EXHIBIT F

Quick Links | Home | Worldwide

Microsoft TechNet

TechNet Home | TechCenters | Downloads | TechNet Program | Subscriptions | My TechNet | Security Bulletins | Archive

Search for
Go

TechNet Home > TechNet Security > Bulletins

TechNet Security
Security Bulletin Search
Virus Alerts
Products
Guidance
Tools
Understanding Security
Partners
Downloads
Community
Events & Webcasts
Scripting for Security
Small Business Security
Midsize Business Security

Additional Resources
Events & Errors
Knowledge Base Search

Microsoft Security Bulletin MS05-053

Vulnerabilities in Graphics Rendering Engine Could Allow Code Execution (896424)

Published: November 8, 2005 | Updated: November 30, 2005

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 several prior security updates. 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

Non-Affected Software:

•Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)

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.

↑Top of section

General Information

⊞ Executive Summary

Executive Summary:

This update resolves several newly-discovered, privately reported and public vulnerabilities. Each vulnerability is documented in this bulletin in its own "Vulnerability Details" section of this bulletin.

An attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

We recommend that customers apply the update immediately.

Severity Ratings and Vulnerability Identifiers:

Vulnerability Identifiers	Impact of Vulnerability	Windows 2000	Windows XP Service Pack 1	Windows XP Service Pack 2	Windows Server 2003	Windows Server 2003 Service Pack 1
Graphics Rendering Engine Vulnerability - CAN-2005-2123	Remote Code Execution	Critical	Critical	Critical	Critical	Critical
Windows Metafile Vulnerability - CAN-2005-2124	Remote Code Execution	Critical	Critical	None	Critical	None

Enhanced Metafile Vulnerability - CAN-2005-0803	Denial of Service	Moderate	Moderate	None	Moderate	None
Aggregate Severity of All Vulnerabilities		**Critical**	**Critical**	**Critical**	**Critical**	**Critical**

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.

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

Top of section

Frequently asked questions (FAQ) related to this security update

Why does this update address several reported security vulnerabilities?
This update contains support for several vulnerabilities because the modifications that are required to address these issues are located in related files. Instead of having to install several updates that are almost the same, customers can install only this update.

What updates does this release replace?
This security update replaces several prior security updates. The security bulletin IDs and affected operating systems are listed in the following table.

Bulletin ID	Windows 2000	Windows XP Service Pack 1	Windows XP Service Pack 2	Windows Server 2003	Windows Server 2003 Service Pack 1
MS03-045	Not Replaced	Replaced	Not Applicable	Not Replaced	Not Applicable
MS05-002	Not Replaced	Replaced	Not Applicable	Not Replaced	Not Applicable

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'm 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 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 additional support for Windows NT 4.0 SP6a and Windows 2000 Service Pack 3 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.

Security update support for Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium) and Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium) ended on June 30, 2005. I'm still using one of these operating systems, what should I do?

With the release of Windows XP Professional x64 Edition, Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium) and Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium) will no longer receive security update support. It should be a priority for customers who have these operating system versions to migrate to supported versions to prevent potential exposure to vulnerabilities. Microsoft will continue to fully support Windows Server 2003 for Itanium-based systems, Windows XP Professional x64 Edition, and Windows Server 2003 x64 Editions for 64-bit computing requirements. Microsoft continues to license and support Windows Server 2003 Enterprise and Datacenter editions for Itanium-based systems, and the 64-bit version of SQL Server 2000 Enterprise Edition. In the future we will expand Itanium support to Visual Studio 2005, .NET Framework 2005 and SQL Server 2005.

Customers who require additional assistance about this issue must contact their Microsoft account team representative, their Technical Account Manager, or the appropriate Microsoft partner representative for information about the available migration 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.

Can I use the Microsoft Baseline Security Analyzer (MBSA) 1.2.1 to determine whether this update is required?

Yes. MBSA 1.2.1 will determine whether this update is required. For more information about MBSA, visit the MBSA Web site.

Can I use the Microsoft Baseline Security Analyzer (MBSA) 2.0 to determine whether this update is required?

Yes. MBSA 2.0 will determine whether this update is required. MBSA 2.0 can detect security updates for products that Microsoft Update supports. For more information about MBSA, visit the MBSA Web site.

