dll	6.0.3790.2778	28-Aug-2006	09:31	1,584,128	x64	SP1QFE\ASMS\60\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:31	1,864		SP1QFE\ASMS\60\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:31	625		SP1QFE\ASMS\60\POLICY\MSFT\WINDOWS\COMMON\CONTROLS
Comctl32.dll	5.82.3790.2778	28-Aug-2006	09:31	599,040	x86	SP1QFE\ASMS\X86\582\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:31	2,174		SP1QFE\ASMS\X86\582\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:31	626		SP1QFE\ASMS\X86\582\POLICY\MSFT\WINDOWS\COMMON\CONTROLS
Comctl32.dll	6.0.3790.2778	28-Aug-2006	09:31	1,051,648	x86	SP1QFE\ASMS\X86\60\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:31	1,864		SP1QFE\ASMS\X86\60\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:31	625		SP1QFE\ASMS\X86\60\POLICY\MSFT\WINDOWS\COMMON\CONTROLS
Wcomctl32.dll	5.82.3790.2778	28-Aug-2006	09:31	599,040	x86	SP1QFE\WOW

Notes When you install these security updates, the installer checks to see if one or more of the files that are being updated on your system have previously been updated by a Microsoft hotfix.

If you have previously installed a hotfix to update one of these files, the installer copies the RTMQFE, SP1QFE, or SP2QFE files to your system. Otherwise, the installer copies the RTMGDR, SP1GDR, or SP2GDR files to your system. Security updates may

not contain all variations of these files. For more information about this behavior, see Microsoft Knowledge Base Article 824994.

For more information about the Update.exe installer, visit the Microsoft TechNet Web site.

For more information about the terminology that appears in this bulletin, such as *hotfix*, see Microsoft Knowledge Base Article 824684.

Verifying that the Update Has Been Applied

- **Microsoft Baseline Security Analyzer**
  To verify that a security update has been applied to an affected system, you may be able to use the Microsoft Baseline Security Analyzer (MBSA) tool. See the frequently asked question, "Can I use the Microsoft Baseline Security Analyzer (MBSA) to determine whether this update is required?" in the section, Frequently Asked Questions (FAQ) Related to This Security Update, earlier in this bulletin.

- **File Version Verification**

  Note Because there are several versions of Microsoft Windows, the following steps may be different on your computer. If they are, see your product documentation to complete these steps.

  1. Click **Start**, and then click **Search**.
  2. In the **Search Results** pane, click **All files and folders** under **Search Companion**.
  3. In the **All or part of the file name** box, type a file name from the appropriate file information table, and then click **Search**.
  4. In the list of files, right-click a file name from the appropriate file information table, and then click **Properties**.

     Note Depending on the version of the operating system or programs installed, some of the files that are listed in the file information table may not be installed.
  5. On the **Version** tab, determine the version of the file that is installed on your computer by comparing it to the version that is documented in the appropriate file information table.

     Note Attributes other than the file version may change during installation. Comparing other file attributes to the information in the file information table is not a supported method of verifying that the update has been applied. Also, in certain cases, files may be renamed during installation. If the file or version information is not present, use one of the other available methods to verify update installation.

- **Registry Key Verification**
  You may also be able to verify the files that this security update has installed by reviewing the following registry keys.

  For Windows XP Home Edition Service Pack 1, Windows XP Professional Service Pack 1, Windows XP Tablet PC Edition, Windows XP Media Center Edition, Windows XP Home Edition Service Pack 2, Windows XP Professional Service Pack 2, Windows XP Tablet PC Edition 2005, and Windows XP Media Center Edition 2005:

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows XP\SP3\KB923191\Filelist

  For Windows XP Professional x64 Edition:

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows XP Version 2003\SP2\KB923191\Filelist

Note These registry keys may not contain a complete list of installed files. Also, these registry keys may not be created correctly if an administrator or an OEM integrates or slipstreams the security update into the Windows installation source files.

