Security Bulletin

Microsoft Security Bulletin MS07-015 - Critical

Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (932554)

Published: February 13, 2007 | Updated: April 23, 2008

Version: 1.2

Summary

Who Should Read this Document: Customers who use Microsoft Office

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: Critical

Recommendation: Customers should apply the update immediately

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

Caveats: None

Tested Software and Security Update Download Locations:

Affected Software:

- Microsoft Office 2000 Service Pack 3 — Download the update (KB 929062)
  - Microsoft Access 2000
  - Microsoft Excel 2000
  - Microsoft FrontPage 2000
  - Microsoft Outlook 2000
  - Microsoft PowerPoint 2000
  - Microsoft Publisher 2000
  - Microsoft Word 2000
- Microsoft Office XP Service Pack 3 — Download the update (KB929063)

  - Microsoft Access 2002
  - Microsoft Excel 2002
  - Microsoft FrontPage 2002
  - Microsoft Outlook 2002
  - Microsoft PowerPoint 2002
  - Microsoft Publisher 2002
  - Microsoft Word 2002
- Microsoft Office 2003 Service Pack 2 — Download the update (KB929064)
  - Microsoft Access 2003
  - Microsoft Excel 2003
  - Microsoft Excel 2003 Viewer
  - Microsoft FrontPage 2003
  - Microsoft InfoPath 2003
  - Microsoft OneNote 2003
  - Microsoft Outlook 2003
  - Microsoft PowerPoint 2003
  - Microsoft Project 2003
  - Microsoft Publisher 2003
  - Microsoft Visio 2003
  - Microsoft Word 2003
  - Microsoft Excel 2003 Viewer
  - Microsoft Word 2003 Viewer
- Microsoft Project 2000 Service Release 1 — Download the update (KB929062)
- Microsoft Project 2002 Service Pack 1 — Download the update (KB929063)
- Microsoft Visio 2002 Service Pack 2 — Download the update (KB929063)
- Microsoft Office 2004 for Mac — Download the update (KB932185)

Non-Affected Software:

- 2007 Microsoft Office System
- Microsoft Office 2003 Service Pack 2
  - Microsoft PowerPoint 2003 Viewer
- Microsoft Works Suites:
  - Microsoft Works Suite 2004
  - Microsoft Works Suite 2005
  - Microsoft Works Suite 2006

The software in this list has been tested to determine whether the versions are affected. Other versions either no longer include security update support or may not be affected. To determine

the support life cycle for your product and version, visit the Microsoft Support Lifecycle Web site.

General Information

Executive Summary

Executive Summary:

This update resolves two newly discovered, privately and publicly reported vulnerabilities. Each vulnerability is documented in its own subsection in the "Vulnerability Details" section of this bulletin.

When using vulnerable versions of Office, if a user were logged on with administrative user rights, an attacker who successfully exploited these vulnerabilities could take complete control of the 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.

We recommend that customers apply the update immediately.

Severity Ratings and Vulnerability Identifiers:

Expandable

Vulnerability Identifiers	Impact of Vulnerability	Microsoft Office 2000	Microsoft Office XP	Microsoft Office 2003	Microsoft Office 2004 for Mac
PowerPoint Malformed Record Memory Corruption Vulnerability - CVE-2006-3877	Remote Code Execution	Critical	Important	Important	Important
Excel Malformed Record Vulnerability - CVE-2007-0671	Remote Code Execution	Critical	Important	Important	Important

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

Frequently Asked Questions (FAQ) Related to This Security Update

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

Expandable

Bulletin ID	Microsoft Office 2000	Microsoft Office XP	Microsoft Office 2003	Microsoft Office 2004 for Mac
MS06-062	Replaced	Replaced	Replaced	Replaced

How is this update related to MS06-058?
Further investigation of CVE-2006-3877 as originally detailed in MS06-058 revealed that the update was not effective in removing the vulnerability from affected systems. This security bulletin has been issued to properly address CVE-2006-3877 and customers should apply the updates in this bulletin immediately.

Why does this update replace MS06-062 and not MS06-058?
Further investigation of CVE-2006-3877 revealed that fixing the vulnerability in PowerPoint.exe was not effective. This update has been issued and installs a version of mso.dll that effectively addresses CVE-2006-3877. Because this security bulletin is a mso.dll update, it replaces the previous mso.dll update which is MS06-062.

Can I use the Microsoft Baseline Security Analyzer (MBSA) to determine whether this update is required?
The following table provides the MBSA detection summary for this security update.

