Security Bulletin

Microsoft Security Bulletin MS09-017 - Critical

Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)

Published: May 12, 2009 | Updated: June 09, 2009

Version: 2.0

General Information

Executive Summary

This security update resolves a publicly disclosed vulnerability and several privately reported vulnerabilities in Microsoft Office PowerPoint that could allow remote code execution if a user opens a specially crafted PowerPoint file. An attacker who successfully exploited any 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. 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.

This security update is rated Critical for supported editions of Microsoft Office PowerPoint 2000. For supported editions of Microsoft Office PowerPoint 2002, Microsoft Office PowerPoint 2003, Microsoft Office PowerPoint 2007, Microsoft Office 2004 for Mac, and Microsoft Office 2008 for Mac; Open XML File Format Converter for Mac; all supported versions of PowerPoint Viewer, and Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats; Microsoft Works 8.5; and Microsoft Works 9, this security update is rated Important. For more information, see the subsection, **Affected and Non-Affected Software**, in this section.

The security update addresses the vulnerabilities by modifying the way that PowerPoint handles conditions that could cause memory corruption when opening specially crafted PowerPoint files. This update also addresses the vulnerabilities by preventing Microsoft Office PowerPoint 2000 and Microsoft Office PowerPoint 2002 from opening PowerPoint 4.0 native file formats. For more information about the vulnerability, see the Frequently Asked Questions (FAQ) subsection for the specific vulnerability entry under the next section, **Vulnerability Information**.

This security update also addresses the vulnerability first described in Microsoft Security Advisory 969136.

Recommendation. Microsoft recommends that customers apply the update immediately.

Known Issues. Microsoft Knowledge Base Article 967340 documents the currently known issues that customers may experience when installing this security update. The article also documents recommended solutions for these issues. When currently known issues and recommended solutions pertain only to specific releases of this software, this article provides links to further articles.

Affected and Non-Affected Software

The following software have been tested to determine which versions or editions are affected. Other versions or editions are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, visit Microsoft Support Lifecycle.

Affected Software

Expand table

Office Suite and Other Software	Component	Maximum Security Impact	Aggregate Severity Rating	Bulletins Replaced by this Update
Microsoft Office Suites and Components				
Microsoft Office 2000 Service Pack 3	Microsoft Office PowerPoint 2000 Service Pack 3 (KB957790)	Remote Code Execution	Critical	MS08-051
Microsoft Office XP Service Pack 3	Microsoft Office PowerPoint 2002 Service Pack 3 (KB957781)	Remote Code Execution	Important	MS08-051
Microsoft Office 2003 Service Pack 3	Microsoft Office PowerPoint 2003 Service Pack 3 (KB957784)	Remote Code Execution	Important	MS08-051
2007 Microsoft Office System Service Pack 1	Microsoft Office PowerPoint 2007 Service Pack 1 (KB957789)	Remote Code Execution	Important	MS08-051
2007 Microsoft Office System Service Pack 2	Microsoft Office PowerPoint 2007 Service Pack 2 (KB957789)	Remote Code Execution	Important	None
Microsoft Office for Mac				
Microsoft Office 2004 for Mac (KB969661)	Not applicable	Remote Code Execution	Important	MS09-009
Microsoft Office 2008 for Mac (KB971822)	Not applicable	Remote Code Execution	Important	MS09-009
Open XML File Format Converter for Mac (KB971824)	Not applicable	Remote Code Execution	Important	MS08-074
Other Office Software				
PowerPoint Viewer 2003 (KB969615)	Not applicable	Remote Code Execution	Important	MS08-052
PowerPoint Viewer 2007 Service Pack 1 and PowerPoint Viewer 2007 Service Pack 2 (KB970059)	Not applicable	Remote Code Execution	Important	None
Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Service Pack 1 (KB969618)	Not applicable	Remote Code Execution	Important	MS08-051

Office Suite and Other Software	Component	Maximum Security Impact	Aggregate Severity Rating	Bulletins Replaced by this Update
Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Service Pack 2 (KB969618)	Not applicable	Remote Code Execution	Important	None
Microsoft Works 8.5 (KB967043)	Not applicable	Remote Code Execution	Important	MS08-072
Microsoft Works 9 (KB967044)	Not applicable	Remote Code Execution	Important	None

Frequently Asked Questions (FAQ) Related to This Security Update

Why was this bulletin rereleased on June 9, 2009? Microsoft rereleased this security bulletin to provide security update packages for Microsoft Office 2004 for Mac, Microsoft Office 2008 for Mac, Open XML File Format Converter for Mac, Microsoft Works 8.5, and Microsoft Works 9. Customers who currently have these software installed need to apply this update immediately. When this bulletin was first released, these security update packages were still in development. At the time, Microsoft released this bulletin because we had update packages ready on the regular bulletin release cycle for an entire product line to address the vast majority of customers at risk. This current release now completes the range of updates for software that are affected by the vulnerabilities discussed in this bulletin.

MS09-021 and MS09-027 also describe vulnerabilities in Microsoft Office 2004 for Mac, Microsoft Office 2008 for Mac, and Open XML File Format Converter for Mac. How do MS09-021 and MS09-027 relate to this bulletin (MS09-017)?
The security update packages for Microsoft Office 2004 for Mac (KB969661), Microsoft Office 2008 for Mac (KB971822), and Open XML File Format Converter for Mac (KB971824) in this bulletin, MS09-017, also address the vulnerabilities described in MS09-021 and MS09-027. Users with Microsoft Office 2004 for Mac, Microsoft Office 2008 for Mac, or Open XML File Format Converter for Mac installed will only need to install the update packages once.

MS09-024 also describes vulnerabilities in Microsoft Works 8.5 and Microsoft Works 9. How does MS09-024 relate to this bulletin (MS09-017)?
The security update packages for Microsoft Works 8.5 (KB967043) and Microsoft Works 9 (KB967044) in this bulletin, MS09-017, also address the vulnerabilities described in MS09-024. Users with Microsoft Works 8.5 or Microsoft Works 9 installed will only need to install the update packages once.

Where are the file information details?
The file information details can be found in Microsoft Knowledge Base Article 967340.

Do users need to make special considerations regarding PowerPoint 4.0 file formats?
With this update, the ability to open PowerPoint 4.0 file formats will be disabled by default in Microsoft Office PowerPoint 2000 and Microsoft Office PowerPoint 2002. This functionality has already been disabled by default in Microsoft Office PowerPoint 2003 Service Pack 3. This functionality also no longer exists in Microsoft Office PowerPoint 2007. For more information regarding this change, please see Microsoft Knowledge Base Article 970980.

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 need to install this update only.

Why is this update Critical for PowerPoint 2000 but only Important for all other affected versions of PowerPoint?
Microsoft Office PowerPoint 2002 and later versions have a built-in feature that prompts a user to Open, Save, or Cancel before opening a document. This mitigating factor reduces the vulnerability from Critical to Important because the vulnerability requires more than a single user action to complete the exploit.

What components of the Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats are updated by this bulletin?
The update included with this security bulletin applies only to the specific component within the Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats that is affected. For example, in an Excel bulletin, only the Excel compatibility pack component files are included in the update packages and not Word or PowerPoint compatibility pack component files. Word compatibility pack component files are updated in a Word bulletin and PowerPoint compatibility pack component files are updated in a PowerPoint bulletin.

The Office component discussed in this article is part of the Office Suite that I have installed on my system; however, I did not choose to install this specific component. Will I be offered this update?
Yes, if the version of the Office Suite installed on your system shipped with the component discussed in this bulletin, the system will be offered updates for it whether the component is installed or not. The detection logic used to scan for affected systems is designed to check for updates for all components that shipped with the particular Office Suite and offer the updates to a system. Users who choose not to apply an update for a component that is not installed, but is included in the version of the Office Suite, will not increase the security risk of that system. However, users who do choose to install the update will not have a negative impact on the security or performance of a system. For more information on this issue, please see Microsoft Knowledge Base Article 830335.

Does the offer to update a non-vulnerable version of Microsoft Office constitute an issue in the Microsoft update mechanism No, the update mechanism is functioning correctly in that it detects a lower version of the files on the system than in the update package and thus, offers the update.

I am using an older release of the software discussed in this security bulletin. What should I do?
The affected software listed in this bulletin have been tested to determine which releases are affected. Other releases are past their support life cycle. To determine the support life cycle for your software release, visit Microsoft Support Lifecycle.

It should be a priority for customers who have older releases of the software to migrate to supported releases to prevent potential exposure to vulnerabilities. For more information about the Windows Product Lifecycle, visit Microsoft Support Lifecycle. For more information about the extended security update support period for these software versions or editions, visit Microsoft Product Support Services.

Customers who require custom support for older releases 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 Microsoft Worldwide Information, 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.

Vulnerability Information

Severity Ratings and Vulnerability Identifiers

The following severity ratings assume the potential maximum impact of the vulnerability. For information regarding the likelihood, within 30 days of this security bulletin's release, of the exploitability of the vulnerability in relation to its severity rating and security impact, please see the Exploitability Index in the May bulletin summary. For more information, see Microsoft Exploitability Index.

Expand table

Affected Software	Legacy File Format Vulnerability - CVE-2009-0220	Integer Overflow Vulnerability - CVE-2009-0221	Legacy File Format Vulnerability - CVE-2009-0222	Legacy File Format Vulnerability - CVE-2009-0223	Memory Corruption Vulnerability - CVE-2009-0224	PP7 Memory Corruption Vulnerability - CVE-2009-0225	Legacy File Format Vulnerability - CVE-2009-0226
Part 1							
Microsoft Office PowerPoint 2000 Service Pack 3	**Critical** Remote Code Execution	Not applicable	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	Not applicable	**Critical** Remote Code Execution
Microsoft Office PowerPoint 2002 Service Pack 3	**Important** Remote Code Execution	**Important** Remote Code Execution	**Important** Remote Code Execution	**Important** Remote Code Execution	**Important** Remote Code Execution	**Important** Remote Code Execution	**Important** Remote Code Execution
Microsoft Office PowerPoint 2003 Service Pack 3	**Moderate** Remote Code Execution	**Important** Remote Code Execution	**Moderate** Remote Code Execution	**Moderate** Remote Code Execution	**Important** Remote Code Execution	Not applicable	**Important** Remote Code Execution
Microsoft Office PowerPoint 2007 Service Pack 1	Not applicable	Not applicable	Not applicable	Not applicable	**Important** Remote Code Execution	Not applicable	Not applicable
Microsoft Office PowerPoint 2007 Service Pack 2	Not applicable	Not applicable	Not applicable	Not applicable	**Important** Remote Code Execution	Not applicable	Not applicable
Microsoft Office 2004 for Mac	Not applicable	Not applicable	Not applicable	Not applicable	**Important** Remote Code Execution	Not applicable	Not applicable
Microsoft Office 2008 for Mac	Not applicable	Not applicable	Not applicable	Not applicable	**Important** Remote Code Execution	Not applicable	Not applicable
Open XML File Format Converter for Mac	Not applicable	Not applicable	Not applicable	Not applicable	**Important** Remote Code Execution	Not applicable	Not applicable
PowerPoint Viewer 2003	Not applicable	Not applicable	Not applicable	Not applicable	**Important** Remote Code Execution	Not applicable	Not applicable
PowerPoint Viewer 2007 Service Pack 1	Not applicable	Not applicable	Not applicable	Not applicable	**Important** Remote Code Execution	Not applicable	Not applicable

Affected Software	Legacy File Format Vulnerability - CVE-2009-0220	Integer Overflow Vulnerability - CVE-2009-0221	Legacy File Format Vulnerability - CVE-2009-0222	Legacy File Format Vulnerability - CVE-2009-0223	Memory Corruption Vulnerability - CVE-2009-0224	PP7 Memory Corruption Vulnerability - CVE-2009-0225	Legacy File Format Vulnerability - CVE-2009-0226
and PowerPoint Viewer 2007 Service Pack 2							
Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Service Pack 1 and Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Service Pack 2	Not applicable	Not applicable	Not applicable	Not applicable	**Important** Remote Code Execution	Not applicable	Not applicable
Microsoft Works 8.5	Not applicable	Not applicable	Not applicable	Not applicable	**Important** Remote Code Execution	Not applicable	Not applicable
Microsoft Works 9	Not applicable	Not applicable	Not applicable	Not applicable	**Important** Remote Code Execution	Not applicable	Not applicable

Expand table

Affected Software	Legacy File Format Vulnerability - CVE-2009-0227	Memory Corruption Vulnerability - CVE-2009-0556	PP7 Memory Corruption Vulnerability - CVE-2009-1128	PP7 Memory Corruption Vulnerability - CVE-2009-1129	Heap Corruption Vulnerability - CVE-2009-1130	Data Out of Bounds Vulnerability - CVE-2009-1131	Legacy File Format Vulnerability - CVE-2009-1137	Aggregate Severity Rating (including Part 1)
Part 2								
Microsoft Office PowerPoint 2000 Service Pack 3	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	Not applicable	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical**
Microsoft Office PowerPoint 2002 Service Pack 3	**Important** Remote Code Execution	**Important** Remote Code Execution	**Important** Remote Code Execution	**Important** Remote Code Execution	**Important** Remote Code Execution	Not applicable	**Important** Remote Code Execution	**Important**