Can I use Systems Management Server (SMS) to determine whether this update is required?

Yes. SMS can help detect and deploy this security update. For information about SMS, visit the SMS Web site. The Security Update Inventory Tool can be used by SMS for detecting security updates that are offered by Windows Update, that are supported by Software Update Services, and other security updates that are supported by MBSA 1.2.1. For more information about the Security Update Inventory Tool, see the following Microsoft Web site. For more information about the limitations of the Security Update Inventory Tool, see Microsoft Knowledge Base Article 306460. The SMS 2003 Inventory Tool for Microsoft Updates can be used by SMS for detecting security updates that are offered by Microsoft Update and that are supported by Windows Server Update Services. For more information about the SMS 2003 Inventory Tool for Microsoft Updates, see the following Microsoft Web site.

↑Top of section

⊞ Vulnerability Details

⊞ Graphics Rendering Engine - CAN-2005-2123:

A remote code execution vulnerability exists in the rendering of Windows Metafile (WMF) and Enhanced Metafile (EMF) image formats that could allow remote code execution on an affected system. Any program that renders WMF or EMF images on the affected systems could be vulnerable to this attack. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

⊞ Mitigating Factors for Graphics Rendering Engine - CAN-2005-2123:

- The vulnerability could be exploited by an attacker who persuaded a user to open a specially crafted file or to view a folder that contains the specially crafted image. There is no way for an attacker to force a user to open a malicious file, except potentially through previewing an email message.
- In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to exploit this vulnerability. An attacker would have no way to force users to visit a malicious 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.

↑Top of section

⊞ Workarounds for Graphics Rendering Engine - CAN-2005-2123:

Microsoft has tested the following workarounds. While these workarounds will not correct the underlying vulnerability, they help block known attack vectors. When a workaround reduces functionality, it is identified in the following section.

- **Read e-mail messages in plain text format if you are using Outlook 2002 or a later version, to help protect yourself from the HTML e-mail attack vector.**

  Microsoft Outlook 2002 users who have applied Office XP Service Pack 1 or a later version and Microsoft Outlook Express 6 users who have applied Internet Explorer 6 Service Pack 1 or a later version can enable this setting and view e-mail messages that are not digitally signed or e-mail messages that are not encrypted in plain text only.

  Digitally signed e-mail messages or encrypted e-mail messages are not affected by the setting and may be read in their original formats. For more information about how to enable this setting in Outlook 2002, see Microsoft Knowledge Base Article 307594.

  Impact of Workaround: E-mail messages that are viewed in plain text format will not contain pictures, specialized fonts, animations, or other rich content. Additionally:

  - The changes are applied to the preview pane and to open messages.
  - Pictures become attachments so that they are not lost.
  - Because the message is still in Rich Text or HTML format in the store, the object model (custom code solutions) may behave unexpectedly.

↑Top of section

⊞ FAQ for Graphics Rendering Engine - CAN-2005-2123:

What is the scope of the vulnerability?
This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability could remotely take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. This vulnerability could also be used to attempt to perform a local elevation of privilege or a remote denial of service.

What causes the vulnerability?
An unchecked buffer in the rendering of Windows Metafile (WMF) and Enhanced Metafile (EMF) image formats.

What are Windows Metafile (WMF) and Enhanced Metafile (EMF) image formats?

A WMF image is a 16-bit metafile format that can contain both vector information and bitmap information. It is optimized for the Windows operating system.

An EMF image is a 32-bit format that can contain both vector information and bitmap information. This format is an improvement over the Windows Metafile Format and contains extended features.

For more information about image types and formats, see Microsoft Knowledge Base Article 320314. Additional information about these file formats is also available at the MSDN Library Web Site.