Expandable

Product	MBSA 1.2.1	MBSA 2.0
Microsoft Office 2000	Yes	No
Microsoft Office XP	Yes	Yes
Microsoft Office 2003	Yes	Yes
Microsoft Office 2004 for Mac	No	No

Note MBSA 1.2.1 uses an integrated version of the Office Detection Tool (ODT) which does not support remote scans of this security update. For more information about MBSA, visit the MBSA Web site.

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

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

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

Expandable

Software	SMS 2.0	SMS 2003
Microsoft Office 2000	Yes	No
Microsoft Office XP	Yes	Yes
Microsoft Office 2003	Yes	Yes
Microsoft Office 2004 for Mac	No	No

SMS uses MBSA for detection. Therefore, SMS has the same limitation that is listed earlier in this bulletin related to programs that MBSA does not detect. For SMS 2.0, the SMS SUS Feature Pack, which includes the Security Update Inventory Tool, can be used by SMS to detect security updates. SMS SUIT uses the MBSA 1.2.1 engine for detection. For more information about the Security Update Inventory Tool, visit the following Microsoft Web site. For more information about the limitations of the Security Update Inventory Tool, see Microsoft Knowledge Base Article 306460. The SMS SUS Feature Pack also includes the Microsoft Office Inventory Tool to detect required updates for Microsoft Office applications.

For SMS 2003, the SMS 2003 Inventory Tool for Microsoft Updates 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 Inventory Tool for Microsoft Updates, visit the following Microsoft Web site. SMS 2003 can also use the Microsoft Office Inventory Tool to detect required updates for Microsoft Office applications.

Note If you have used an Administrative Installation Point 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 about how to change the source for a client computer from an updated administrative installation point to an Office 2000 original baseline source or Service Pack 3 (SP3) see, Microsoft Knowledge Base Article 932889.
- For more information on how to change the source for a client computer from an updated administrative installation point to an Office XP original baseline source or Service Pack 3 (SP3), see Microsoft Knowledge Base Article 922665.
- For more information about 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 2 (SP2) see, Microsoft Knowledge Base Article 902349.

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

Vulnerability Details

PowerPoint Malformed Record Memory Corruption Vulnerability - CVE-2006-3877:

A remote code execution vulnerability exists in PowerPoint and could be exploited when PowerPoint opened a specially crafted file. Such a file might be included in an e-mail attachment or hosted on a malicious web site. An attacker could exploit the vulnerability by constructing a specially crafted PowerPoint file that could allow remote code execution.

If a user were logged on with administrative user rights, 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. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

Mitigating Factors for PowerPoint Malformed Record Memory Corruption Vulnerability - CVE-2006-3877:

- 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.
- In a Web-based attack scenario, an attacker would have to host a Web site that contains a PowerPoint file that is used to attempt to exploit this vulnerability. In addition, compromised

Web sites and Web sites that accept or host user-provided content could contain specially crafted content that could exploit this vulnerability. An attacker would have no way to force users to visit a malicious Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's site.
- 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.
- 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 Office 2003.
- 2007 Microsoft Office System is not affected by this vulnerability.
- PowerPoint 2003 Viewer is not affected by this vulnerability.

Workarounds for PowerPoint Malformed Record Memory Corruption Vulnerability - CVE-2006-3877:

- Do not open or save Microsoft PowerPoint 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 PowerPoint Malformed Record Memory Corruption Vulnerability - CVE-2006-3877:

What is the scope of the vulnerability?
A remote code execution vulnerability exists in PowerPoint and could be exploited when PowerPoint opens a file containing malformed record. Such a file might be included in an e-mail attachment or hosted on a malicious web site. An attacker could exploit the vulnerability by constructing a specially crafted PowerPoint file that could allow remote code execution.

If a user were logged on with administrative user rights, 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. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

What causes the vulnerability?
The vulnerability is caused when PowerPoint opens a specially crafted PowerPoint file which will result in the access of memory outside intended regions when parsing placeholder data.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could cause arbitrary code to run with the privileges of the user who opened the file.

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

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

What does the update do?
The update removes the vulnerability by modifying the way that PowerPoint parses the file and validates the record before passing it to the allocated buffer.

When this security bulletin was issued, had this vulnerability been publicly disclosed?
No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information to indicate that this vulnerability had been publicly disclosed when this security bulletin was originally issued. This security bulletin addresses the privately disclosed vulnerability as well as additional issues discovered through internal investigations.

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.