Affected Software	Legacy File Format Vulnerability - CVE-2009-0227	Memory Corruption Vulnerability - CVE-2009-0556	PP7 Memory Corruption Vulnerability - CVE-2009-1128	PP7 Memory Corruption Vulnerability - CVE-2009-1129	Heap Corruption Vulnerability - CVE-2009-1130	Data Out of Bounds Vulnerability - CVE-2009-1131	Legacy File Format Vulnerability - CVE-2009-1137	Aggregate Severity Rating (including Part 1)
Microsoft Office PowerPoint 2003 Service Pack 3	**Moderate** Remote Code Execution	**Important** Remote Code Execution	**Moderate** Remote Code Execution	**Moderate** Remote Code Execution	**Important** Remote Code Execution	Not applicable	**Moderate** Remote Code Execution	**Important**
Microsoft Office PowerPoint 2007 Service Pack 1	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	**Important**
Microsoft Office PowerPoint 2007 Service Pack 2	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	**Important**
Microsoft Office 2004 for Mac	Not applicable	**Important** Remote Code Execution	Not applicable	Not applicable	**Important** Remote Code Execution	Not applicable	Not applicable	**Important**
Microsoft Office 2008 for Mac	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	**Important**
Open XML File Format Converter for Mac	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	**Important**
PowerPoint Viewer 2003	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	**Important**
PowerPoint Viewer 2007 Service Pack 1 and PowerPoint Viewer 2007 Service Pack 2	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	**Important**
Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	**Important**

Affected Software	Legacy File Format Vulnerability - CVE-2009-0227	Memory Corruption Vulnerability - CVE-2009-0556	PP7 Memory Corruption Vulnerability - CVE-2009-1128	PP7 Memory Corruption Vulnerability - CVE-2009-1129	Heap Corruption Vulnerability - CVE-2009-1130	Data Out of Bounds Vulnerability - CVE-2009-1131	Legacy File Format Vulnerability - CVE-2009-1137	Aggregate Severity Rating (including Part 1)
Formats Service Pack 1 and Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Service Pack 2								
Microsoft Works 8.5	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	**Important**
Microsoft Works 9	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	**Important**

Note The Aggregate Severity Rating is the highest severity rating from both Part 1 and Part 2 of the table.

Legacy File Format Vulnerability - CVE-2009-0220

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

To view this vulnerability as a standard entry in the Common Vulnerabilities and Exposures list, see CVE-2009-0220.

Mitigating Factors for Legacy File Format Vulnerability - CVE-2009-0220

Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation:

- Microsoft Office 2003 Service Pack 3 blocks the opening and saving of certain files by default upon installation. For Microsoft Office PowerPoint 2003 Service Pack 3, these are files that are older than PowerPoint 97 and that have file types such as .ppt, .pot, .pps, and .ppa. Notice that this feature does not apply to Microsoft Office PowerPoint 97 files. For more information, see Microsoft Knowledge Base Article 938810.
- Users who have installed and are using the Office Document Open Confirmation Tool for Office 2000 will be prompted with Open, Save, or Cancel before opening a document. The features of the Office Document Open Confirmation Tool are incorporated in Office XP and later editions of Office.
- The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful a user must open an attachment that is sent in an e-mail message.

- In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users 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.
- This vulnerability does not affect PowerPoint 2007, PowerPoint Viewer 2003, and PowerPoint Viewer 2007.

Workarounds for Legacy File Format Vulnerability - CVE-2009-0220

Workaround refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update. Microsoft has tested the following workarounds and states in the discussion whether a workaround reduces functionality:

- **Restrict access to pp4x322.dll in Microsoft Office PowerPoint 2000 or Microsoft Office PowerPoint 2002**

  Note You will need administrator privileges to set these file restrictions.

  - On 32-bit editions of Microsoft Windows 2000, Windows XP and Windows Server 2003, run the following command from a command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

  - On 64-bit editions of Windows XP and Windows Server 2003, run the following command from a command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

  - On 32-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

  - On 64-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

  Impact of Workaround. You will not be able to open PowerPoint 4.0 files.

  How to Undo the Workaround:

  - On 32-bit editions of Microsoft Windows 2000, Windows XP and Windows Server 2003, run the following command from a command prompt:

for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

- On 64-bit editions of Windows XP and Windows Server 2003, run the following command from a command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

- On 32-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

- On 64-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

FAQ for Legacy File Format Vulnerability - CVE-2009-0220

What is the scope of the vulnerability?
This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability 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.

What causes the vulnerability?
When PowerPoint reads paragraph formatting data from specially crafted PowerPoint 4.0 files, an error may corrupt memory in such a way that an attacker could execute arbitrary code.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could take complete control of an affected system in the context of the current logged-on user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

How could an attacker exploit the vulnerability?
This vulnerability requires that a user open a specially crafted PowerPoint 4.0 file with an affected version of Microsoft Office PowerPoint.

In a Web-based attack scenario, a Web site could contain a PowerPoint file that is used to exploit this vulnerability. An attacker would have to convince users to visit the Web site and open a specially crafted PowerPoint file, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site, and then convincing them to open the specially crafted PowerPoint file.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted PowerPoint file to the user and convincing the user to open the file.

What systems are primarily at risk from the vulnerability?
Systems where an affected version of Microsoft Office PowerPoint is used, such as 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.

What does the update do?
This update prevents Microsoft Office PowerPoint 2000 and Microsoft Office PowerPoint 2002 from opening PowerPoint 4.0 native file formats.

When this security bulletin was issued, had this vulnerability been publicly disclosed?
No. Microsoft received information about this vulnerability through responsible disclosure.

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.

Integer Overflow Vulnerability - CVE-2009-0221

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

To view this vulnerability as a standard entry in the Common Vulnerabilities and Exposures list, see CVE-2009-0221.

Mitigating Factors for Integer Overflow Vulnerability - CVE-2009-0221

Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation:

- Microsoft Office 2003 Service Pack 3 blocks the opening and saving of certain files by default upon installation. For Microsoft Office PowerPoint 2003 Service Pack 3, these are files that are older than PowerPoint 97 and that have file types such as .ppt, .pot, .pps, and .ppa. Notice that this feature does not apply to Microsoft Office PowerPoint 97 files. For more information, see Microsoft Knowledge Base Article 938810.
- In a Web-based attack scenario, a Web site could contain a PowerPoint file that is used to exploit this vulnerability. An attacker would have to convince users to visit the Web site and open a specially crafted PowerPoint file, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site, and then convincing them to open the specially crafted PowerPoint file.
- The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful a user must open an attachment that is sent in an e-mail message.
- 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.

Workarounds for Integer Overflow Vulnerability - CVE-2009-0221

Workaround refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update. Microsoft has tested the following workarounds and states in the

discussion whether a workaround reduces functionality:

- **Use the Microsoft Office Isolated Conversion Environment (MOICE) when opening files from unknown or untrusted sources**

  The Microsoft Office Isolated Conversion Environment (MOICE) will protect Office 2003 installations by more securely opening Word, Excel, and PowerPoint binary format files.

  To install MOICE, you must have Office 2003 or 2007 Office system installed.

  To install MOICE, you must have the Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats. The compatibility pack is available as a free download from the Microsoft Download Center:

  Download the FileFormatConverters.exe package now

  MOICE requires all updates that are recommended for all Office programs. Visit Microsoft Update to install all recommended updates:

  https:

  To enable MOICE, change the registered handler for the .ppt, .pot, and .pps file formats. The following table describes the command to enable or to disable MOICE for the .ppt, .pot, and .pps file formats:

Expand table

Command to use to enable MOICE to be the registered handler	Command to use to disable MOICE as the registered handler
ASSOC .PPT=oice.powerpoint.show	ASSOC .ppt=PowerPoint.Show.8
ASSOC .POT=oice.powerpoint.template	ASSOC .pot=PowerPoint.Template.8
ASSOC .PPS=oice.powerpoint.slideshow	ASSOC .pps=PowerPoint.SlideShow.8

Note On Windows Vista and Windows Server 2008, the commands above will need to be run from an elevated command prompt.

For more information on MOICE, see Microsoft Knowledge Base Article 935865.

Impact of Workaround: Office 2003 and earlier formatted documents that are converted to the 2007 Microsoft Office System Open XML format by MOICE will not retain macro functionality. Additionally, documents with passwords or that are protected with Digital Rights Management cannot be converted.

- **Use Microsoft Office File Block policy to block the opening of Office 2003 and earlier documents from unknown or untrusted sources and locations**

  The following registry scripts can be used to set the File Block policy.

  Note Modifying the Registry incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from incorrect modification of the Registry can be solved. Modify the Registry at your own risk.

  - For Office 2003

    Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\PowerPoint\Security\FileOpenBlock]

"BinaryFiles"=dword:00000001

Note In order to use 'FileOpenBlock' with Office 2003, all of the latest Office 2003 security updates must be applied.

Impact of Workaround: Users who have configured the File Block policy and have not configured a special "exempt directory" as discussed in Microsoft Knowledge Base Article 970980 will be unable to open Office 2003 files or earlier versions in Office 2003 or 2007 Microsoft Office System.

How to Undo the Workaround:

- For Office 2003

  Windows Registry Editor Version 5.00

  [HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\PowerPoint\Security\FileOpenBlock]

  "BinaryFiles"=dword:00000000

- Do not open or save Microsoft Office files that you receive from untrusted sources or that you receive unexpectedly from trusted sources. This vulnerability could be exploited when a user opens a specially crafted file.

FAQ for Integer Overflow Vulnerability - CVE-2009-0221

What is the scope of the vulnerability?
This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability 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.

What causes the vulnerability?
When PowerPoint reads an invalid record type in a specially crafted PowerPoint file, an error may corrupt memory in such a way that an attacker could execute arbitrary code.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could take complete control of an affected system in the context of the current logged-on user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

How could an attacker exploit the vulnerability?
This vulnerability requires that a user open a specially crafted PowerPoint file with an affected version of Microsoft Office PowerPoint.

In a Web-based attack scenario, a Web site could contain a PowerPoint file that is used to exploit this vulnerability. An attacker would have to convince users to visit the Web site and open a specially crafted PowerPoint file, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site, and then convincing them to open the specially crafted PowerPoint file.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted PowerPoint file to the user and convincing the user to open the file.

What systems are primarily at risk from the vulnerability?
Systems where an affected version of Microsoft Office PowerPoint is used, such as 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.

What does the update do?
The update modifies the way that PowerPoint validates record types when opening PowerPoint files.

When this security bulletin was issued, had this vulnerability been publicly disclosed?
No. Microsoft received information about this vulnerability through responsible disclosure.

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.

Legacy File Format Vulnerability - CVE-2009-0222

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

To view this vulnerability as a standard entry in the Common Vulnerabilities and Exposures list, see CVE-2009-0222.

Mitigating Factors for Legacy File Format Vulnerability - CVE-2009-0222

Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation:

- Microsoft Office 2003 Service Pack 3 blocks the opening and saving of certain files by default upon installation. For Microsoft Office PowerPoint 2003 Service Pack 3, these are files that are older than PowerPoint 97 and that have file types such as .ppt, .pot, .pps, and .ppa. Notice that this feature does not apply to Microsoft Office PowerPoint 97 files. For more information, see Microsoft Knowledge Base Article 938810.
- Users who have installed and are using the Office Document Open Confirmation Tool for Office 2000 will be prompted with Open, Save, or Cancel before opening a document. The features of the Office Document Open Confirmation Tool are incorporated in Office XP and later editions of Office.
- The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful a user must open an attachment that is sent in an e-mail message.
- In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users 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.
- This vulnerability does not affect PowerPoint 2007, PowerPoint Viewer 2003, and PowerPoint Viewer 2007.

Workarounds for Legacy File Format Vulnerability - CVE-2009-0222

Workaround refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update. Microsoft has tested the following workarounds and states in the discussion whether a workaround reduces functionality:

- **Restrict access to pp4x322.dll in Microsoft Office PowerPoint 2000 or Microsoft Office PowerPoint 2002**

  Note You will need administrator privileges to set these file restrictions.

  - On 32-bit editions of Microsoft Windows 2000, Windows XP and Windows Server 2003, run the following command from a command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

  - On 64-bit editions of Windows XP and Windows Server 2003, run the following command from a command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

  - On 32-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

  - On 64-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

  Impact of Workaround. You will not be able to open PowerPoint 4.0 files.

  How to Undo the Workaround:

  - On 32-bit editions of Microsoft Windows 2000, Windows XP and Windows Server 2003, run the following command from a command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

  - On 64-bit editions of Windows XP and Windows Server 2003, run the following command from a command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

  - On 32-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

- On 64-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

FAQ for Legacy File Format Vulnerability - CVE-2009-0222

What is the scope of the vulnerability?
This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability 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.