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 this vulnerability?
Any program that renders the affected image types could be vulnerable to this attack. Here are some examples of how an attacker could attempt to exploit this vulnerability:

- An attacker could host a malicious Web site that is designed to exploit this vulnerability through Internet Explorer and then persuade a user to view the Web site.
- An attacker could create an HTML e-mail message that has a specially crafted image attached. The specially crafted image could be designed to exploit this vulnerability through Microsoft Outlook or through Outlook Express 6. An attacker could persuade the user to view the HTML e-mail message.
- An attacker could embed a specially crafted image in an Office document and then persuade the user to view the document.
- An attacker could add a specially crafted image to the local file system or onto a network share and then persuade the user to preview the folder.
- If an attacker is able to log on locally, they could then run a specially-designed program that could exploit the vulnerability, and thereby gain complete control over the affected system.

An attacker could also access the affected component through another vector. For example, an attacker could log on to the system interactively or by using another program that passes parameters to the vulnerable component (locally or remotely). To locally exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially-designed application that could exploit the vulnerability, and thereby gain complete control over the affected system.

What systems are primarily at risk from the vulnerability?
The vulnerability could be exploited on the affected systems by an attacker who persuaded a user to open a specially crafted file or to view a folder that contains the specially crafted image. There is no way for an attacker to force a user to open a specially crafted file, except potentially through previewing an email message. Workstations and terminal servers are primarily at risk. Servers could be at more risk if users who do not have sufficient administrative permissions are given the ability to log on to servers and run programs or browse the Internet. However, best practices strongly discourage allowing this.

Could the vulnerability be exploited over the Internet?
Yes. An attacker could try to exploit this vulnerability through malicious Web sites or through email over the Internet.

What does the update do?
The update removes the vulnerability by modifying the way that the Graphics Rendering Engine processes Windows Metafile (WMF) and Enhanced Metafile (EMF) image formats.

When this security bulletin was issued, had this vulnerability been publicly disclosed?
No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information to indicate that this vulnerability had been publicly disclosed when this security bulletin was originally issued.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?
No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code

published when this security bulletin was originally issued.

↑Top of section

↑Top of section

⊞ Windows Metafile Vulnerability - CAN-2005-2124:

A remote code execution vulnerability exists in the rendering of Windows Metafile (WMF) image format that could allow remote code execution on an affected system. Any program that renders WMF images on the affected systems could be vulnerable to this attack. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

⊞ Mitigating Factors for Windows Metafile Vulnerability - CAN-2005-2124:

- The vulnerability could be exploited by an attacker who persuaded a user to open a specially crafted file or to view a folder that contains the specially crafted image. There is no way for an attacker to force a user to open a malicious file, except potentially through previewing an email message.
- In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to exploit this vulnerability. An attacker would have no way to force users to visit a malicious 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.

↑Top of section

⊞ Workarounds for Windows Metafile Vulnerability - CAN-2005-2124:

Microsoft has tested the following workarounds. While these workarounds will not correct the underlying vulnerability, they help block known attack vectors. When a workaround reduces functionality, it is identified in the following section.

- **Read e-mail messages in plain text format if you are using Outlook 2002 or a later version, to help protect yourself from the HTML e-mail attack vector.**

  Microsoft Outlook 2002 users who have applied Office XP Service Pack 1 or a later version and Microsoft Outlook Express 6 users who have applied Internet Explorer 6 Service Pack 1 or a later version can enable this setting and view e-mail messages that are not digitally signed or e-mail messages that are not encrypted in plain text only.

  Digitally signed e-mail messages or encrypted e-mail messages are not affected by the setting and may be read in their original formats. For more information about how to enable this setting in Outlook 2002, see Microsoft Knowledge Base Article 307594.

  Impact of Workaround: E-mail messages that are viewed in plain text format will not contain pictures, specialized fonts, animations, or other rich content. Additionally:

  - The changes are applied to the preview pane and to open messages.
  - Pictures become attachments so that they are not lost.

- Because the message is still in Rich Text or HTML format in the store, the object model (custom code solutions) may behave unexpectedly.

⇡Top of section

⊞ FAQ for Windows Metafile Vulnerability - CAN-2005-2124:

What is the scope of the vulnerability?
This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability could remotely take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. This vulnerability could also be used to attempt to perform a local elevation of privilege or a remote denial of service.

What causes the vulnerability?
An unchecked buffer in the rendering of Windows Metafile (WMF) image formats.

What are Windows Metafile (WMF) image formats?