Windows Server 2003 (all versions)

Prerequisites This security update requires Windows Server 2003 or Windows Server 2003 Service Pack 1.

Note The security updates for Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1 also apply to Microsoft Windows Server 2003 R2.

Inclusion in Future Service Packs The update for this issue will be included in future Service Pack or Update Rollup.

Installation Information

This security update supports the following setup switches.

Expand table

Switch	Description
/help	Displays the command-line options.
Setup Modes	
/passive	Unattended Setup mode. No user interaction is required, but installation status is displayed. If a restart is required at the end of setup, a dialog box will be presented to the user with a timer warning that the computer will restart in 30 seconds.
/quiet	Quiet mode. This is the same as unattended mode, but no status or error messages are displayed.
Restart Options	
/norestart	Does not restart when installation has completed.
/forcerestart	Restarts the computer after installation and forces other applications to close at shutdown without saving open files first.
/warnrestart[:x]	Displays a dialog box with a timer warning the user that the computer will restart in *x* seconds. (The default setting is 30 seconds.) Intended for use with the **/quiet** switch or the **/passive** switch.
/promptrestart	Display a dialog box prompting the local user to allow a restart.
Special Options	
/overwriteoem	Overwrites OEM files without prompting.
/nobackup	Does not back up files needed for uninstallation.
/forceappsclose	Forces other programs to close when the computer shuts down.
/log: path	Allows the redirection of installation log files.
/integrate:path	Integrates the update into the Windows source files. These files are located at the path that is specified in the switch.
/extract[:path]	Extracts files without starting the Setup program.
/ER	Enables extended error reporting.

Switch	Description
/verbose	Enables verbose logging. During installation, creates %Windir%\CabBuild.log. This log details the files that are copied. Using this switch may cause the installation to proceed more slowly.

Note You can combine these switches into one command. For backward compatibility, the security update also supports many of the setup switches that the earlier version of the Setup program uses. For more information about the supported installation switches, see Microsoft Knowledge Base Article 262841. For more information about the Update.exe installer, visit the Microsoft TechNet Web site.

Deployment Information

To install the security update without any user intervention, use the following command at a command prompt for Windows Server 2003:

Windowsserver2003-kb923191-x86-enu /quiet

Note Use of the **/quiet** switch will suppress all messages. This includes suppressing failure messages. Administrators should use one of the supported methods to verify the installation was successful when they use the **/quiet** switch. Administrators should also review the KB923191.log file for any failure messages when they use this switch.

To install the security update without forcing the system to restart, use the following command at a command prompt for Windows Server 2003:

Windowsserver2003-kb923191-x86-enu /norestart

For information about how to deploy this security update by using Software Update Services, visit the Software Update Services Web site. For more information about how to deploy this security update using Windows Server Update Services, visit the Windows Server Update Services Web site. This security update will also be available through the Microsoft Update Web site.

Restart Requirement

You must restart your system after you apply this security update.

This security update does not support HotPatching. For more information about HotPatching, see Microsoft Knowledge Base Article 897341.

Note Not all security updates support HotPatching, and some security updates that support HotPatching might require that you restart the server after you install the security update. HotPatching is only supported if the files being replaced by the security update are General Distribution Release (GDR) files. HotPatching is not supported if you have previously installed a hotfix to update one of the files included in the security update. For more information about this behavior, see Microsoft Knowledge Base Article 897341 and Microsoft Knowledge Base Article 824994.

Removal Information

To remove this update, use the Add or Remove Programs tool in Control Panel.

System administrators can also use the Spuninst.exe utility to remove this security update. The Spuninst.exe utility is located in the %Windir%\$NTUninstallKB923191$\Spuninst folder.