Excel Malformed Record Vulnerability - CVE-2007-0671:

A remote code execution vulnerability exists in Excel and could be exploited when Excel opened a specially crafted file. Such a file might be included in an e-mail attachment or hosted on a malicious web site. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

If a user were logged on with administrative user rights, 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. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

Mitigating Factors for Excel Malformed Record Vulnerability - CVE-2007-0671:

- 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.
- In a Web-based attack scenario, an attacker would have to host a Web site that contains an Excel file that is used to attempt to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content could contain specially crafted content that could exploit this vulnerability. An attacker would have no way to force users to visit a malicious Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's site.
- 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.
- 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 Office 2003.
- 2007 Microsoft Office System is not affected by this vulnerability.

Workarounds for Excel Malformed Record Vulnerability - CVE-2007-0671:

- Do not open or save Microsoft Excel 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 Excel Malformed Record Vulnerability - CVE-2007-0671:

What is the scope of the vulnerability?

A remote code execution vulnerability exists in Excel and could be exploited when Excel opens a file containing malformed record. Such a file might be included in an e-mail attachment or hosted on a malicious web site. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

If a user were logged on with administrative user rights, 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. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

What causes the vulnerability?

The vulnerability is caused when Excel opens a specially crafted Excel file which will results in the access of memory outside intended regions when parsing placeholder data.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause arbitrary code to run with the privileges of the user who opened the file.

How could an attacker exploit the vulnerability?

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

What systems are primarily at risk from the vulnerability?

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

What does the update do?

The update removes the vulnerability by modifying the way that Excel parses the file and validates the record before passing it to the allocated buffer.

When this security bulletin was issued, had this vulnerability been publicly disclosed?
Yes. This vulnerability has been publicly disclosed. It has been assigned Common Vulnerability and Exposure number CVE-2007-0671.

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

Security Update Information

Affected Software:

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

Office 2000

Prerequisites and Additional Update Details

Important Before you install this update, make sure that the following requirements have been met:

- Microsoft Windows Installer 2.0 must be installed. Microsoft Windows Server 2003, Windows XP and Microsoft Windows 2000 Service Pack 3 (SP3) include Windows Installer 2.0 or a later version. To install the latest version of Windows Installer, visit one of the following Microsoft Web sites:

Windows Installer 2.0 for Windows 95, Windows 98, Windows 98 SE, and Windows Millennium Edition

Windows Installer 2.0 for Windows 2000 and Windows NT 4.0

- Office 2000 Service Pack 3 (SP3) must be installed. Before you install this update, install Office 2000 SP3. For more information about how to install Office 2000 SP3, see Microsoft Knowledge Base Article 326585.
- To install the Project 2000 Service Release 1 (SR1) update, Project 2000 Service Release 1 (SR1) must be installed. Before you install this update, install Project 2000 SR1. For more

information about how to install Project 2000 SR1, see Microsoft Knowledge Base Article 288953.

For more information about how to determine the version of Office 2000 that is installed on your computer, see Microsoft Knowledge Base Article 255275.

Inclusion in Future Service Packs

None. Service Pack 3 is the last service pack for Office 2000.

Restart Requirement

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.

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 CD-ROM.

Automated Client Installation Information

Office Update Web Site

We recommend that you install the Microsoft Office 2000 client updates by using the Office Update Web site. The Office Update Web site detects which installation you have and prompts you to install exactly what you must have to make sure that your installation is completely up to date.

To have the Office Update Web site detect the updates that you must install on your computer, visit the Office Update Web site, and then click **Check for Updates**. After detection is complete, you will receive a list of recommended updates for your approval. Click **Agree and Install** to complete the process.

Manual Client Installation Information

For detailed information about how to manually install this update, review the following section.

Installation Information

The security update supports the following setup switches.

Expandable

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	Override install command defined by author. Specifies the path and name of the Setup.inf or .exe file.
/r:n	Never restarts the computer after installation.
/r:l	Prompts the user to restart the computer if a restart is required, except when used with **/q:a**.
/r:a	Always restarts the computer after installation.
/r:s	Restarts the computer after installation without prompting the user.
/n:v	No version checking - Install the program over any earlier version.

Note These switches do not necessarily work with all updates. If a switch is not available, that functionality is required for the correct installation of the update. Also, using the **/n:v** switch is unsupported and may result in an unbootable system. If the installation is unsuccessful, you should contact your support professional to understand why it could not install.

For more information about the supported setup switches, see Microsoft Knowledge Base Article 197147.