A WMF image is a 16-bit metafile format that can contain both vector information and bitmap information. It is optimized for the Windows operating system.

For more information about image types and formats, see Microsoft Knowledge Base Article 320314. Additional information about these file formats is also available at the MSDN Library Web Site.

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 this vulnerability?
Any program that renders the affected image types could be vulnerable to this attack. Here are some examples of how an attacker could attempt to exploit this vulnerability:

- An attacker could host a malicious Web site that is designed to exploit this vulnerability through Internet Explorer and then persuade a user to view the Web site.
- An attacker could create an HTML e-mail message that has a specially crafted image attached. The specially crafted image could be designed to exploit this vulnerability through Microsoft Outlook or through Outlook Express 6. An attacker could persuade the user to view the HTML e-mail message.
- An attacker could embed a specially crafted image in an Office document and then persuade the user to view the document.
- An attacker could add a specially crafted image to the local file system or onto a network share and then persuade the user to preview the folder.
- An attacker could locally log on to the system. An attacker could then run a specially-designed program that could exploit the vulnerability, and thereby gain complete control over the affected system.

An attacker could also access the affected component through another vector. For example, an attacker could log on to the system interactively or by using another program that passes parameters to the vulnerable component (locally or remotely). To locally exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially-designed application that could exploit the vulnerability, and thereby gain complete control over the affected system.

What systems are primarily at risk from the vulnerability?
The vulnerability could be exploited on the affected systems by an attacker who persuaded a user to open a specially crafted file or to view a folder that contains the specially crafted image. There is no way for an attacker to force a user to open a specially crafted file, except potentially through previewing an email message. Workstations and terminal servers are primarily at risk. Servers could be at more risk if users who do not have sufficient administrative permissions are given the ability to log on to servers and run programs or browse the Internet. However, best practices strongly discourage allowing this.

Could the vulnerability be exploited over the Internet?
Yes. An attacker could try to exploit this vulnerability through malicious Web sites or through email over the Internet.

What does the update do?
The update removes the vulnerability by modifying the way that the affected operating system versions validate the length of a message before it passes the message to the allocated buffer.

When this security bulletin was issued, had this vulnerability been publicly disclosed?
No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information to indicate that this vulnerability had been publicly disclosed when this security bulletin was originally issued.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?
No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

↑Top of section

↑Top of section

⊞ Enhanced Metafile Vulnerability - CAN-2005-0803:

A denial of service vulnerability exists in the rendering of Enhanced Metafile (EMF) image format that could allow any program that renders EMF images to be vulnerable to attack. An attacker who successfully exploited this vulnerability could cause the affected programs to stop responding.

⊞ Mitigating Factors for Enhanced Metafile Vulnerability - CAN-2005-0803:

- The vulnerability could be exploited by an attacker who persuaded a user to open a specially crafted file or to view a folder that contains the specially crafted image. There is no way for an attacker to force a user to open a malicious file, except potentially through previewing an email message.
- In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to exploit this vulnerability. An attacker would have no way to force users to visit a malicious 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.

↑Top of section

⊞ Workarounds for Enhanced Metafile Vulnerability - CAN-2005-0803:

Microsoft has tested the following workarounds. While these workarounds will not correct the underlying vulnerability, they help block known attack vectors. When a workaround reduces functionality, it is identified in the following section.

- **Read e-mail messages in plain text format if you are using Outlook 2002 or a later version, to help protect yourself from the HTML e-mail attack vector.**

  Microsoft Outlook 2002 users who have applied Office XP Service Pack 1 or a later version and Microsoft Outlook Express 6 users who have applied Internet Explorer 6 Service Pack 1 or a later version can enable this setting and view e-mail messages that are not digitally signed or e-mail messages that are not encrypted in plain text only.

  Digitally signed e-mail messages or encrypted e-mail messages are not affected by the setting and may be read in their original formats. For more information about how to enable this setting in Outlook 2002, see Microsoft Knowledge Base Article 307594.

  Impact of Workaround: E-mail messages that are viewed in plain text format will not contain pictures, specialized fonts, animations, or other rich content. Additionally:

  - The changes are applied to the preview pane and to open messages.
  - Pictures become attachments so that they are not lost.
  - Because the message is still in Rich Text or HTML format in the store, the object model (custom code solutions) may behave unexpectedly.