Expand table

Switch	Description
/help	Displays the command-line options.
Setup Modes	
/passive	Unattended Setup mode. No user interaction is required, but installation status is displayed. If a restart is required at the end of setup, a dialog box will be presented to the user with a timer warning that the computer will restart in 30 seconds.
/quiet	Quiet mode. This is the same as unattended mode, but no status or error messages are displayed.
Restart Options	
/norestart	Does not restart when installation has completed.
/forcerestart	Restarts the computer after installation and forces other applications to close at shutdown without saving open files first.
/warnrestart[:x]	Displays a dialog box with a timer warning the user that the computer will restart in *x* seconds. (The default setting is 30 seconds.) Intended for use with the **/quiet** switch or the **/passive** switch.
/promptrestart	Display a dialog box prompting the local user to allow a restart.
Special Options	
/forceappsclose	Forces other programs to close when the computer shuts down.
/log:path	Allows the redirection of installation log files.

File Information

The English version of this security update has the file attributes that are listed in the following table. The dates and times for these files are listed in coordinated universal time (UTC). When you view the file information, it is converted to local time. To find the difference between UTC and local time, use the **Time Zone** tab in the Date and Time tool in Control Panel.

Windows Server 2003, Web Edition; Windows Server 2003, Standard Edition; Windows Server 2003, Datacenter Edition; Windows Server 2003, Enterprise Edition; Windows Small Business Server 2003; Windows Server 2003, Web Edition with SP1; Windows Server 2003, Standard Edition with SP1; Windows Server 2003, Enterprise Edition with SP1; Windows Server 2003, Datacenter Edition with SP1; Windows Server 2003 R2, Web Edition; Windows Server 2003 R2, Standard Edition; Windows Server 2003 R2, Datacenter Edition; Windows Server 2003 R2, Enterprise Edition; Windows Small Business Server 2003 R2:

Expand table

File Name	Version	Date	Time	Size	CPU	Folder
Comctl32.dll	5.82.3790.583	28-Aug-2006	08:23	574,976	x86	RTMQFE
Comctl32.dll	5.82.3790.583	28-Aug-2006	08:23	574,976	x86	RTMQFE\ASMS\582\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	08:57	2,173		RTMQFE\ASMS\582\MSFT\WINDOWS\COMMON\CONTROLS

File Name	Version	Date	Time	Size	CPU	Folder
Controls.man		28-Aug-2006	08:57	608		RTMQFE\ASMS\582\POLICY\MSFT\WINDOWS\COMMON\CONTROLS
Comctl32.dll	6.0.3790.583	28-Aug-2006	08:23	928,768	x86	RTMQFE\ASMS\60\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	08:57	1,861		RTMQFE\ASMS\60\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	08:57	618		RTMQFE\ASMS\60\POLICY\MSFT\WINDOWS\COMMON\CONTROLS
Comctl32.dll	5.82.3790.2778	28-Aug-2006	08:25	599,040	x86	SP1QFE
Comctl32.dll	5.82.3790.2778	28-Aug-2006	08:25	599,040	x86	SP1QFE\ASMS\582\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:30	2,174		SP1QFE\ASMS\582\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	08:29	626		SP1QFE\ASMS\582\POLICY\MSFT\WINDOWS\COMMON\CONTROLS
Comctl32.dll	6.0.3790.2778	28-Aug-2006	08:25	1,051,136	x86	SP1QFE\ASMS\60\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	08:29	1,862		SP1QFE\ASMS\60\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	08:29	621		SP1QFE\ASMS\60\POLICY\MSFT\WINDOWS\COMMON\CONTROLS

Windows Server, 2003 Enterprise Edition for Itanium-based Systems; Windows Server 2003, Datacenter Edition for Itanium-based Systems; Windows Server 2003, Enterprise Edition with SP1 for Itanium-based Systems; and Windows Server 2003, Datacenter Edition with SP1 for Itanium-based Systems:

Expand table

File Name	Version	Date	Time	Size	CPU	Folder
Comctl32.dll	5.82.3790.583	28-Aug-2006	09:25	1,621,504	IA-64	RTMQFE