What causes the vulnerability?
When PowerPoint reads sound data from specially crafted PowerPoint 4.0 files, an error may corrupt memory in such a way that an attacker could execute arbitrary code.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could take complete control of an affected system in the context of the current logged-on user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

How could an attacker exploit the vulnerability?
This vulnerability requires that a user open a specially crafted PowerPoint 4.0 file with an affected version of Microsoft Office PowerPoint.

In a Web-based attack scenario, a Web site could contain a PowerPoint file that is used to exploit this vulnerability. An attacker would have to convince users to visit the Web site and open a specially crafted PowerPoint file, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site, and then convincing them to open the specially crafted PowerPoint file.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted PowerPoint file to the user and convincing the user to open the file.

What systems are primarily at risk from the vulnerability?
Systems where an affected version of Microsoft Office PowerPoint is used, such as 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.

What does the update do?
This update prevents Microsoft Office PowerPoint 2000 and Microsoft Office PowerPoint 2002 from opening PowerPoint 4.0 native file formats.

When this security bulletin was issued, had this vulnerability been publicly disclosed?
No. Microsoft received information about this vulnerability through responsible disclosure.

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.

Legacy File Format Vulnerability - CVE-2009-0223

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

To view this vulnerability as a standard entry in the Common Vulnerabilities and Exposures list, see CVE-2009-0223.

Mitigating Factors for Legacy File Format Vulnerability - CVE-2009-0223

Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation:

- Microsoft Office 2003 Service Pack 3 blocks the opening and saving of certain files by default upon installation. For Microsoft Office PowerPoint 2003 Service Pack 3, these are files that are older than PowerPoint 97 and that have file types such as .ppt, .pot, .pps, and .ppa. Notice that this feature does not apply to Microsoft Office PowerPoint 97 files. For more information, see Microsoft Knowledge Base Article 938810.
- Users who have installed and are using the Office Document Open Confirmation Tool for Office 2000 will be prompted with Open, Save, or Cancel before opening a document. The features of the Office Document Open Confirmation Tool are incorporated in Office XP and later editions of Office.
- The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful a user must open an attachment that is sent in an e-mail message.
- In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users 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.
- This vulnerability does not affect PowerPoint 2007, PowerPoint Viewer 2003, and PowerPoint Viewer 2007.

Workarounds for Legacy File Format Vulnerability - CVE-2009-0223

Workaround refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update. Microsoft has tested the following workarounds and states in the discussion whether a workaround reduces functionality:

- **Restrict access to pp4x322.dll in Microsoft Office PowerPoint 2000 or Microsoft Office PowerPoint 2002**

  Note You will need administrator privileges to set these file restrictions.

- On 32-bit editions of Microsoft Windows 2000, Windows XP and Windows Server 2003, run the following command from a command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

- On 64-bit editions of Windows XP and Windows Server 2003, run the following command from a command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

- On 32-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

- On 64-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

Impact of Workaround. You will not be able to open PowerPoint 4.0 files.

How to Undo the Workaround:

- On 32-bit editions of Microsoft Windows 2000, Windows XP and Windows Server 2003, run the following command from a command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

- On 64-bit editions of Windows XP and Windows Server 2003, run the following command from a command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

- On 32-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

- On 64-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

FAQ for Legacy File Format Vulnerability - CVE-2009-0223

What is the scope of the vulnerability?
This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability 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.

What causes the vulnerability?
When PowerPoint reads sound data from specially crafted PowerPoint 4.0 files, an error may corrupt memory in such a way that an attacker could execute arbitrary code.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could take complete control of an affected system in the context of the current logged-on user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

How could an attacker exploit the vulnerability?
This vulnerability requires that a user open a specially crafted PowerPoint 4.0 file with an affected version of Microsoft Office PowerPoint.

In a Web-based attack scenario, a Web site could contain a PowerPoint file that is used to exploit this vulnerability. An attacker would have to convince users to visit the Web site and open a specially crafted PowerPoint file, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site, and then convincing them to open the specially crafted PowerPoint file.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted PowerPoint file to the user and convincing the user to open the file.

What systems are primarily at risk from the vulnerability?
Systems where an affected version of Microsoft Office PowerPoint is used, such as 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.

What does the update do?
This update prevents Microsoft Office PowerPoint 2000 and Microsoft Office PowerPoint 2002 from opening PowerPoint 4.0 native file formats.

When this security bulletin was issued, had this vulnerability been publicly disclosed?
No. Microsoft received information about this vulnerability through responsible disclosure.

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.

Memory Corruption Vulnerability - CVE-2009-0224

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be

included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

To view this vulnerability as a standard entry in the Common Vulnerabilities and Exposures list, see CVE-2009-0224.

Mitigating Factors for Memory Corruption Vulnerability - CVE-2009-0224

Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation:

- Users who have installed and are using the Office Document Open Confirmation Tool for Office 2000 will be prompted with Open, Save, or Cancel before opening a document. The features of the Office Document Open Confirmation Tool are incorporated in Office XP and later editions of Office.
- The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful, a user must open an attachment that is sent in an e-mail message.
- In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users 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.

Workarounds for Memory Corruption Vulnerability - CVE-2009-0224

Workaround refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update. Microsoft has tested the following workarounds and states in the discussion whether a workaround reduces functionality:

- **Use the Microsoft Office Isolated Conversion Environment (MOICE) when opening files from unknown or untrusted sources**

  The Microsoft Office Isolated Conversion Environment (MOICE) will protect Office 2003 installations by more securely opening Word, Excel, and PowerPoint binary format files.

  To install MOICE, you must have Office 2003 or 2007 Office system installed.

  To install MOICE, you must have the Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats. The compatibility pack is available as a free download from the Microsoft Download Center:

  Download the FileFormatConverters.exe package now

  MOICE requires all updates that are recommended for all Office programs. Visit Microsoft Update to install all recommended updates:

  </https:>https:

  To enable MOICE, change the registered handler for the .ppt, .pot, and .pps file formats. The following table describes the command to enable or to disable MOICE for the .ppt, .pot, and .pps file formats:

Expand table

Command to use to enable MOICE to be the registered handler	Command to use to disable MOICE as the registered handler
ASSOC .PPT=oice.powerpoint.show	ASSOC .ppt=PowerPoint.Show.8
ASSOC .POT=oice.powerpoint.template	ASSOC .pot=PowerPoint.Template.8
ASSOC .PPS=oice.powerpoint.slideshow	ASSOC .pps=PowerPoint.SlideShow.8

Note On Windows Vista and Windows Server 2008, the commands above will need to be run from an elevated command prompt.

For more information on MOICE, see Microsoft Knowledge Base Article 935865.

Impact of Workaround: Office 2003 and earlier formatted documents that are converted to the 2007 Microsoft Office System Open XML format by MOICE will not retain macro functionality. Additionally, documents with passwords or that are protected with Digital Rights Management cannot be converted.

- **Use Microsoft Office File Block policy to block the opening of Office 2003 and earlier documents from unknown or untrusted sources and locations**

  The following registry scripts can be used to set the File Block policy.

  Note Modifying the Registry incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from incorrect modification of the Registry can be solved. Modify the Registry at your own risk.

  - For Office 2003

    Windows Registry Editor Version 5.00

    [HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\PowerPoint\Security\FileOpenBlock]

    "BinaryFiles"=dword:00000001

    Note In order to use 'FileOpenBlock' with Office 2003, all of the latest Office 2003 security updates must be applied.

  Impact of Workaround: Users who have configured the File Block policy and have not configured a special "exempt directory" as discussed in Microsoft Knowledge Base Article 970980 will be unable to open Office 2003 files or earlier versions in Office 2003 or 2007 Microsoft Office System.

  How to Undo the Workaround:

  - For Office 2003

    Windows Registry Editor Version 5.00

    [HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\PowerPoint\Security\FileOpenBlock]

    "BinaryFiles"=dword:00000000

- Do not open or save Microsoft Office files that you receive from untrusted sources or that you receive unexpectedly from trusted sources. This vulnerability could be exploited when a user opens a specially crafted file.

FAQ for Memory Corruption Vulnerability - CVE-2009-0224

What is the scope of the vulnerability?
This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability 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.

What causes the vulnerability?
When PowerPoint reads an invalid record type in a specially crafted PowerPoint file, an error may corrupt memory in such a way that an attacker could execute arbitrary code.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could take complete control of an affected system in the context of the current logged-on user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

How could an attacker exploit the vulnerability?
This vulnerability requires that a user open a specially crafted PowerPoint file with an affected version of Microsoft Office PowerPoint.

In a Web-based attack scenario, a Web site could contain a PowerPoint file that is used to exploit this vulnerability. An attacker would have to convince users to visit the Web site and open a specially crafted PowerPoint file, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site, and then convincing them to open the specially crafted PowerPoint file.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted PowerPoint file to the user and convincing the user to open the file.

What systems are primarily at risk from the vulnerability?
Systems where an affected version of Microsoft Office PowerPoint is used, such as 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.

What does the update do?
The update modifies the way that PowerPoint validates list records when opening PowerPoint files.

When this security bulletin was issued, had this vulnerability been publicly disclosed?
No. Microsoft received information about this vulnerability through responsible disclosure.

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.

PP7 Memory Corruption Vulnerability - CVE-2009-0225

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

To view this vulnerability as a standard entry in the Common Vulnerabilities and Exposures list, see CVE-2009-0225.

Mitigating Factors for PP7 Memory Corruption Vulnerability - CVE-2009-0225

Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation:

- The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful a user must open an attachment that is sent in an e-mail message.
- In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users 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.
- This vulnerability does not affect PowerPoint 2000, PowerPoint 2003, PowerPoint 2007, PowerPoint Viewer 2003, and PowerPoint Viewer 2007.

Workarounds for PP7 Memory Corruption Vulnerability - CVE-2009-0225

Workaround refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update. Microsoft has tested the following workarounds and states in the discussion whether a workaround reduces functionality:

- **Restrict access to pp7x32.dll in Microsoft Office PowerPoint 2002**

  Note You will need administrator privileges to set these file restrictions.

  - On 32-bit editions of Microsoft Windows 2000, Windows XP and Windows Server 2003, run the following command from a command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /P everyone:N

  - On 64-bit editions of Windows XP and Windows Server 2003, run the following command from a command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /P everyone:N

  - On 32-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /P everyone:N

- On 64-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /P everyone:N

Impact of Workaround. You will not be able to open PowerPoint 95 files.

How to Undo the Workaround:

- On 32-bit editions of Microsoft Windows 2000, Windows XP and Windows Server 2003, run the following command from a command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /R everyone

- On 64-bit editions of Windows XP and Windows Server 2003, run the following command from a command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /R everyone

- On 32-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /R everyone

- On 64-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /R everyone

FAQ for PP7 Memory Corruption Vulnerability - CVE-2009-0225

What is the scope of the vulnerability?
This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability 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.

What causes the vulnerability?
When PowerPoint reads sound data from specially crafted PowerPoint 95 files, an error may corrupt memory in such a way that an attacker could execute arbitrary code.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could take complete control of an affected system in the context of the current logged-on user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

How could an attacker exploit the vulnerability?
This vulnerability requires that a user open a specially crafted PowerPoint 95 file with an affected version of Microsoft Office PowerPoint.

In a Web-based attack scenario, a Web site could contain a PowerPoint file that is used to exploit this vulnerability. An attacker would have to convince users to visit the Web site and open a specially crafted PowerPoint file, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site, and then convincing them to open the specially crafted PowerPoint file.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted PowerPoint file to the user and convincing the user to open the file.

What systems are primarily at risk from the vulnerability?
Systems where an affected version of Microsoft Office PowerPoint is used, such as 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.

What does the update do?
This update modifies the way that Microsoft Office PowerPoint 2002 opens PowerPoint 95 native file formats.

When this security bulletin was issued, had this vulnerability been publicly disclosed?
No. Microsoft received information about this vulnerability through responsible disclosure.

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.

Legacy File Format Vulnerability - CVE-2009-0226

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

To view this vulnerability as a standard entry in the Common Vulnerabilities and Exposures list, see CVE-2009-0226.

Mitigating Factors for Legacy File Format Vulnerability - CVE-2009-0226

Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation:

- Microsoft Office 2003 Service Pack 3 blocks the opening and saving of certain files by default upon installation. For Microsoft Office PowerPoint 2003 Service Pack 3, these are files that are older than PowerPoint 97 and that have file types such as .ppt, .pot, .pps, and .ppa. Notice that this feature does not apply to Microsoft Office PowerPoint 97 files. For more information, see Microsoft Knowledge Base Article 938810.
- Users who have installed and are using the Office Document Open Confirmation Tool for Office 2000 will be prompted with Open, Save, or Cancel before opening a document. The features of the Office Document Open Confirmation Tool are incorporated in Office XP and later editions of Office.

- The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful a user must open an attachment that is sent in an e-mail message.
- In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users 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.
- This vulnerability does not affect PowerPoint 2007, PowerPoint Viewer 2003, and PowerPoint Viewer 2007.