↑Top of section

⊞ FAQ for Enhanced Metafile Vulnerability - CAN-2005-0803:

What is the scope of the vulnerability?
This is a denial of service vulnerability. An attacker who exploited this vulnerability could cause the affected program to stop responding. The program could be restarted in order to return to normal operation. Note that the denial of service vulnerability would not allow attackers to execute code or elevate their privileges, but it could cause the affected program to stop responding.

What causes the vulnerability?
An unchecked buffer in the rendering of Enhanced Metafile (EMF) image formats.

What are Enhanced Metafile (EMF) image formats?

An EMF image is a 32-bit format that can contain both vector information and bitmap information. This format is an improvement over the Windows Metafile Format and contains extended features.

For more information about image types and formats, see Microsoft Knowledge Base Article 320314. Additional information about these file formats is also available at the MSDN Library Web Site.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could cause a program to stop responding.

How could an attacker exploit this vulnerability?
Any program that renders the affected image types could be vulnerable to this attack. Here are some examples of how an attacker could attempt to exploit this vulnerability:

- An attacker could host a malicious Web site that is designed to exploit this vulnerability through Internet Explorer and then persuade a user to view the Web site.
- An attacker could create an HTML e-mail message that has a specially crafted image attached. The specially crafted image could be designed to exploit this vulnerability through Microsoft Outlook or through Outlook Express 6. An attacker could persuade the user to view the HTML e-mail message.
- An attacker could embed a specially crafted image in an Office document and then persuade the user to view the document.
- An attacker could add a specially crafted image to the local file system or onto a network share and then persuade the user to preview the folder.
- An attacker could locally log on to the system. An attacker could then run a specially-designed program that could exploit the vulnerability.

An attacker could also access the affected component through another vector. For example, an attacker could log on to the system interactively or by using another program that passes parameters to the vulnerable component (locally or remotely). To locally exploit this vulnerability, an attacker would first have to log on to the system.

What systems are primarily at risk from the vulnerability?
The vulnerability could be exploited on the affected systems by an attacker who persuaded a user to open a specially crafted file or to view a folder that contains the specially crafted image. There is no way for an attacker to force a user to open a specially crafted file, except potentially through previewing an email message. Workstations and terminal servers are primarily at risk. Servers could be at more risk if users who do not have sufficient administrative permissions are given the ability to log on to servers and run programs or browse the Internet. However, best practices strongly discourage allowing this.

Could the vulnerability be exploited over the Internet?
Yes. An attacker could try to exploit this vulnerability through malicious Web sites or through email over the Internet.

What does the update do?
The update removes the vulnerability by modifying the way that the affected operating system versions validate the length of a message before it passes the message to the allocated buffer.

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 CAN-2005-0803.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?
No. Microsoft had seen examples of proof of concept code published publicly but had not received any information to indicate that this vulnerability had been publicly used to attack customers when this security bulletin was originally issued.

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 CAN-2005-0803.

↑Top of section

↑Top of section

↑Top of section

⊞ Security Update Information

Affected Software:

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

⊞ Windows Server 2003 (all versions)

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

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.

Supported Security Update Installation Switches	
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 force other applications to close at shutdown without saving open files first.
/warnrestart[:x]	Presents 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 uninstall
/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 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-kb896424-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 KB896424.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-kb896424-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 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%\$NTUninstallKB896424$\Spuninst folder.

Supported Spuninst.exe Switches	
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 force other applications to close at shutdown without saving open files first.
/warnrestart[:x]	Presents 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; and Windows Server 2003, Datacenter Edition with SP1:

File Name	Version	Date	Time	Size	Folder
Gdi32.dll	5.2.3790.419	06-Oct-2005	02:48	271,872	RTMGDR
Win32k.sys	5.2.3790.419	05-Oct-2005	23:51	1,815,552	RTMGDR
Gdi32.dll	5.2.3790.419	06-Oct-2005	02:38	272,384	RTMQFE
Win32k.sys	5.2.3790.419	05-Oct-2005	23:56	1,818,112	RTMQFE