File Name	Version	Date	Time	Size	CPU	Folder
Comctl32.dll	5.82.3790.583	28-Aug-2006	09:25	1,621,504	IA-64	RTMQFE\ASMS\582\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:25	2,174		RTMQFE\ASMS\582\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:25	610		RTMQFE\ASMS\582\POLICY\MSFT\WINDOWS\COMMON\CONTROLS
Comctl32.dll	6.0.3790.583	28-Aug-2006	09:25	2,285,568	IA-64	RTMQFE\ASMS\60\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:25	1,862		RTMQFE\ASMS\60\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:25	620		RTMQFE\ASMS\60\POLICY\MSFT\WINDOWS\COMMON\CONTROLS
Comctl32.dll	5.82.3790.583	28-Aug-2006	09:25	574,976	x86	RTMQFE\ASMS\X86\582\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:25	2,173		RTMQFE\ASMS\X86\582\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:25	608		RTMQFE\ASMS\X86\582\POLICY\MSFT\WINDOWS\COMMON\CONTROLS
Wcomctl32.dll	5.82.3790.583	28-Aug-2006	09:25	574,976	x86	RTMQFE\WOW
Comctl32.dll	5.82.3790.2778	28-Aug-2006	09:32	1,803,264	IA-64	SP1QFE
Comctl32.dll	5.82.3790.2778	28-Aug-2006	09:32	1,803,264	IA-64	SP1QFE\ASMS\582\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:32	2,175		SP1QFE\ASMS\582\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:32	628		SP1QFE\ASMS\582\POLICY\MSFT\WINDOWS\COMMON\CONTROLS
Comctl32.dll	6.0.3790.2778	28-Aug-	09:32	2,617,856	IA-64	SP1QFE\ASMS\60\MSFT\WINDOWS\COMMON\CONTROLS

File Name	Version	Date	Time	Size	CPU	Folder
		2006				
Controls.man		28-Aug-2006	09:32	1,863		SP1QFE\ASMS\60\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:32	623		SP1QFE\ASMS\60\POLICY\MSFT\WINDOWS\COMMON\CONTROLS
Comctl32.dll	5.82.3790.2778	28-Aug-2006	09:32	599,040	x86	SP1QFE\ASMS\X86\582\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:32	2,174		SP1QFE\ASMS\X86\582\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:32	626		SP1QFE\ASMS\X86\582\POLICY\MSFT\WINDOWS\COMMON\CONTROLS
Comctl32.dll	6.0.3790.2778	28-Aug-2006	09:32	1,051,648	x86	SP1QFE\ASMS\X86\60\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:32	1,864		SP1QFE\ASMS\X86\60\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:32	625		SP1QFE\ASMS\X86\60\POLICY\MSFT\WINDOWS\COMMON\CONTROLS
Wcomctl32.dll	5.82.3790.2778	28-Aug-2006	09:32	599,040	x86	SP1QFE\WOW

Windows Server 2003, Standard x64 Edition; Windows Server 2003, Enterprise x64 Edition; and Windows Server 2003, Datacenter x64 Edition; Windows Server 2003 R2, Standard x64 Edition; Windows Server 2003 R2, Enterprise x64 Edition; and Windows Server 2003 R2, Datacenter x64 Edition:

Expand table

File Name	Version	Date	Time	Size	CPU	Folder
Comctl32.dll	5.82.3790.2778	28-Aug-2006	09:31	956,928	x64	SP1QFE
Comctl32.dll	5.82.3790.2778	28-Aug-2006	09:31	956,928	x64	SP1QFE\ASMS\582\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:31	2,176		SP1QFE\ASMS\582\MSFT\WINDOWS\COMMON\CONTROLS