Workarounds for Legacy File Format Vulnerability - CVE-2009-0226

Workaround refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update. Microsoft has tested the following workarounds and states in the discussion whether a workaround reduces functionality:

- **Restrict access to pp4x322.dll in Microsoft Office PowerPoint 2000 or Microsoft Office PowerPoint 2002**

  Note You will need administrator privileges to set these file restrictions.

  - On 32-bit editions of Microsoft Windows 2000, Windows XP and Windows Server 2003, run the following command from a command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

  - On 64-bit editions of Windows XP and Windows Server 2003, run the following command from a command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

  - On 32-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

  - On 64-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

  Impact of Workaround. You will not be able to open PowerPoint 4.0 files.

  How to Undo the Workaround:

- On 32-bit editions of Microsoft Windows 2000, Windows XP and Windows Server 2003, run the following command from a command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

- On 64-bit editions of Windows XP and Windows Server 2003, run the following command from a command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

- On 32-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

- On 64-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

FAQ for Legacy File Format Vulnerability - CVE-2009-0226

What is the scope of the vulnerability?
This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability 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.

What causes the vulnerability?
When PowerPoint reads sound data from specially crafted PowerPoint 4.0 files, an error may corrupt memory in such a way that an attacker could execute arbitrary code.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could take complete control of an affected system in the context of the current logged-on user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

How could an attacker exploit the vulnerability?
This vulnerability requires that a user open a specially crafted PowerPoint 4.0 file with an affected version of Microsoft Office PowerPoint.

In a Web-based attack scenario, a Web site could contain a PowerPoint file that is used to exploit this vulnerability. An attacker would have to convince users to visit the Web site and open a specially crafted PowerPoint file, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site, and then convincing them to open the specially crafted PowerPoint file.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted PowerPoint file to the user and convincing the user to open the file.

What systems are primarily at risk from the vulnerability?
Systems where an affected version of Microsoft Office PowerPoint is used, such as 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.

What does the update do?
This update prevents Microsoft Office PowerPoint 2000 and Microsoft Office PowerPoint 2002 from opening PowerPoint 4.0 native file formats.

When this security bulletin was issued, had this vulnerability been publicly disclosed?
No. Microsoft received information about this vulnerability through responsible disclosure.

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.

Legacy File Format Vulnerability - CVE-2009-0227

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

To view this vulnerability as a standard entry in the Common Vulnerabilities and Exposures list, see CVE-2009-0227.

Mitigating Factors for Legacy File Format Vulnerability - CVE-2009-0227

Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation:

- Microsoft Office 2003 Service Pack 3 blocks the opening and saving of certain files by default upon installation. For Microsoft Office PowerPoint 2003 Service Pack 3, these are files that are older than PowerPoint 97 and that have file types such as .ppt, .pot, .pps, and .ppa. Notice that this feature does not apply to Microsoft Office PowerPoint 97 files. For more information, see Microsoft Knowledge Base Article 938810.
- Users who have installed and are using the Office Document Open Confirmation Tool for Office 2000 will be prompted with Open, Save, or Cancel before opening a document. The features of the Office Document Open Confirmation Tool are incorporated in Office XP and later editions of Office.
- The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful a user must open an attachment that is sent in an e-mail message.
- In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users 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.
- This vulnerability does not affect PowerPoint 2007, PowerPoint Viewer 2003, and PowerPoint Viewer 2007.

Workarounds for Legacy File Format Vulnerability - CVE-2009-0227

Workaround refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update. Microsoft has tested the following workarounds and states in the discussion whether a workaround reduces functionality:

- **Restrict access to pp4x322.dll in Microsoft Office PowerPoint 2000 or Microsoft Office PowerPoint 2002**

  Note You will need administrator privileges to set these file restrictions.

  - On 32-bit editions of Microsoft Windows 2000, Windows XP and Windows Server 2003, run the following command from a command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

  - On 64-bit editions of Windows XP and Windows Server 2003, run the following command from a command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

  - On 32-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

  - On 64-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

  Impact of Workaround. You will not be able to open PowerPoint 4.0 files.

  How to Undo the Workaround:

  - On 32-bit editions of Microsoft Windows 2000, Windows XP and Windows Server 2003, run the following command from a command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

  - On 64-bit editions of Windows XP and Windows Server 2003, run the following command from a command prompt:

for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

- On 32-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

- On 64-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

FAQ for Legacy File Format Vulnerability - CVE-2009-0227

What is the scope of the vulnerability?
This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability 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.

What causes the vulnerability?
When PowerPoint reads sound data from specially crafted PowerPoint 4.0 files, an error may corrupt memory in such a way that an attacker could execute arbitrary code.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could take complete control of an affected system in the context of the current logged-on user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

How could an attacker exploit the vulnerability?
This vulnerability requires that a user open a specially crafted PowerPoint 4.0 file with an affected version of Microsoft Office PowerPoint.

In a Web-based attack scenario, a Web site could contain a PowerPoint file that is used to exploit this vulnerability. An attacker would have to convince users to visit the Web site and open a specially crafted PowerPoint file, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site, and then convincing them to open the specially crafted PowerPoint file.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted PowerPoint file to the user and convincing the user to open the file.

What systems are primarily at risk from the vulnerability?
Systems where an affected version of Microsoft Office PowerPoint is used, such as 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.

What does the update do?
This update prevents Microsoft Office PowerPoint 2000 and Microsoft Office PowerPoint 2002 from opening PowerPoint

4.0 native file formats.

When this security bulletin was issued, had this vulnerability been publicly disclosed?
No. Microsoft received information about this vulnerability through responsible disclosure.

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.

Memory Corruption Vulnerability - CVE-2009-0556

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

To view this vulnerability as a standard entry in the Common Vulnerabilities and Exposures list, see CVE-2009-0556.

Mitigating Factors for Memory Corruption Vulnerability - CVE-2009-0556

Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation:

- Users who have installed and are using the Office Document Open Confirmation Tool for Office 2000 will be prompted with Open, Save, or Cancel before opening a document. The features of the Office Document Open Confirmation Tool are incorporated in Office XP and later editions of Office.
- The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful, a user must open an attachment that is sent in an e-mail message.
- In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users 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.

Workarounds for Memory Corruption Vulnerability - CVE-2009-0556

Workaround refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update. Microsoft has tested the following workarounds and states in the discussion whether a workaround reduces functionality:

- **Use the Microsoft Office Isolated Conversion Environment (MOICE) when opening files from unknown or untrusted sources**

The Microsoft Office Isolated Conversion Environment (MOICE) will protect Office 2003 installations by more securely opening Word, Excel, and PowerPoint binary format files.

To install MOICE, you must have Office 2003 or 2007 Office system installed.

To install MOICE, you must have the Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats. The compatibility pack is available as a free download from the Microsoft Download Center:

Download the FileFormatConverters.exe package now

MOICE requires all updates that are recommended for all Office programs. Visit Microsoft Update to install all recommended updates:

</https:>https:

To enable MOICE, change the registered handler for the .ppt, .pot, and .pps file formats. The following table describes the command to enable or to disable MOICE for the .ppt, .pot, and .pps file formats:

Expand table

Command to use to enable MOICE to be the registered handler	Command to use to disable MOICE as the registered handler
ASSOC .PPT=oice.powerpoint.show	ASSOC .ppt=PowerPoint.Show.8
ASSOC .POT=oice.powerpoint.template	ASSOC .pot=PowerPoint.Template.8
ASSOC .PPS=oice.powerpoint.slideshow	ASSOC .pps=PowerPoint.SlideShow.8

Note On Windows Vista and Windows Server 2008, the commands above will need to be run from an elevated command prompt.

For more information on MOICE, see Microsoft Knowledge Base Article 935865 .

Impact of Workaround: Office 2003 and earlier formatted documents that are converted to the 2007 Microsoft Office System Open XML format by MOICE will not retain macro functionality. Additionally, documents with passwords or that are protected with Digital Rights Management cannot be converted.

- **Use Microsoft Office File Block policy to block the opening of Office 2003 and earlier documents from unknown or untrusted sources and locations**

  The following registry scripts can be used to set the File Block policy.

  Note Modifying the Registry incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from incorrect modification of the Registry can be solved. Modify the Registry at your own risk.

  - For Office 2003

    Windows Registry Editor Version 5.00

    [HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\PowerPoint\Security\FileOpenBlock]

    "BinaryFiles"=dword:00000001

Note In order to use 'FileOpenBlock' with Office 2003, all of the latest Office 2003 security updates must be applied.

Impact of Workaround: Users who have configured the File Block policy and have not configured a special "exempt directory" as discussed in Microsoft Knowledge Base Article 970980 will be unable to open Office 2003 files or earlier versions in Office 2003 or 2007 Microsoft Office System.

How to Undo the Workaround:

- For Office 2003

  Windows Registry Editor Version 5.00

  [HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\PowerPoint\Security\FileOpenBlock]

  "BinaryFiles"=dword:00000000

- Do not open or save Microsoft Office files that you receive from untrusted sources or that you receive unexpectedly from trusted sources. This vulnerability could be exploited when a user opens a specially crafted file.

FAQ for Memory Corruption Vulnerability - CVE-2009-0556

What is the scope of the vulnerability?
This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability 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.

What causes the vulnerability?
The vulnerability is caused by memory corruption when PowerPoint reads an invalid index value in a specially crafted PowerPoint file. The resulting error may corrupt memory in such a way that an attacker could execute arbitrary code.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could take complete control of an affected system in the context of the logged-in user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

How could an attacker exploit the vulnerability?
This vulnerability requires that a user open a specially crafted PowerPoint file with an affected version of Microsoft Office PowerPoint.

In a Web-based attack scenario, a Web site could contain a PowerPoint file that is used to exploit this vulnerability. An attacker would have to convince users to visit the Web site and open a specially crafted PowerPoint file, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site, and then convincing them to open the specially crafted PowerPoint file.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted PowerPoint file to the user and convincing the user to open the file.

What systems are primarily at risk from the vulnerability?
Systems where an affected version of Microsoft Office PowerPoint is used, such as 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.

What does the update do?
The update removes the vulnerability by modifying the way that PowerPoint validates memory allocations when opening PowerPoint files.

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-2009-0556. This vulnerability was first described in Microsoft Security Advisory 969136.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?
Yes. Microsoft is aware of limited, targeted attacks attempting to exploit the vulnerability.

PP7 Memory Corruption Vulnerability - CVE-2009-1128

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

To view this vulnerability as a standard entry in the Common Vulnerabilities and Exposures list, see CVE-2009-1128.

Mitigating Factors for PP7 Memory Corruption Vulnerability - CVE-2009-1128

Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation:

- Microsoft Office 2003 Service Pack 3 blocks the opening and saving of certain files by default upon installation. For Microsoft Office PowerPoint 2003 Service Pack 3, these are files that are older than PowerPoint 97 and that have file types such as .ppt, .pot, .pps, and .ppa. Notice that this feature does not apply to Microsoft Office PowerPoint 97 files. For more information, see Microsoft Knowledge Base Article 938810.
- Users who have installed and are using the Office Document Open Confirmation Tool for Office 2000 will be prompted with Open, Save, or Cancel before opening a document. The features of the Office Document Open Confirmation Tool are incorporated in Office XP and later editions of Office.
- The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful a user must open an attachment that is sent in an e-mail message.
- In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users 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.
- This vulnerability does not affect PowerPoint 2007, PowerPoint Viewer 2003, and PowerPoint Viewer 2007.

Workarounds for PP7 Memory Corruption Vulnerability - CVE-2009-1128

Workaround refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update. Microsoft has tested the following workarounds and states in the discussion whether a workaround reduces functionality:

- **Restrict access to pp7x32.dll in Microsoft Office PowerPoint 2000 or Microsoft Office PowerPoint 2002**

  Note You will need administrator privileges to set these file restrictions.

  - On 32-bit editions of Microsoft Windows 2000, Windows XP and Windows Server 2003, run the following command from a command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /P everyone:N

  - On 64-bit editions of Windows XP and Windows Server 2003, run the following command from a command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /P everyone:N

  - On 32-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /P everyone:N

  - On 64-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /P everyone:N

  Impact of Workaround. You will not be able to open PowerPoint 95 files.

  How to Undo the Workaround:

  - On 32-bit editions of Microsoft Windows 2000, Windows XP and Windows Server 2003, run the following command from a command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /R everyone

  - On 64-bit editions of Windows XP and Windows Server 2003, run the following command from a command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /R everyone

  - On 32-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /R everyone

- On 64-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /R everyone

FAQ for PP7 Memory Corruption Vulnerability - CVE-2009-1128

What is the scope of the vulnerability?
This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability 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.

What causes the vulnerability?
This vulnerability causes memory corruption when reading sound data from specially crafted older PowerPoint 95 formatted files.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could take complete control of an affected system in the context of the logged-on user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

How could an attacker exploit the vulnerability?
This vulnerability requires that a user open a specially crafted PowerPoint file with an affected version of Microsoft Office PowerPoint.