Gdi32.dll	5.2.3790.2542	06-Oct-2005	02:03	281,600	SP1GDR
Win32k.sys	5.2.3790.2542	06-Oct-2005	00:42	1,848,320	SP1GDR
Gdi32.dll	5.2.3790.2542	06-Oct-2005	02:12	281,600	SP1QFE
Win32k.sys	5.2.3790.2542	06-Oct-2005	00:53	1,847,808	SP1QFE
Arpidfix.exe	5.2.3790.2542	06-Oct-2005	00:21	32,256	

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:

File Name	Version	Date	Time	Size	CPU	Folder
Gdi32.dll	5.2.3790.419	06-Oct-2005	03:03	806,912	IA-64	RTMGDR
Win32k.sys	5.2.3790.419	06-Oct-2005	03:03	4,959,744	IA-64	RTMGDR
Wgdi32.dll	5.2.3790.419	06-Oct-2005	03:03	250,880	x86	RTMGDR\WOW
Gdi32.dll	5.2.3790.419	06-Oct-2005	03:03	807,936	IA-64	RTMQFE
Win32k.sys	5.2.3790.419	06-Oct-2005	03:03	4,965,888	IA-64	RTMQFE
Wgdi32.dll	5.2.3790.419	06-Oct-2005	03:03	250,880	x86	RTMQFE\WOW
Gdi32.dll	5.2.3790.2542	06-Oct-2005	03:03	907,264	IA-64	SP1GDR
Win32k.sys	5.2.3790.2542	06-Oct-2005	03:03	5,547,008	IA-64	SP1GDR
Wgdi32.dll	5.2.3790.2542	06-Oct-2005	03:03	285,184	x86	SP1GDR\WOW
Gdi32.dll	5.2.3790.2542	06-Oct-2005	03:03	907,264	IA-64	SP1QFE
Win32k.sys	5.2.3790.2542	06-Oct-2005	03:03	5,545,984	IA-64	SP1QFE
Wgdi32.dll	5.2.3790.2542	06-Oct-2005	03:03	285,184	x86	SP1QFE\WOW
Arpidfix.exe	5.2.3790.2542	06-Oct-2005	03:03	74,752	IA-64	

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

File Name	Version	Date	Time	Size	CPU	Folder
Gdi32.dll	5.2.3790.2542	06-Oct-2005	03:03	609,792	x64	SP1GDR
Win32k.sys	5.2.3790.2542	06-Oct-2005	03:03	4,517,376	x64	SP1GDR
Wgdi32.dll	5.2.3790.2542	06-Oct-2005	03:03	285,184	x86	SP1GDR\WOW
Gdi32.dll	5.2.3790.2542	06-Oct-2005	03:03	609,792	x64	SP1QFE
Win32k.sys	5.2.3790.2542	06-Oct-2005	03:03	4,516,864	x64	SP1QFE

Wgdi32.dll	5.2.3790.2542	06-Oct-2005	03:03	285,184	x86	SP1QFE\WOW
Arpidfix.exe	5.2.3790.2542	06-Oct-2005	03:03	43,008	x64	

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.

Arpidfix.exe is used by the security update installer to address an issue documented in Microsoft Knowledge Base Article 904630. This file is not installed onto the affected system.

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 can use the Microsoft Baseline Security Analyzer (MBSA) tool. MBSA allows administrators to scan local and remote systems for missing security updates and for common security misconfigurations. For more information about MBSA, visit the Microsoft Baseline Security Analyzer Web site.

•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\KB896424\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 896424 security update into the Windows installation source files.

↑Top of section

⊞ 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.

Supported Security Update Installation Switches	
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 force other applications to close at shutdown without saving open files first.
/warnrestart[:x]	Presents 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 uninstall
/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-kb896424-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 KB896424.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-kb896424-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%\$NTUninstallKB896424$\Spuninst folder.