Note The full file office update is intended for both client and administrative deployment scenarios.

Client Deployment Information

1. Download this security update for Office 2000 and/or Project 2000 Service Pack 1.

2. Click **Save this program to disk**, and then click **OK**.
3. Click **Save**.
4. Using Windows Explorer, find the folder that contains the saved file, and then double-click the saved file.
5. If you are prompted to install the update, click **Yes**.
6. Click **Yes** to accept the License Agreement.
7. Insert your original source CD-ROM when you are prompted to do so, and then click **OK**.
8. When you receive a message that states the installation was successful, click **OK**.

Note If the security update is already installed on your computer, you receive the following error message: **This update has already been applied or is included in an update that has already been applied**.

Client Installation File Information

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

Office 2000:

Expandable

File Name	Version	Date	Time	Size
Mso9.dll	9.0.0.8960	07-Feb-2007	13:02	5,595,185

Project 2000:

Expandable

File Name	Version	Date	Time	Size
Atlconv.dll	9.0.2001.1109	17-Jun-2006	17:36	294,966
Blnmgr.dll	9.0.0.8830	17-Jun-2006	17:36	73,785
Mso9.dll	9.0.0.8960	07-Feb-2007	13:02	5,595,185
Odbcmon.dll	10.0.2002.401	17-Jun-2006	17:36	47,616
Pj9od9.dll	9.0.2002.523	17-Jun-2006	17:36	782,389

File Name	Version	Date	Time	Size
Pjbknd09.dll	9.0.2002.523	17-Jun-2006	17:36	3,391,543
Winproj.exe	9.0.2007.104	05-Jan-2007	04:39	6,164,534

Verifying that the Update Has Been Applied

- **Microsoft Baseline Security Analyzer**

Note MBSA 1.2.1 uses an integrated version of the Office Detection Tool (ODT) which does not support remote scans of this issue. For more information about MBSA, visit the MBSA Web site. For more information about MBSA support, visit the following Microsoft Baseline Security Analyzer 1.2 Q&A; Web site.

- **File Version Verification**

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

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

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

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

Administrative Installation Information

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 computer.

Installation Information

The following setup switches are relevant to administrative installations as they allow an administrator to customize how the files are extracted from the security update.

Expandable

Switch	Description
/?	Displays the command-line options.
/q	Specifies quiet mode, or suppresses prompts, when files are being extracted.
/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.

For more information about the supported setup switches, see Microsoft Knowledge Base Article 197147.

Administrative Deployment Information

To update your administrative installation, follow these steps:

1. Download this security update for Office 2000 and/or Project 2000 Service Pack 1.
2. Click **Save this program to disk**, and then click **OK**.
3. Click **Save**.
4. Using Windows Explorer, locate the folder that contains the saved file. Click **Start**, click **Run**, type the following command, and then click **OK** to extract the .msp file:

   [path\name of EXE file] /c /t:C:\AdminUpdate

Note Double-clicking the .exe file does not extract the .msp file; it applies the update to the local computer. In order to update an administrative image, you must first extract the .msp file.

5. Click **Yes** to accept the License Agreement.

6. Click **Yes** if you are prompted to create the folder.

7. If you are familiar with the procedure for updating your administrative installation, click **Start**, click **Run**, type the following command, and then click **OK**:

   msiexec /a *Admin Path***MSI File **/p C:\AdminUpdate***MSP File* **SHORTFILENAMES=TRUE**

   Note *Admin Path* is the path of your administrative installation point for your application (for example, C:\Office2000), *MSI File* is the .msi database package for the application (for example, Data1.msi), and *MSP File* is the name of the administrative update (for example, SHAREDff.msp).

   Note You can append /**qb+** to the command line so that the **Administrative Installation** dialog box and the **End User License Agreement** dialog box do not appear.

8. Click **Next** in the provided dialog box. Do not change your CD key, installation location, or company name in the provided dialog box.

9. Click **I accept the terms in the License Agreement**, and then click **Install**.

At this point, your administrative installation point is updated. Next, you must update the workstations configurations that were originally installed from this administrative installation. To do this, please review the "Workstation Deployment Information" section. Any new installations that you run from this administrative installation point will include the update.

Warning Any workstation configuration that was originally installed from this administrative installation before you installed the update cannot use this administrative installation for actions like repairing Office or adding new features until you complete the steps in the "Workstation Deployment Information" section for this workstation.