File Name	Version	Date	Time	Size	CPU	Folder
Controls.man		28-Aug-2006	09:31	630		SP1QFE\ASMS\582\POLICY\MSFT\WINDOWS\COMMON\CONTROLS
Comctl32.dll	6.0.3790.2778	28-Aug-2006	09:31	1,584,128	x64	SP1QFE\ASMS\60\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:31	1,864		SP1QFE\ASMS\60\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:31	625		SP1QFE\ASMS\60\POLICY\MSFT\WINDOWS\COMMON\CONTROLS
Comctl32.dll	5.82.3790.2778	28-Aug-2006	09:31	599,040	x86	SP1QFE\ASMS\X86\582\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:31	2,174		SP1QFE\ASMS\X86\582\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:31	626		SP1QFE\ASMS\X86\582\POLICY\MSFT\WINDOWS\COMMON\CONTROLS
Comctl32.dll	6.0.3790.2778	28-Aug-2006	09:31	1,051,648	x86	SP1QFE\ASMS\X86\60\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:31	1,864		SP1QFE\ASMS\X86\60\MSFT\WINDOWS\COMMON\CONTROLS
Controls.man		28-Aug-2006	09:31	625		SP1QFE\ASMS\X86\60\POLICY\MSFT\WINDOWS\COMMON\CONTROLS
Wcomctl32.dll	5.82.3790.2778	28-Aug-2006	09:31	599,040	x86	SP1QFE\WOW

Notes When you install these security updates, the installer checks to see if one or more of the files that are being updated on your system have previously been updated by a Microsoft hotfix.

If you have previously installed a hotfix to update one of these files, the installer copies the RTMQFE, SP1QFE, or SP2QFE files to your system. Otherwise, the installer copies the RTMGDR, SP1GDR, or SP2GDR files to your system. Security updates may not contain all variations of these files. For more information about this behavior, see Microsoft Knowledge Base Article 824994.

For more information about this behavior, see Microsoft Knowledge Base Article 824994.

For more information about the Update.exe installer, visit the Microsoft TechNet Web site.

For more information about the terminology that appears in this bulletin, such as *hotfix*, see Microsoft Knowledge Base Article 824684.

Verifying that the Update Has Been Applied

- **Microsoft Baseline Security Analyzer**
  To verify that a security update has been applied to an affected system, you may be able to use the Microsoft Baseline Security Analyzer (MBSA) tool. See the frequently asked question, "Can I use the Microsoft Baseline Security Analyzer (MBSA) to determine whether this update is required?" in the section, Frequently Asked Questions (FAQ) Related to This Security Update, earlier in this bulletin.

- **File Version Verification**

  Note Because there are several versions of Microsoft Windows, the following steps may be different on your computer. If they are, see your product documentation to complete these steps.

  1. Click **Start**, and then click **Search**.
  2. In the **Search Results** pane, click **All files and folders** under **Search Companion**.
  3. In the **All or part of the file name** box, type a file name from the appropriate file information table, and then click **Search**.
  4. In the list of files, right-click a file name from the appropriate file information table, and then click **Properties**.

     Note Depending on the version of the operating system or programs installed, some of the files that are listed in the file information table may not be installed.
  5. On the **Version** tab, determine the version of the file that is installed on your computer by comparing it to the version that is documented in the appropriate file information table.

     Note Attributes other than the file version may change during installation. Comparing other file attributes to the information in the file information table is not a supported method of verifying that the update has been applied. Also, in certain cases, files may be renamed during installation. If the file or version information is not present, use one of the other available methods to verify update installation.

- **Registry Key Verification**
  You may also be able to verify the files that this security update has installed by reviewing the following registry keys.