Supported Spuninst.exe Switches	
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 force other applications to close at shutdown without saving open files first.
/warnrestart[:x]	Presents 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:

File Name	Version	Date	Time	Size	Folder
Gdi32.dll	5.1.2600.1755	06-Oct-2005	03:19	260,608	SP1QFE
Mf3216.dll	5.1.2600.1331	30-Mar-2004	01:48	36,864	SP1QFE
User32.dll	5.1.2600.1634	02-Mar-2005	18:20	561,152	SP1QFE
Win32k.sys	5.1.2600.1755	04-Oct-2005	01:38	1,799,552	SP1QFE
Gdi32.dll	5.1.2600.2770	06-Oct-2005	03:09	280,064	SP2GDR
Win32k.sys	5.1.2600.2770	06-Oct-2005	00:05	1,839,488	SP2GDR
Gdi32.dll	5.1.2600.2770	06-Oct-2005	03:18	280,064	SP2QFE
Win32k.sys	5.1.2600.2770	06-Oct-2005	00:10	1,839,360	SP2QFE
Arpidfix.exe	5.1.2600.2770	05-Oct-2005	23:39	30,720	

Windows XP Professional x64:

File Name	Version	Date	Time	Size	CPU	Folder
Gdi32.dll	5.2.3790.2542	06-Oct-2005	03:03	609,792	x64	SP1GDR
Win32k.sys	5.2.3790.2542	06-Oct-2005	03:03	4,517,376	x64	SP1GDR
Wgdi32.dll	5.2.3790.2542	06-Oct-2005	03:03	285,184	x86	SP1GDR\WOW
Gdi32.dll	5.2.3790.2542	06-Oct-2005	03:03	609,792	x64	SP1QFE
Win32k.sys	5.2.3790.2542	06-Oct-2005	03:03	4,516,864	x64	SP1QFE
Wgdi32.dll	5.2.3790.2542	06-Oct-2005	03:03	285,184	x86	SP1QFE\WOW
Arpidfix.exe	5.2.3790.2542	06-Oct-2005	03:03	43,008	x64	

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.

Arpidfix.exe is used by the security update installer to address an issue documented in Microsoft Knowledge Base Article 904630. This file is not installed onto the affected system.

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 can use the Microsoft Baseline Security Analyzer (MBSA) tool. MBSA allows administrators to scan local and remote systems for missing security updates and for common security misconfigurations. For more information about MBSA, visit the Microsoft Baseline Security Analyzer Web site.

•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\KB896424\Filelist

For Windows XP Professional x64 Edition:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\Windows XP Version 2003\SP2\KB896424\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 896424 security update into the Windows installation source files.

Top of section

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.

Supported Security Update Installation Switches	
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 force other applications to close at shutdown without saving open files first.
/warnrestart[:x]	Presents 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 uninstall
/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-kb896424-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 KB896424.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-kb896424-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%\$NTUninstallKB896424$\Spuninst folder.

Supported Spuninst.exe Switches	
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 force other applications to close at shutdown without saving open files first.
/warnrestart[:x]	Presents 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:

File Name	Version	Date	Time	Size	Folder
Gdi32.dll	5.0.2195.7069	07-Oct-2005	06:19	233,744	
Mf3216.dll	5.0.2195.6898	24-Mar-2004	02:17	37,136	
Win32k.sys	5.0.2195.7071	06-Oct-2005	09:33	1,638,672	
Win32k.sys	5.0.2195.7071	06-Oct-2005	09:33	1,638,672	UNIPROC

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 can use the Microsoft Baseline Security Analyzer (MBSA) tool. MBSA allows administrators to scan local and remote systems for missing security updates and for common security misconfigurations. For more information about MBSA, visit the Microsoft Baseline Security Analyzer Web site.

- **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
  \KB896424\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 896424 security update into the Windows installation source files.

Top of section

Top of section

Acknowledgments

Microsoft thanks the following for working with us to help protect customers:

- eEye Digital Security for reporting the Metafile Vulnerability (CAN-2005-2123).
- Venustech ADLab, eEye Digital Security and Peter Ferrie of Symantec Security Response for reporting the Windows Metafile Vulnerability (CAN-2005-2124).

Obtaining Other Security Updates:

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

- Security updates are available in 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.
- 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 Scanning 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 (November 8, 2005): Bulletin published.
•V1.1 (November 30, 2005): Bulletin updated to correct file information for x64 platforms.

Top of page

Manage Your Profile | Contact Us | Newsletter