Workstation Deployment Information

To deploy the update to the client workstations, click **Start**, click **Run**, type the following command, and then click **OK**:

msiexec /I *Admin Path***MSI File **/qb REINSTALL=**Feature List **REINSTALLMODE=vomu**

Note *Admin Path* is the path of your administrative installation point for your application (for example, C:\Office2000), *MSI File* is the .msi database package for the application (for example, Data1.msi), and *Feature List* is 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.

Expandable

Product	Feature
MSPUB, O9PRMCD2	GraphicsFiltersGIFFiles, TCWord97Files, GraphicsFiltersPNGFiles
O9ACC	ProductFiles, ACCESSNonBootFiles
O9ART	AccessRuntimeMaster
O9EXL	ProductFiles, EXCELNonBootFiles
O9OLK	ProductFiles, OUTLOOKNonBootFiles
O9PP	ProductFiles, PPTNonBootFiles
O9WRD	ProductFiles, WORDNonBootFiles
O9PRM	ProductFiles, OUTLOOKNonBootFiles, WORDNonBootFiles, ACCESSNonBootFiles, EXCELNonBootFiles, FPClientNonBootFiles, PPTNonBootFiles, ProductNonBootFiles
O9PRO	ProductFiles, OUTLOOKNonBootFiles, WORDNonBootFiles, ACCESSNonBootFiles, EXCELNonBootFiles, PPTNonBootFiles
O9SBE, 9327_o9procd1_sbe_coxs_slv_data1 product	ProductFiles, OUTLOOKNonBootFiles,WORDNonBootFiles, EXCELNonBootFiles
O9FP	ProductFiles, FPClientNonBootFiles, ProductNonBootFiles
O9PIPC1	ProductFiles, OUTLOOKNonBootFiles, MSDrawFiles, WORDNonBootFiles, EXCELNonBootFiles
O9PIPC2	ProductFiles, MSDrawFiles, WORDNonBootFiles, EXCELNonBootFiles
O9PRMCD2	ProductFiles,AccessRuntimeMaster, PubPrimary, MSDrawFiles, SBCMNonBootFiles

Product	Feature
O9STD	ProductFiles, OUTLOOKNonBootFiles, WORDNonBootFiles, EXCELNonBootFiles, PPTNonBootFiles

Project 2000:

Expandable

Product	Feature
Project 2000	PROJECTFiles,ASSISTANTFiles,ProductFiles,PROJECTNonBootFiles

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.

Administrative Installation File Information

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

Office 2000:

Expandable

File Name	Version	Date	Time	Size
Mso9.dll	9.0.0.8960	07-Feb-2007	13:02	5,595,185

Project 2000:

Expandable

File Name	Version	Date	Time	Size
Atlconv.dll	9.0.2001.1109	17-Jun-2006	17:36	294,966

File Name	Version	Date	Time	Size
Blnmgr.dll	9.0.0.8830	17-Jun-2006	17:36	73,785
Mso9.dll	9.0.0.8960	07-Feb-2007	13:02	5,595,185
Odbcmon.dll	10.0.2002.401	17-Jun-2006	17:36	47,616
Pj9od9.dll	9.0.2002.523	17-Jun-2006	17:36	782,389
Pjbknd09.dll	9.0.2002.523	17-Jun-2006	17:36	3,391,543
Winproj.exe	9.0.2007.104	05-Jan-2007	04:39	6,164,534

Verifying that the Update Has Been Applied

- **Microsoft Baseline Security Analyzer**

Note MBSA 1.2.1 uses an integrated version of the Office Detection Tool (ODT) which does not support remote scans of this security update. For more information about MBSA, visit the MBSA Web site.

- **File Version Verification**

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

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

   Note Depending on the version of the operating system or programs installed, some of the files that are listed in the file information table may not be installed.

5. On the **Version** tab, determine the version of the file that is installed on your computer by comparing it to the version that is documented in the appropriate file information table.

   Note Attributes other than the file version may change during installation. Comparing other file attributes to the information in the file information table is not a supported method of

verifying that the update has been applied. Also, in certain cases, files may be renamed during installation. If the file or version information is not present, use one of the other available methods to verify update installation.