In a Web-based attack scenario, a Web site could contain a PowerPoint file that is used to exploit this vulnerability. An attacker would have to convince users to visit the Web site and open a specially crafted PowerPoint file, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site, and then convincing them to open the specially crafted PowerPoint file.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted PowerPoint file to the user and convincing the user to open the file.

What systems are primarily at risk from the vulnerability?
Systems where an affected version of Microsoft Office PowerPoint is used, such as 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.

What does the update do?
This update modifies the way that Microsoft Office PowerPoint 2000, Microsoft Office PowerPoint 2002, and Microsoft Office PowerPoint 2003 open PowerPoint 95 native file formats.

When this security bulletin was issued, had this vulnerability been publicly disclosed?
No. Microsoft received information about this vulnerability through responsible disclosure.

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.

PP7 Memory Corruption Vulnerability - CVE-2009-1129

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

To view this vulnerability as a standard entry in the Common Vulnerabilities and Exposures list, see CVE-2009-1129.

Mitigating Factors for PP7 Memory Corruption Vulnerability - CVE-2009-1129

Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation:

- Microsoft Office 2003 Service Pack 3 blocks the opening and saving of certain files by default upon installation. For Microsoft Office PowerPoint 2003 Service Pack 3, these are files that are older than PowerPoint 97 and that have file types such as .ppt, .pot, .pps, and .ppa. Notice that this feature does not apply to Microsoft Office PowerPoint 97 files. For more information, see Microsoft Knowledge Base Article 938810.
- Users who have installed and are using the Office Document Open Confirmation Tool for Office 2000 will be prompted with Open, Save, or Cancel before opening a document. The features of the Office Document Open Confirmation Tool are incorporated in Office XP and later editions of Office.
- The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful a user must open an attachment that is sent in an e-mail message.
- In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users 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.
- This vulnerability does not affect PowerPoint 2007, PowerPoint Viewer 2003, and PowerPoint Viewer 2007.

Workarounds for PP7 Memory Corruption Vulnerability - CVE-2009-1129

Workaround refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update. Microsoft has tested the following workarounds and states in the discussion whether a workaround reduces functionality:

- **Restrict access to pp7x32.dll in Microsoft Office PowerPoint 2000 or Microsoft Office PowerPoint 2002**

  Note You will need administrator privileges to set these file restrictions.

- On 32-bit editions of Microsoft Windows 2000, Windows XP and Windows Server 2003, run the following command from a command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /P everyone:N

- On 64-bit editions of Windows XP and Windows Server 2003, run the following command from a command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /P everyone:N

- On 32-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /P everyone:N

- On 64-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /P everyone:N

Impact of Workaround. You will not be able to open PowerPoint 95 files.

How to Undo the Workaround:

- On 32-bit editions of Microsoft Windows 2000, Windows XP and Windows Server 2003, run the following command from a command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /R everyone

- On 64-bit editions of Windows XP and Windows Server 2003, run the following command from a command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /R everyone

- On 32-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /R everyone

- On 64-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp7x32.dll^"') DO cacls "%G" /E /R everyone

FAQ for PP7 Memory Corruption Vulnerability - CVE-2009-1129

What is the scope of the vulnerability?
This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability 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.

What causes the vulnerability?
This vulnerability causes memory corruption when reading sound data from specially crafted older PowerPoint 95 formatted files.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could take complete control of an affected system in the context of the logged-on user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

How could an attacker exploit the vulnerability?
This vulnerability requires that a user open a specially crafted PowerPoint file with an affected version of Microsoft Office PowerPoint

In a Web-based attack scenario, a Web site could contain a PowerPoint file that is used to exploit this vulnerability. An attacker would have to convince users to visit the Web site and open a specially crafted PowerPoint file, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site, and then convincing them to open the specially crafted PowerPoint file.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted PowerPoint file to the user and convincing the user to open the file.

What systems are primarily at risk from the vulnerability?
Systems where an affected version of Microsoft Office PowerPoint is used, such as 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.

What does the update do?
This update modifies the way that Microsoft Office PowerPoint 2000, Microsoft Office PowerPoint 2002, and Microsoft Office PowerPoint 2003 open PowerPoint 95 native file formats.

When this security bulletin was issued, had this vulnerability been publicly disclosed?
No. Microsoft received information about this vulnerability through responsible disclosure.

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.

Heap Corruption Vulnerability - CVE-2009-1130

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be

included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

To view this vulnerability as a standard entry in the Common Vulnerabilities and Exposures list, see CVE-2009-1130 .

Mitigating Factors for Heap Corruption Vulnerability - CVE-2009-1130

Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation:

- The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful, a user must open an attachment that is sent in an e-mail message.
- In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users 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.

Workarounds for Heap Corruption Vulnerability - CVE-2009-1130

Workaround refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update. Microsoft has tested the following workarounds and states in the discussion whether a workaround reduces functionality:

- **Use the Microsoft Office Isolated Conversion Environment (MOICE) when opening files from unknown or untrusted sources**

  The Microsoft Office Isolated Conversion Environment (MOICE) will protect Office 2003 installations by more securely opening Word, Excel, and PowerPoint binary format files.

  To install MOICE, you must have Office 2003 or 2007 Office system installed.

  To install MOICE, you must have the Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats. The compatibility pack is available as a free download from the Microsoft Download Center:

  Download the FileFormatConverters.exe package now

  MOICE requires all updates that are recommended for all Office programs. Visit Microsoft Update to install all recommended updates:

  </https:>https:

  To enable MOICE, change the registered handler for the .ppt, .pot, and .pps file formats. The following table describes the command to enable or to disable MOICE for the .ppt, .pot, and .pps file formats:

Expand table

Command to use to enable MOICE to be the registered handler	Command to use to disable MOICE as the registered handler
ASSOC .PPT=oice.powerpoint.show	ASSOC .ppt=PowerPoint.Show.8
ASSOC .POT=oice.powerpoint.template	ASSOC .pot=PowerPoint.Template.8
ASSOC .PPS=oice.powerpoint.slideshow	ASSOC .pps=PowerPoint.SlideShow.8

Note On Windows Vista and Windows Server 2008, the commands above will need to be run from an elevated command prompt.

For more information on MOICE, see Microsoft Knowledge Base Article 935865 .

Impact of Workaround: Office 2003 and earlier formatted documents that are converted to the 2007 Microsoft Office System Open XML format by MOICE will not retain macro functionality. Additionally, documents with passwords or that are protected with Digital Rights Management cannot be converted.

- **Use Microsoft Office File Block policy to block the opening of Office 2003 and earlier documents from unknown or untrusted sources and locations**

  The following registry scripts can be used to set the File Block policy.

  Note Modifying the Registry incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from incorrect modification of the Registry can be solved. Modify the Registry at your own risk.

  - For Office 2003

    Windows Registry Editor Version 5.00

    [HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\PowerPoint\Security\FileOpenBlock]

    "BinaryFiles"=dword:00000001

    Note In order to use 'FileOpenBlock' with Office 2003, all of the latest Office 2003 security updates must be applied.

  Impact of Workaround: Users who have configured the File Block policy and have not configured a special “exempt directory” as discussed in Microsoft Knowledge Base Article 970980 will be unable to open Office 2003 files or earlier versions in Office 2003 or 2007 Microsoft Office System.

  How to Undo the Workaround:

  - For Office 2003

    Windows Registry Editor Version 5.00

    [HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\PowerPoint\Security\FileOpenBlock]

    "BinaryFiles"=dword:00000000

- Do not open or save Microsoft Office files that you receive from untrusted sources or that you receive unexpectedly from trusted sources. This vulnerability could be exploited when a user opens a specially crafted file.

FAQ for Heap Corruption Vulnerability - CVE-2009-1130

What is the scope of the vulnerability?
This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability 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.

What causes the vulnerability?
The vulnerability is caused by memory corruption when PowerPoint reads a malformed structure value in a specially crafted PowerPoint file. The resulting error may corrupt memory in such a way that an attacker could execute arbitrary code.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could take complete control of an affected system in the context of the logged-on user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

How could an attacker exploit the vulnerability?
This vulnerability requires that a user open a specially crafted PowerPoint file with an affected version of Microsoft Office PowerPoint

In a Web-based attack scenario, a Web site could contain a PowerPoint file that is used to exploit this vulnerability. An attacker would have to convince users to visit the Web site and open a specially crafted PowerPoint file, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site, and then convincing them to open the specially crafted PowerPoint file.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted PowerPoint file to the user and convincing the user to open the file.

What systems are primarily at risk from the vulnerability?
Systems where an affected version of Microsoft Office PowerPoint is used, such as 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.

What does the update do?
The update addresses the vulnerability by modifying the way that Microsoft Office PowerPoint validates the vulnerable memory structure when opening PowerPoint files.

When this security bulletin was issued, had this vulnerability been publicly disclosed?
No. Microsoft received information about this vulnerability through responsible disclosure.

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.

Data Out of Bounds Vulnerability - CVE-2009-1131

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

To view this vulnerability as a standard entry in the Common Vulnerabilities and Exposures list, see CVE-2009-1131.

Mitigating Factors for Data Out of Bounds Vulnerability - CVE-2009-1131

Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation:

- Users who have installed and are using the Office Document Open Confirmation Tool for Office 2000 will be prompted with Open, Save, or Cancel before opening a document. The features of the Office Document Open Confirmation Tool are incorporated in Office XP and later editions of Office.
- The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful, a user must open an attachment that is sent in an e-mail message.
- In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users 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.

Workarounds for Data Out of Bounds Vulnerability - CVE-2009-1131

Workaround refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update. Microsoft has tested the following workarounds and states in the discussion whether a workaround reduces functionality:

- Do not open or save Microsoft Office files that you receive from untrusted sources or that you receive unexpectedly from trusted sources. This vulnerability could be exploited when a user opens a specially crafted file.

FAQ for Data Out of Bounds Vulnerability - CVE-2009-1131

What is the scope of the vulnerability?
This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability 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.

What causes the vulnerability?
When Microsoft Office PowerPoint reads data that is too large in a specially crafted PowerPoint file, an error may corrupt memory in such a way that an attacker could execute arbitrary code.

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

of the logged-on in user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

How could an attacker exploit the vulnerability?
This vulnerability requires that a user open a specially crafted PowerPoint file with an affected version of Microsoft Office PowerPoint

In a Web-based attack scenario, a Web site could contain a PowerPoint file that is used to exploit this vulnerability. An attacker would have to convince users to visit the Web site and open a specially crafted PowerPoint file, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site, and then convincing them to open the specially crafted PowerPoint file.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted PowerPoint file to the user and convincing the user to open the file.

What systems are primarily at risk from the vulnerability?
Systems where an affected version of Microsoft Office PowerPoint is used, such as 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.

What does the update do?
The update removes the vulnerability by modifying the way that Microsoft Office PowerPoint validates memory allocations when opening PowerPoint files.

When this security bulletin was issued, had this vulnerability been publicly disclosed?
No. Microsoft received information about this vulnerability through responsible disclosure.

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.

Legacy File Format Vulnerability - CVE-2009-1137

A remote code execution vulnerability exists in the way that Microsoft Office PowerPoint handles specially crafted PowerPoint files. An attacker could exploit the vulnerability by creating a specially crafted PowerPoint file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

To view this vulnerability as a standard entry in the Common Vulnerabilities and Exposures list, see CVE-2009-1137 .

Mitigating Factors for Legacy File Format Vulnerability - CVE-2009-1137

Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation:

- Microsoft Office 2003 Service Pack 3 blocks the opening and saving of certain files by default upon installation. For Microsoft Office PowerPoint 2003 Service Pack 3, these are files that are older than PowerPoint 97 and that have file

types such as .ppt, .pot, .pps, and .ppa. Notice that this feature does not apply to Microsoft Office PowerPoint 97 files. For more information, see Microsoft Knowledge Base Article 938810.

- Users who have installed and are using the Office Document Open Confirmation Tool for Office 2000 will be prompted with Open, Save, or Cancel before opening a document. The features of the Office Document Open Confirmation Tool are incorporated in Office XP and later editions of Office.
- The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful a user must open an attachment that is sent in an e-mail message.
- In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users 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.
- This vulnerability does not affect PowerPoint 2007, PowerPoint Viewer 2003, and PowerPoint Viewer 2007.

Workarounds for Legacy File Format Vulnerability - CVE-2009-1137

Workaround refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update. Microsoft has tested the following workarounds and states in the discussion whether a workaround reduces functionality:

- **Restrict access to pp4x322.dll in Microsoft Office PowerPoint 2000 or Microsoft Office PowerPoint 2002**

  Note You will need administrator privileges to set these file restrictions.

  - On 32-bit editions of Microsoft Windows 2000, Windows XP and Windows Server 2003, run the following command from a command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

  - On 64-bit editions of Windows XP and Windows Server 2003, run the following command from a command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

  - On 32-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

    for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

  - On 64-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /P everyone:N

Impact of Workaround. You will not be able to open PowerPoint 4.0 files.