  Windows Server 2003, Web Edition; Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; Windows Server 2003, Datacenter Edition; Windows Small Business Server 2003; Windows Server 2003, Web Edition with SP1; Windows Server 2003, Standard Edition with SP1; Windows Server 2003, Enterprise Edition with SP1; Windows Server 2003, Datacenter Edition with SP1; Windows Server 2003, Enterprise Edition for Itanium-based Systems; Windows Server 2003, Datacenter Edition for Itanium-based Systems; Windows Server 2003, Enterprise Edition with SP1 for Itanium-based Systems; Windows Server 2003, Datacenter Edition with SP1 for Itanium-based Systems; Windows Server 2003, Standard x64 Edition; Windows Server 2003, Enterprise x64 Edition; and Windows Server 2003, Datacenter x64 Edition:

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows Server 2003\SP2\KB923191\Filelist

  Note This registry key may not contain a complete list of installed files. Also, this registry key may not be created correctly if an administrator or an OEM integrates or slipstreams the security update into the Windows installation source files.

Other Information

Obtaining Other Security Updates:

Updates for other security issues are available at the following locations:

- Security updates are available at the Microsoft Download Center. You can find them most easily by doing a keyword search for "security_patch."
- Updates for consumer platforms are available at the Microsoft Update Web site.

Support:

- Customers in the U.S. and Canada can receive technical support from Microsoft Product Support Services at 1-866-PCSAFETY. There is no charge for support calls that are associated with security updates.
- International customers can receive support from their local Microsoft subsidiaries. There is no charge for support that is associated with security updates. For more information about how to contact Microsoft for support issues, visit the International Support Web site.

Security Resources:

- The Microsoft TechNet Security Web site provides additional information about security in Microsoft products.
- TechNet Update Management Center
- Microsoft Software Update Services
- Microsoft Windows Server Update Services
- Microsoft Baseline Security Analyzer (MBSA)
- Windows Update
- Microsoft Update
- Windows Update Catalog: For more information about the Windows Update Catalog, see Microsoft Knowledge Base Article 323166.
- Office Update

Software Update Services:

By using Microsoft Software Update Services (SUS), administrators can quickly and reliably deploy the latest critical updates and security updates to Windows 2000 and Windows Server 2003-based servers, and to desktop systems that are running Windows 2000 Professional or Windows XP Professional.

For more information about how to deploy security updates by using Software Update Services, visit the Software Update Services Web site.

Windows Server Update Services:

By using Windows Server Update Services (WSUS), administrators can quickly and reliably deploy the latest critical updates and security updates for Windows 2000 operating systems and later, Office XP and later, Exchange Server 2003, and SQL Server 2000 onto Windows 2000 and later operating systems.

For more information about how to deploy security updates using Windows Server Update Services, visit the Windows Server Update Services Web site.

Systems Management Server:

Microsoft Systems Management Server (SMS) delivers a highly configurable enterprise solution for managing updates. By using SMS, administrators can identify Windows-based systems that require security updates and can perform controlled

deployment of these updates throughout the enterprise with minimal disruption to end users. For more information about how administrators can use SMS 2003 to deploy security updates, visit the SMS 2003 Security Patch Management Web site. SMS 2.0 users can also use Software Updates Service Feature Pack to help deploy security updates. For information about SMS, visit the SMS Web site.

Note SMS uses the Microsoft Baseline Security Analyzer, the Microsoft Office Detection Tool, and the Enterprise Update Scan Tool to provide broad support for security bulletin update detection and deployment. Some software updates may not be detected by these tools. Administrators can use the inventory capabilities of the SMS in these cases to target updates to specific systems. For more information about this procedure, visit the following Web site. Some security updates require administrative rights following a restart of the system. Administrators can use the Elevated Rights Deployment Tool (available in the SMS 2003 Administration Feature Pack and in the SMS 2.0 Administration Feature Pack) to install these updates.

Disclaimer:

The information provided in the Microsoft Knowledge Base is provided "as is" without warranty of any kind. Microsoft disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Microsoft Corporation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Microsoft Corporation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Revisions:

- V1.0 (October 10, 2006): Bulletin published.

Built at 2014-04-18T13:49:36Z-07:00

Last updated on 06/08/2023