How to Undo the Workaround:

- On 32-bit editions of Microsoft Windows 2000, Windows XP and Windows Server 2003, run the following command from a command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

- On 64-bit editions of Windows XP and Windows Server 2003, run the following command from a command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

- On 32-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

- On 64-bit editions of Windows Vista and Windows Server 2008, run the following command from an elevated command prompt:

  for /F "tokens=*" %G IN ('dir /b /s ^"%programfiles(x86)%\Microsoft Office\pp4x322.dll^"') DO cacls "%G" /E /R everyone

FAQ for Legacy File Format Vulnerability - CVE-2009-1137

What is the scope of the vulnerability?
This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability 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.

What causes the vulnerability?
When PowerPoint reads sound data from specially crafted PowerPoint 4.0 files, an error may corrupt memory in such a way that an attacker could execute arbitrary code.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could take complete control of an affected system in the context of the current logged-on user. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

How could an attacker exploit the vulnerability?
This vulnerability requires that a user open a specially crafted PowerPoint 4.0 file with an affected version of Microsoft Office PowerPoint.

In a Web-based attack scenario, a Web site could contain a PowerPoint file that is used to exploit this vulnerability. An attacker would have to convince users to visit the Web site and open a specially crafted PowerPoint file, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site, and then convincing them to open the specially crafted PowerPoint file.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted PowerPoint file to the user and convincing the user to open the file.

What systems are primarily at risk from the vulnerability?
Systems where an affected version of Microsoft Office PowerPoint is used, such as 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.

What does the update do?
This update prevents Microsoft Office PowerPoint 2000 and Microsoft Office PowerPoint 2002 from opening PowerPoint 4.0 native file formats.

When this security bulletin was issued, had this vulnerability been publicly disclosed?
No. Microsoft received information about this vulnerability through responsible disclosure.

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.

Update Information

Detection and Deployment Tools and Guidance

Manage the software and security updates you need to deploy to the servers, desktop, and mobile systems in your organization. For more information see the TechNet Update Management Center. The Microsoft TechNet Security Web site provides additional information about security in Microsoft products.

Security updates are available from Microsoft Update, Windows Update, and Office Update. Security updates are also available from the Microsoft Download Center. You can find them most easily by doing a keyword search for "security update."

Finally, security updates can be downloaded from the Microsoft Update Catalog. The Microsoft Update Catalog provides a searchable catalog of content made available through Windows Update and Microsoft Update, including security updates, drivers and service packs. By searching using the security bulletin number (such as, "MS07-036"), you can add all of the applicable updates to your basket (including different languages for an update), and download to the folder of your choosing. For more information about the Microsoft Update Catalog, see the Microsoft Update Catalog FAQ.

Detection and Deployment Guidance

Microsoft has provided detection and deployment guidance for this month's security updates. This guidance will also help IT professionals understand how they can use various tools to help deploy the security update, such as Windows Update, Microsoft Update, Office Update, the Microsoft Baseline Security Analyzer (MBSA), the Office Detection Tool, Microsoft

Systems Management Server (SMS), and the Extended Security Update Inventory Tool. For more information, see Microsoft Knowledge Base Article 910723.

Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer (MBSA) allows administrators to scan local and remote systems for missing security updates as well as common security misconfigurations. For more information about MBSA, visit Microsoft Baseline Security Analyzer.

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

Expand table

Software	MBSA 2.1
Microsoft Office PowerPoint 2000 Service Pack 3	No
Microsoft Office PowerPoint 2002 Service Pack 3	Yes
Microsoft Office PowerPoint 2003 Service Pack 3	Yes
Microsoft Office PowerPoint 2007 Service Pack 1	Yes
Microsoft Office PowerPoint 2007 Service Pack 2	Yes
Microsoft Office 2004 for Mac	No
Microsoft Office 2008 for Mac	No
Open XML File Format Converter for Mac	No
PowerPoint Viewer 2003	Yes
PowerPoint Viewer 2007 Service Pack 1 and PowerPoint Viewer 2007 Service Pack 2	Yes
Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Service Pack 1 and Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Service Pack 2	Yes
Microsoft Works 8.5	Yes
Microsoft Works 9	Yes

For more information about MBSA 2.1, see MBSA 2.1 Frequently Asked Questions.

Note For customers using legacy software not supported by MBSA 2.1, Microsoft Update, and Windows Server Update Services: please visit Microsoft Baseline Security Analyzer and reference the Legacy Product Support section on how to create comprehensive security update detection with legacy tools.

Windows Server Update Services

By using Windows Server Update Services (WSUS), administrators can 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. For more information about how to deploy this security update using Windows Server Update Services, visit the Windows Server Update Services Web site.

Systems Management Server

The following table provides the SMS detection and deployment summary for this security update.

Expand table

Software	SMS 2.0	SMS 2003 with SUSFP	SMS 2003 with ITMU	Configuration Manager 2007
Microsoft Office PowerPoint 2000 Service Pack 3	Yes	Yes	No	No
Microsoft Office PowerPoint 2002 Service Pack 3	Yes	Yes	Yes	Yes
Microsoft Office PowerPoint 2003 Service Pack 3	Yes	Yes	Yes	Yes
Microsoft Office PowerPoint 2007 Service Pack 1	No	No	Yes	Yes
Microsoft Office PowerPoint 2007 Service Pack 2	No	No	Yes	Yes
Microsoft Office 2004 for Mac	No	No	No	No
Microsoft Office 2008 for Mac	No	No	No	No
Open XML File Format Converter for Mac	No	No	No	No
PowerPoint Viewer 2003	No	No	Yes	Yes
PowerPoint Viewer 2007 Service Pack 1 and PowerPoint Viewer 2007 Service Pack 2	No	No	Yes	Yes
Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Service Pack 1 and Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Service Pack 2	No	No	Yes	Yes
Microsoft Works 8.5	No	No	Yes	Yes
Microsoft Works 9	No	No	Yes	Yes

For SMS 2.0 and SMS 2003, the SMS SUS Feature Pack (SUSFP), which includes the Security Update Inventory Tool (SUIT), can be used by SMS to detect security updates. See also Downloads for Systems Management Server 2.0.

For SMS 2003, the SMS 2003 Inventory Tool for Microsoft Updates (ITMU) can be used by SMS to detect security updates that are offered by Microsoft Update and that are supported by Windows Server Update Services. For more information about the SMS 2003 ITMU, see SMS 2003 Inventory Tool for Microsoft Updates. SMS 2003 can also use the Microsoft Office Inventory Tool to detect required updates for Microsoft Office applications. For more information about the Office Inventory Tool and other scanning tools, see SMS 2003 Software Update Scanning Tools. See also Downloads for Systems Management Server 2003.

System Center Configuration Manager 2007 uses WSUS 3.0 for detection of updates. For more information about Configuration Manager 2007 Software Update Management, visit System Center Configuration Manager 2007.

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

For more detailed information, see Microsoft Knowledge Base Article 910723: Summary list of monthly detection and deployment guidance articles.

Note If you have used an Administrative Installation Point (AIP) for deploying Office 2000, Office XP or Office 2003, you may not be able to deploy the update using SMS if you have updated the AIP from the original baseline. For more

information, see the **Office Administrative Installation Point** heading in this section.

Office Administrative Installation Point

If you installed your application from a server location, the server administrator must update the server location with the administrative update and deploy that update to your system.

- For supported versions of Microsoft Office 2000, see How to Create an Administrative Installation Point. For more information about how to change the source for a client system from an updated administrative installation point to an Office 2000 Service Pack 3 (SP3), see Microsoft Knowledge Base Article 932889. **Note** If you plan to manage software updates centrally from an updated administrative image, you can find more information in the article Updating Office 2000 Clients from a Patched Administrative Image.
- For supported versions of Microsoft Office XP, see Creating an Administrative Installation Point. For more information on how to change the source for a client system from an updated administrative installation point to an Office XP original baseline source, see Microsoft Knowledge Base Article 922665. **Note** If you plan to manage software updates centrally from an updated administrative image, you can find more information in the article Updating Office XP Clients from a Patched Administrative Image.
- For supported versions of Microsoft Office 2003, see Creating an Administrative Installation Point. For more information on how to change the source for a client computer from an updated administrative installation point to an Office 2003 original baseline source or Service Pack 3 (SP3), see Microsoft Knowledge Base Article 902349. **Note** If you plan to manage software updates centrally from an updated administrative image, you can find more information in the article, Distributing Office 2003 Product Upgrades.
- For supported versions of the 2007 Microsoft Office system, see Create a network installation point for the 2007 Office system. **Note** If you plan to manage security updates centrally, use Windows Server Update Services. For more information about how to deploy security updates for the 2007 Microsoft Office system using Windows Server Update Services, visit the Windows Server Update Services Web site.

Update Compatibility Evaluator and Application Compatibility Toolkit

Updates often write to the same files and registry settings required for your applications to run. This can trigger incompatibilities and increase the time it takes to deploy security updates. You can streamline testing and validating Windows updates against installed applications with the Update Compatibility Evaluator components included with Application Compatibility Toolkit 5.0.

The Application Compatibility Toolkit (ACT) contains the necessary tools and documentation to evaluate and mitigate application compatibility issues before deploying Microsoft Windows Vista, a Windows Update, a Microsoft Security Update, or a new version of Windows Internet Explorer in your environment.

Security Update Deployment

Affected Software

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

PowerPoint 2000 (all editions)

Reference Table

The following table contains the security update information for this software. You can find additional information in the subsection, **Deployment Information**, in this section.

Expand table

Inclusion in Future Service Packs	**There are no more service packs planned for this software. The update for this issue may be included in a future update rollup.**
Deployment	
Installing without user intervention	office2000-KB957790-fullfile-enu /q:a
Installing without restarting	office2000-KB957790-fullfile-enu /r:n
Update log file	Not applicable
Further information	For detection and deployment, see the earlier section, **Detection and Deployment Tools and Guidance.** \ \ For features you can selectively install, see the **Office Features for Administrative Installations** subsection in this section.
Restart Requirement	
Restart required?	In some cases, this update does not require a restart. If the required files are being used, this update will require a restart. If this behavior occurs, a message appears that advises you to restart.\ \ To help reduce the chance that a restart will be required, stop all affected services and close all applications that may use the affected files prior to installing the security update. For more information about the reasons why you may be prompted to restart, see Microsoft Knowledge Base Article 887012.
Hotpatching	Not applicable
Removal Information	After you install the update, you cannot remove it. To revert to an installation before the update was installed; you must remove the application, and then install it again from the original media.
File Information	See Microsoft Knowledge Base Article 967340
Registry Key Verification	Not applicable

Office Features for Administrative Installations

Server administrators who use a Windows Installer Administrative Installation must update the server location. For more information about Administrative Installation Points, refer to the **Office Administrative Installation Point** information in the **Detection and deployment Tools and Guidance** subsection.

The following table contains the list of feature names (case sensitive) that must be reinstalled for the update.

To install all features, you can use **REINSTALL=ALL** or you can install the following features:

Expand table

Product	Feature
O9PRM, O9PRO, O9PP, O9STD	PPTFiles

Note Administrators working in managed environments can find resources for deploying Office updates in an organization at the Office Admin Update Center. At that site, scroll down and look under the **Update Resources** section for the software version you are updating. The Windows Installer Documentation also provides more information about the setup switches supported by Windows Installer.

Deployment Information

Installing the Update

You can install the update from the appropriate download link in the Affected and Non-Affected Software section. If you installed your application from a server location, the server administrator must instead update the server location with the administrative update and deploy that update to your system. For more information about Administrative Installation Points, refer to the **Office Administrative Installation Point** information in the **Detection and Deployment Tools and Guidance** subsection.

This security update requires that Windows Installer 2.0 or later be installed on the system. All supported versions of Windows include Windows Installer 2.0 or a later version.

To install the 2.0 or later version of Windows Installer, visit one of the following Microsoft Web sites:

- Windows Installer 4.5 Redistributable for Windows Server 2008, Windows Vista, Windows Server 2003, and Windows XP
- Windows Installer 3.1 Redistributable for Windows Server 2003, Windows XP, and Windows 2000
- Windows Installer 2.0 Redistributable for Windows 2000 and Windows NT 4.0

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

This security update supports the following setup switches.

Expand table

Switch	Description
/q	Specifies quiet mode, or suppresses prompts, when files are being extracted.
/q:u	Specifies user-quiet mode, which presents some dialog boxes to the user.
/q:a	Specifies administrator-quiet mode, which does not present any dialog boxes to the user.
/t:path	Specifies the target folder for extracting files.
/c	Extracts the files without installing them. If **/t:path** is not specified, you are prompted for a target folder.
/c:path	Overrides the install command that is defined by author. Specifies the path and name of the Setup.inf or .exe file.
/r:n	Never restarts the system after installation.
/r:l	Prompts the user to restart the system if a restart is required, except when used with **/q:a**.

Switch	Description
/r:a	Always restarts the system after installation.
/r:s	Restarts the system after installation without prompting the user.
/n:v	No version checking - Install the program over any earlier version.

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.

Removing the Update

After you install the update, you cannot remove it. To revert to an installation before the update was installed; you must remove the application, and then install it again from the original media.

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 section, **Detection and Deployment Tools and Guidance**, earlier in this bulletin for more information.

- **File Version Verification**

  Because there are several versions and editions of Microsoft Office, the following steps may be different on your system. 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 system 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.

PowerPoint 2002 (all editions)

Reference Table

The following table contains the security update information for this software. You can find additional information in the subsection, **Deployment Information**, in this section.

Expand table

Inclusion in Future Service Packs	**There are no more service packs planned for this software. The update for this issue may be included in a future update rollup.**
Deployment	
Installing without user intervention	officexp-KB957781-FullFile-ENU /q:a
Installing without restarting	officexp-KB957781-FullFile-ENU /r:n
Update log file	Not applicable
Further information	For detection and deployment, see the earlier section, **Detection and Deployment Tools and Guidance.** \ \ For features you can selectively install, see the **Office Features for Administrative Installations** subsection in this section.
Restart Requirement	
Restart required?	In some cases, this update does not require a restart. If the required files are being used, this update will require a restart. If this behavior occurs, a message appears that advises you to restart.\ \ To help reduce the chance that a restart will be required, stop all affected services and close all applications that may use the affected files prior to installing the security update. For more information about the reasons why you may be prompted to restart, see Microsoft Knowledge Base Article 887012.
Hotpatching	Not applicable
Removal Information	Use **Add or Remove Programs** tool in Control Panel.**Note** When you remove this update, you may be prompted to insert the Microsoft Office XP CD in the CD drive. Additionally, you may not have the option to uninstall the update from the Add or Remove Programs tool in Control Panel. There are several possible causes for this issue. For more information about the removal, see Microsoft Knowledge Base Article 903771.
File Information	See Microsoft Knowledge Base Article 967340
Registry Key Verification	Not applicable

Office Features

The following table contains the list of feature names (case sensitive) that must be reinstalled for the update. To install all features, you can use **REINSTALL=ALL** or you can install the following features:

Expand table

Product	Feature
PPT, PROPLUS, PRO, STD, STDEDU	PPTFiles

Note Administrators working in managed environments can find complete resources for deploying Office updates in an organization at the Office Admin Update Center. At that site, scroll down and look under the **Update Resources** section for the software version you are updating. The Windows Installer Documentation also provides more information about the parameters supported by Windows Installer.

Deployment Information

Installing the Update

You can install the update from the appropriate download link in the Affected and Non-Affected Software section. If you installed your application from a server location, the server administrator must instead update the server location with the administrative update and deploy that update to your system. For more information about Administrative Installation Points, refer to the **Office Administrative Installation Point** information in the **Detection and deployment Tools and Guidance** subsection.

This security update requires that Windows Installer 2.0 or later be installed on the system. All supported versions of Windows include Windows Installer 2.0 or a later version.

To install the 2.0 or later version of Windows Installer, visit one of the following Microsoft Web sites:

- Windows Installer 4.5 Redistributable for Windows Server 2008, Windows Vista, Windows Server 2003, and Windows XP
- Windows Installer 3.1 Redistributable for Windows Server 2003, Windows XP, and Windows 2000
- Windows Installer 2.0 Redistributable for Windows 2000 and Windows NT 4.0

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

This security update supports the following setup switches.

Expand table

Switch	Description
/q	Specifies quiet mode, or suppresses prompts, when files are being extracted.
/q:u	Specifies user-quiet mode, which presents some dialog boxes to the user.
/q:a	Specifies administrator-quiet mode, which does not present any dialog boxes to the user.
/t:path	Specifies the target folder for extracting files.
/c	Extracts the files without installing them. If **/t:path** is not specified, you are prompted for a target folder.
/c:path	Overrides the install command that is defined by author. Specifies the path and name of the Setup.inf or .exe file.
/r:n	Never restarts the system after installation.
/r:l	Prompts the user to restart the system if a restart is required, except when used with **/q:a**.
/r:a	Always restarts the system after installation.
/r:s	Restarts the system after installation without prompting the user.
/n:v	No version checking - Install the program over any earlier version.

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.

Removing the Update

To remove this security update, use the Add or Remove Programs tool in Control Panel. **Note** When you remove this update, you may be prompted to insert the Microsoft Office XP CD in the CD drive. Additionally, you may not have the option to uninstall the update from the Add or Remove Programs tool in Control Panel. There are several possible causes for this issue. For more information about the removal, see Microsoft Knowledge Base Article 903771.

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 section, **Detection and Deployment Tools and Guidance**, earlier in this bulletin for more information.

- **File Version Verification**

  Because there are several versions and editions of Microsoft Windows, the following steps may be different on your system. 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 system 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.

PowerPoint 2003 (all editions)

Reference Table

The following table contains the security update information for this software. You can find additional information in the subsection, **Deployment Information**, in this section.

Expand table

Inclusion in Future Service Packs	**There are no more service packs planned for this software. The update for this issue may be included in a future update rollup.**
Deployment	
Installing without user intervention	For PowerPoint 2003:\ Office2003-KB957784-FullFile-ENU /q:a

Inclusion in Future Service Packs	**There are no more service packs planned for this software. The update for this issue may be included in a future update rollup.**
Installing without restarting	For PowerPoint 2003:\ Office2003-KB957784-FullFile-ENU /r:n
Update log file	Not applicable
Further information	For detection and deployment, see the earlier section, **Detection and Deployment Tools and Guidance.** \ \ For features you can selectively install, see the **Office Features for Administrative Installations** subsection in this section.
Restart Requirement	
Restart required?	In some cases, this update does not require a restart. If the required files are being used, this update will require a restart. If this behavior occurs, a message appears that advises you to restart.\ \ To help reduce the chance that a restart will be required, stop all affected services and close all applications that may use the affected files prior to installing the security update. For more information about the reasons why you may be prompted to restart, see Microsoft Knowledge Base Article 887012.
Hotpatching	Not applicable
Removal Information	Use **Add or Remove Programs** tool in Control Panel.**Note** When you remove this update, you may be prompted to insert the Microsoft Office 2003 CD in the CD drive. Additionally, you may not have the option to uninstall the update from the Add or Remove Programs tool in Control Panel. There are several possible causes for this issue. For more information about the removal, see Microsoft Knowledge Base Article 903771.
File Information	See Microsoft Knowledge Base Article 967340
Registry Key Verification	Not applicable

Office Features

The following table contains the list of feature names (case sensitive) that must be reinstalled for the update. To install all features, you can use **REINSTALL=ALL** or you can install the following features:

Expand table

Product	Feature
STD11, PPT11, PROI11, PRO11, STDP11, PRO11SB	PPTFiles

Note Administrators working in managed environments can find complete resources for deploying Office updates in an organization at the Office Admin Update Center. At that site, scroll down and look under the **Update Resources** section for the software version you are updating. The Windows Installer Documentation also provides more information about the parameters supported by Windows Installer.

Deployment Information

Installing the Update

You can install the update from the appropriate download link in the Affected and Non-Affected Software section. If you installed your application from a server location, the server administrator must instead update the server location with the administrative update and deploy that update to your system. For more information about Administrative Installation Points, refer to the **Office Administrative Installation Point** information in the **Detection and deployment Tools and Guidance** subsection.

This security update requires that Windows Installer 2.0 or later be installed on the system. All supported versions of Windows include Windows Installer 2.0 or a later version.

To install the 2.0 or later version of Windows Installer, visit one of the following Microsoft Web sites:

- Windows Installer 4.5 Redistributable for Windows Server 2008, Windows Vista, Windows Server 2003, and Windows XP
- Windows Installer 3.1 Redistributable for Windows Server 2003, Windows XP, and Windows 2000
- Windows Installer 2.0 Redistributable for Windows 2000 and Windows NT 4.0

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

This security update supports the following setup switches.

Expand table

Switch	Description
/q	Specifies quiet mode, or suppresses prompts, when files are being extracted.
/q:u	Specifies user-quiet mode, which presents some dialog boxes to the user.
/q:a	Specifies administrator-quiet mode, which does not present any dialog boxes to the user.
/t:path	Specifies the target folder for extracting files.
/c	Extracts the files without installing them. If **/t:path** is not specified, you are prompted for a target folder.
/c:path	Overrides the install command that is defined by author. Specifies the path and name of the Setup.inf or .exe file.
/r:n	Never restarts the system after installation.
/r:l	Prompts the user to restart the system if a restart is required, except when used with **/q:a**.
/r:a	Always restarts the system after installation.
/r:s	Restarts the system after installation without prompting the user.
/n:v	No version checking - Install the program over any earlier version.

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.

Removing the Update

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

Note When you remove this update, you may be prompted to insert the Microsoft Office 2003 CD in the CD drive. Additionally, you may not have the option to uninstall the update from the Add or Remove Programs tool in Control Panel. There are several possible causes for this issue. For more information about the removal, see Microsoft Knowledge Base Article 903771.

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 section, **Detection and Deployment Tools and Guidance**, earlier in this bulletin for more information.

- **File Version Verification**

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

  1. Click **Start** and then enter an update file name in **Start Search**.
  2. When the file appears under **Programs**, right-click on the file name and click **Properties**.
  3. Under the **General** tab, compare the file size with the file information tables provided in the bulletin KB article.
  4. You may also click on the **Details** tab and compare information, such as file version and date modified, with the file information tables provided in the bulletin KB article.
  5. Finally, you may also click on the **Previous Versions** tab and compare file information for the previous version of the file with the file information for the new, or updated, version of the file.

PowerPoint 2007 (all editions), PowerPoint Viewer 2003, PowerPoint Viewer 2007 (all versions), and Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats (all versions)

Reference Table

The following table contains the security update information for this software. You can find additional information in the subsection, **Deployment Information**, in this section.

Expand table

Inclusion in Future Service Packs	**The update for this issue will be included in a future service pack or update rollup**
Deployment	
Installing without user intervention	For PowerPoint 2007:\ powerpoint2007-kb957789-fullfile-x86-glb /passive\ \ For PowerPoint Viewer 2003:\ office2003-kb969615-fullfile-x86-en-us /passive\ \ For PowerPoint Viewer 2007:\ office2007-kb970059-fullfile-x86-glb /passive\ \ For Office Compatibility Pack:\ office2007-kb969618-fullfile-x86-glb /passive
Installing without restarting	For PowerPoint 2007:\ powerpoint2007-kb957789-fullfile-x86-glb /norestart\ \ For PowerPoint Viewer 2003:\ office2003-kb969615-fullfile-x86-en-us /norestart\ \ For PowerPoint Viewer 2007:\ office2007-kb970059-fullfile-x86-glb /norestart\ \ For Office Compatibility Pack:\ office2007-kb969618-fullfile-x86-glb /norestart
Update log file	Not applicable

Inclusion in Future Service Packs	**The update for this issue will be included in a future service pack or update rollup**
Further information	For detection and deployment, see the earlier section, **Detection and Deployment Tools and Guidance**.
Restart Requirement	
Restart required?	In some cases, this update does not require a restart. If the required files are being used, this update will require a restart. If this behavior occurs, a message appears that advises you to restart.\ \ To help reduce the chance that a restart will be required, stop all affected services and close all applications that may use the affected files prior to installing the security update. For more information about the reasons why you may be prompted to restart, see Microsoft Knowledge Base Article 887012 .
Hotpatching	Not applicable
Removal Information	Use **Add or Remove Programs** tool in Control Panel.
File Information	See Microsoft Knowledge Base Article 967340
Registry Key Verification	Not applicable

Deployment Information

Installing the Update

You can install the update from the appropriate download link in the Affected and Non-Affected Software section. If you installed your application from a server location, the server administrator must instead update the server location with the administrative update and deploy that update to your system. For more information about Administrative Installation Points, refer to the **Office Administrative Installation Point** information in the **Detection and deployment Tools and Guidance** subsection.

This security update requires that Windows Installer 3.1 or later be installed on the system.

To install the 3.1 or later version of Windows Installer, visit one of the following Microsoft Web sites:

- Windows Installer 4.5 Redistributable for Windows Server 2008, Windows Vista, Windows Server 2003, and Windows XP
- Windows Installer 3.1 Redistributable for Windows Server 2003, Windows XP, and Windows 2000

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

This security update supports the following setup switches.

Expand table

Switch	Description
/? or **/help**	Displays usage dialog.

Switch	Description
/passive	Specifies passive mode. Requires no user interaction; users see basic progress dialogs but cannot cancel.
/quiet	Specifies quiet mode, or suppresses prompts, when files are being extracted.
/norestart	Suppresses restarting the system if the update requires a restart.
/forcerestart	Automatically restarts the system after applying the update, regardless of whether the update requires the restart.
/extract	Extracts the files without installing them. You are prompted for a target folder.
/extract:<path>	Overrides the install command that is defined by author. Specifies the path and name of the Setup.inf or .exe file.
/lang:<LCID>	Forces the use of a specific language, when the update package supports that language.
/log:<log file>	Enables logging, by both Vnox and Installer, during the update installation.

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.

Removing the Update

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

Note When you remove this update, you may be prompted to insert the 2007 Microsoft Office CD in the CD drive. Additionally, you may not have the option to uninstall the update from the Add or Remove Programs tool in Control Panel. There are several possible causes for this issue. For more information about the removal, see Microsoft Knowledge Base Article 903771.

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 section, **Detection and Deployment Tools and Guidance**, earlier in this bulletin for more information.

- **File Version Verification**

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

  1. Click **Start** and then enter an update file name in **Start Search**.
  2. When the file appears under **Programs**, right-click on the file name and click **Properties**.
  3. Under the **General** tab, compare the file size with the file information tables provided in the bulletin KB article.
  4. You may also click on the **Details** tab and compare information, such as file version and date modified, with the file information tables provided in the bulletin KB article.
  5. Finally, you may also click on the **Previous Versions** tab and compare file information for the previous version of the file with the file information for the new, or updated, version of the file.

Office 2004 for Mac

Deployment Information

Prerequisites

- Mac OS X version 10.2.8 or later on a G3, Mac OS X-compatible processor or higher
- Mac OS X user accounts must have administrator privileges to install this security update

Installing the Update

Download and install the appropriate language version of the Microsoft Office 2004 for Mac 11.5.5 Update from the Microsoft Download Center.

- Quit any applications that are running, including virus-protection applications, all Microsoft Office applications, Microsoft Messenger for Mac, and Office Notifications, because they might interfere with installation.
- Open the Microsoft Office 2004 for Mac 11.5.5 Update volume on your desktop. This step might have been performed for you.
- To start the update process, in the Microsoft Office 2004 for Mac 11.5.5 Update volume window, double-click the Microsoft Office 2004 for Mac 11.5.5 Update application, and follow the instructions on the screen.
- If the installation finishes successfully, you can remove the update installer from your hard disk. To verify that the installation finished successfully, see the following "Verifying Update Installation" heading. To remove the update installer, first drag the Microsoft Office 2004 for 11.5.5 Update volume to the Trash, and then drag the file that you downloaded to the Trash.

Verifying Update Installation

To verify that a security update is installed on an affected system, follow these steps:

1. In the Finder, navigate to the Application Folder (Microsoft Office 2004: Office).
2. Select the file, Microsoft Component Plugin.
3. On the File menu, click **Get Info** or **Show Info**.

If the Version number is **11.5.5**, the update has been successfully installed.

Restart Requirement

This update does not require you to restart your computer.

Removing the Update

This security update cannot be uninstalled.

Additional Information

If you have technical questions or problems downloading or using this update, visit Microsoft for Mac Support to learn about the support options that are available to you.

Office 2008 for Mac

Deployment Information

Prerequisites

- Mac OS X version 10.4.9 or later on an Intel, PowerPC G5, or PowerPC G4 (500 MHz or faster) processor
- Mac OS X user accounts must have administrator privileges to install this security update

Installing the Update

Download and install the appropriate language version of the Microsoft Office 2008 for Mac 12.1.9 Update from the Microsoft Download Center.

- Quit any applications that are running, including virus-protection applications, all Microsoft Office applications, Microsoft Messenger for Mac, and Office Notifications, because they might interfere with installation.
- Open the Microsoft Office 2008 for Mac 12.1.9 Update volume on your desktop. This step might have been performed for you.
- To start the update process, in the Microsoft Office 2008 for Mac 12.1.9 Update volume window, double-click the Microsoft Office 2008 for Mac 12.1.9 Update application, and follow the instructions on the screen.
- If the installation finishes successfully, you can remove the update installer from your hard disk. To verify that the installation finished successfully, see the following "Verifying Update Installation" heading. To remove the update installer, first drag the Microsoft Office 2008 for Mac 12.1.9 Update volume to the Trash, and then drag the file that you downloaded to the Trash.

Verifying Update Installation

To verify that a security update is installed on an affected system, follow these steps:

1. In the Finder, navigate to the Application Folder (Microsoft Office 2008: Office).
2. Select the file, Microsoft Component Plugin.
3. On the File menu, click **Get Info** or **Show Info**.

If the Version number is **12.1.9**, the update has been successfully installed.

Restart Requirement

This update does not require you to restart your computer.

Removing the Update

This security update cannot be uninstalled.

Additional Information

If you have technical questions or problems downloading or using this update, visit Microsoft for Mac Support to learn about the support options that are available to you.

Open XML File Converter For Mac

Deployment Information

Prerequisites

- Mac OS X version 10.4.9 or later on an Intel, PowerPC G5, or PowerPC G4 (500 MHz or faster) processor
- Mac OS X user accounts must have administrator privileges to install this security update

Installing the Update

Download and install the appropriate language version of the Open XML File Converter for Mac 1.0.3 Update from the Microsoft Download Center.

- Quit any applications that are running, including virus-protection applications, all Microsoft Office applications, Microsoft Messenger for Mac, and Office Notifications, because they might interfere with installation.
- Open the Open XML File Converter for Mac 1.0.3 Update volume on your desktop. This step might have been performed for you.
- To start the update process, in the Open XML File Converter for Mac 1.0.3 Update volume window, double-click the Open XML File Converter for Mac 1.0.3 Update application, and follow the instructions on the screen.
- If the installation finishes successfully, you can remove the update installer from your hard disk. To verify that the installation finished successfully, see the following "Verifying Update Installation" heading. To remove the update installer, first drag the Open XML File Converter for Mac 1.0.3 Update volume to the Trash, and then drag the file that you downloaded to the Trash.

Verifying Update Installation

To verify that a security update is installed on an affected system, follow these steps:

1. In the Finder, navigate to the Application Folder (Open XML File Converter for Mac : Office).
2. Select the file, Microsoft Component Plugin.
3. On the File menu, click **Get Info** or **Show Info**.

If the Version number is 1.0.3, the update has been successfully installed.

Restart Requirement

This update does not require you to restart your computer.

Removing the Update

This security update cannot be uninstalled.

Additional Information

If you have technical questions or problems downloading or using this update, visit Microsoft for Mac Support to learn about the support options that are available to you.

Works 8.5 and Works 9

Reference Table

The following table contains the security update information for this software. You can find additional information in the subsection, **Deployment Information**, in this section.

Expand table

Deployment	
Installing without user intervention	For Microsoft Works 8.5:\ Works8_KB967043_en-US /passive\ \ For Microsoft Works 9:\ Works9_KB967044_en-US /passive

Deployment	
Installing without restarting	For Microsoft Works 8.5:\ Works8_KB967043_en-US /norestart\ \ For Microsoft Works 9:\ Works9_KB967044_en-US /norestart
Update log file	Not applicable
Further information	For detection and deployment, see the earlier section, **Detection and Deployment Tools and Guidance**.
Restart Requirement	
Restart required?	In some cases, this update does not require a restart. If the required files are being used, this update will require a restart. If this behavior occurs, a message appears that advises you to restart.\ \ To help reduce the chance that a restart will be required, stop all affected services and close all applications that may use the affected files prior to installing the security update. For more information about the reasons why you may be prompted to restart, see Microsoft Knowledge Base Article 887012.
Hotpatching	Not applicable
Removal Information	Use **Add or Remove Programs** tool in Control Panel.
File Information	For Microsoft Works 8.5:\ See Microsoft Knowledge Base Article 967043 \ \ For Microsoft Works 9:\ See Microsoft Knowledge Base Article 967044
Registry Key Verification	Not applicable

Deployment Information

Installing the Update

You can install the update from the appropriate download link in the Affected and Non-Affected Software section. If you installed your application from a server location, the server administrator must instead update the server location with the administrative update and deploy that update to your system. For more information about Administrative Installation Points, refer to the **Office Administrative Installation Point** information in the **Detection and deployment Tools and Guidance** subsection.

This security update requires that Windows Installer 3.1 or later be installed on the system.

To install the 3.1 or later version of Windows Installer, visit one of the following Microsoft Web sites:

- Windows Installer 4.5 Redistributable for Windows Server 2008, Windows Vista, Windows Server 2003, and Windows XP
- Windows Installer 3.1 Redistributable for Windows Server 2003, Windows XP, and Windows 2000

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

This security update supports the following setup switches.

Expand table

Switch	Description
/? or **/help**	Displays usage dialog.
/passive	Specifies passive mode. Requires no user interaction; users see basic progress dialogs but cannot cancel.
/quiet	Specifies quiet mode, or suppresses prompts, when files are being extracted.
/norestart	Suppresses restarting the system if the update requires a restart.
/forcerestart	Automatically restarts the system after applying the update, regardless of whether the update requires the restart.
/extract	Extracts the files without installing them. You are prompted for a target folder.
/extract:<path>	Overrides the install command that is defined by author. Specifies the path and name of the Setup.inf or .exe file.
/lang:<LCID>	Forces the use of a specific language, when the update package supports that language.
/log:<log file>	Enables logging, by both Vnox and Installer, during the update installation.

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.

Removing the Update

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

Note When you remove this update, you may be prompted to insert the 2007 Microsoft Office CD in the CD drive. Additionally, you may not have the option to uninstall the update from the Add or Remove Programs tool in Control Panel. There are several possible causes for this issue. For more information about the removal, see Microsoft Knowledge Base Article 903771.

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 section, **Detection and Deployment Tools and Guidance**, earlier in this bulletin for more information.

- **File Version Verification**

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

  1. Click **Start** and then enter an update file name in **Start Search**.
  2. When the file appears under **Programs**, right-click on the file name and click **Properties**.
  3. Under the **General** tab, compare the file size with the file information tables provided in the bulletin KB article.
  4. You may also click on the **Details** tab and compare information, such as file version and date modified, with the file information tables provided in the bulletin KB article.
  5. Finally, you may also click on the **Previous Versions** tab and compare file information for the previous version of the file with the file information for the new, or updated, version of the file.

Other Information

Acknowledgments

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

- An anonymous researcher, working with VeriSign iDefense Labs, for reporting the Legacy File Format Vulnerability (CVE-2009-0220)
- Sean Larsson of VeriSign iDefense Labs for reporting the Integer Overflow Vulnerability (CVE-2009-0221)
- Nicolas Joly of VUPEN Security for reporting the Legacy File Format Vulnerability (CVE-2009-0222)
- Marsu Pilami of VeriSign iDefense Labs for reporting the Legacy File Format Vulnerability (CVE-2009-0223)
- Sean Larsson of VeriSign iDefense Labs for reporting the Memory Corruption Vulnerability (CVE-2009-0224)
- Nicolas Joly of VUPEN Security for reporting the PP7 Memory Corruption Vulnerability (CVE-2009-0225)
- Marsu Pilami of VeriSign iDefense Labs for reporting the Legacy File Format Vulnerability (CVE-2009-0226)
- Marsu Pilami of VeriSign iDefense Labs for reporting the Legacy File Format Vulnerability (CVE-2009-0227)
- Marsu Pilami, working with Zero Day Initiative, for reporting the Memory Corruption Vulnerability (CVE-2009-0556)
- Marsu Pilami of VeriSign iDefense Labs for reporting the PP7 Memory Corruption Vulnerability (CVE-2009-1128)
- Marsu Pilami of VeriSign iDefense Labs for reporting the PP7 Memory Corruption Vulnerability (CVE-2009-1129)
- Ling and Wushi of team509, working with TippingPoint and the Zero Day Initiative, and Sean Larsson of VeriSign iDefense Labs for reporting the Heap Corruption Vulnerability (CVE-2009-1130)
- Carsten H. Eiram of Secunia for reporting the Data Out of Bounds Vulnerability (CVE-2009-1131)
- An anonymous researcher, working with VeriSign iDefense Labs, for reporting the Legacy File Format Vulnerability (CVE-2009-1137)

Microsoft Active Protections Program (MAPP)

To improve security protections for customers, Microsoft provides vulnerability information to major security software providers in advance of each monthly security update release. Security software providers can then use this vulnerability information to provide updated protections to customers via their security software or devices, such as antivirus, network-based intrusion detection systems, or host-based intrusion prevention systems. To determine whether active protections are available from security software providers, please visit the active protections Web sites provided by program partners, listed in Microsoft Active Protections Program (MAPP) Partners.

Support

- Customers in the U.S. and Canada can receive technical support from Security Support or 1-866-PCSAFETY. There is no charge for support calls that are associated with security updates. For more information about available support options, see Microsoft Help and Support.
- 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.

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 (May 12, 2009): Bulletin published.
- V1.1 (May 13, 2009): Corrected the entry in the Affected Software table for "Bulletins Replaced by this Update" and the SMS detection and deployment information for the PowerPoint Viewer 2003 (KB969615) update. Also removed an erroneous footnote from the Affected Software table pertaining to security updates KB969618 and KB957789 for supported versions of Microsoft Office PowerPoint 2007. This is an informational change only. There were no changes to detection or to the files included in this update.
- V2.0 (June 9, 2009): Bulletin rereleased to provide security update packages for Microsoft Office 2004 for Mac, Microsoft Office 2008 for Mac, Open XML File Format Converter for Mac, Microsoft Works 8.5, and Microsoft Works 9. Customers who currently have this software installed need to apply this update immediately.

Built at 2014-04-18T13:49:36Z-07:00 </https:>

Last updated on 06/08/2023