Office XP

Prerequisites and Additional Update Details

Important: Before you install this update, make sure that the following requirements have been met:

- Microsoft Windows Installer 2.0 must be installed. Microsoft Windows Server 2003, Windows XP, and Microsoft Windows 2000 Service Pack 3 (SP3) include Windows Installer 2.0 or a later version. To install the latest version of the Windows Installer, visit one of the following Microsoft Web sites:

Windows Installer 2.0 for Windows 95, Windows 98, Windows 98 SE, and Windows Millennium Edition

Windows Installer 2.0 for Windows 2000 and Windows NT 4.0

- Office XP Service Pack 3 (SP3) must be installed. Before you install this update, install Office XP SP3. For more information about how to install Office XP SP3, see Microsoft Knowledge Base Article 832671.
- To install the Project 2002 Service Pack 1 (SP1) update, Project 2002 Service Pack 1 (SP1) must be installed. Before you install this update, install Project 2000 SR1. For more information about how to install see Project 2002 Service Pack 1 (SP1).
- To install the Visio 2002 Service Pack 2 (SP2) update, Visio 2002 Service Pack 2 (SP2) must be installed. Before you install this update, install Service Pack 3 (SP-3) for Multilanguage Pack. For more information about how to install Visio 2002 Service Pack 2 (SP2), Visio 2002 Service Pack 2 (SP2).

For more information about how to determine the version of Office XP that is installed on your computer, see Microsoft Knowledge Base Article 291331. For more information about the version information displayed in the **About** dialog box, see Microsoft Knowledge Base Article 328294.

Inclusion in Future Service Packs

None. Service Pack 3 is the last service pack for Office XP.

Restart Requirement

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 .

Removal Information

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 .

Automated Client Installation Information

Microsoft Update Web Site

This update will be available through the Microsoft Update Web site . Microsoft Update consolidates updates that are provided by Windows Update and Office Update into one location and lets you choose automatic delivery and installation of high-priority and security updates. We recommend that you install this update by using the Microsoft Update Web site. The Microsoft Update Web site detects your particular installation and prompts you to install exactly what you must have to make sure that your installation is completely up to date.

To have the Microsoft Update Web site detect the required updates that you must install on your computer, visit the Microsoft Update Web site. You will be given the choice of **Express (Recommended)** or **Custom**. After detection is complete, you will receive a list of recommended updates for your approval. Click **Install Updates** or **Review and Install Updates** to complete the process.

Manual Client Installation Information

For detailed information about how to manually install this update, review the following section.

Installation Information

The security update supports the following setup switches.

Expandable

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	Override install command defined by author. Specifies the path and name of the Setup.inf or .exe file.
/r:n	Never restarts the computer after installation.
/r:l	Prompts the user to restart the computer if a restart is required, except when used with **/q:a**.
/r:a	Always restarts the computer after installation.
/r:s	Restarts the computer after installation without prompting the user.
/n:v	No version checking - Install the program over any earlier version.

Note These switches do not necessarily work with all updates. If a switch is not available, that functionality is required for the correct installation of the update. Also, using the **/n:v** switch is unsupported and may result in an unbootable system. If the installation is unsuccessful, you should contact your support professional to understand why it could not install.

For more information about the supported setup switches, see Microsoft Knowledge Base Article 197147.

Note The full file office update is intended for both client and administrative deployment scenarios.

Client Deployment Information

1. Download this security update for Office XP and/or Project 2002 Service Pack 1 and/or Visio 2002 Service Pack 2.
2. Click **Save this program to disk**, and then click **OK**.
3. Click **Save**.

4. Using Windows Explorer, find the folder that contains the saved file, and then double-click the saved file.
5. If you are prompted to install the update, click **Yes**.
6. Click **Yes** to accept the License Agreement.
7. Insert your original source CD-ROM when you are prompted to do so, and then click **OK**.
8. When you receive a message that states the installation was successful, click **OK**.

Note If the security update is already installed on your computer, you see the following error message: **This update has already been applied or is included in an update that has already been applied**.

Client Installation File Information

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

Office XP:

Expandable

File Name	Version	Date	Time	Size
Mso.dll	10.0.6825.0	15-Dec-2006	05:59	9,816,840

Visio 2002:

Expandable

File Name	Version	Date	Time	Size
Mso.dll	10.0.6825.0	15-Dec-2006	05:59	9,816,840

Project 2002:

Expandable

File Name	Version	Date	Time	Size
Mso.dll	10.0.6825.0	15-Dec-2006	05:59	9,816,840

Administrative Installation Information

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 computer.

Installation Information

The following setup switches are relevant to administrative installations as they allow an administrator to customize how the files are extracted from within the security update.

Expandable

Switch	Description
/?	Displays the command-line options.
/q	Specifies quiet mode, or suppresses prompts, when files are being extracted.
/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	Override install command defined by author. Specifies the path and name of the Setup.inf or .exe file.

For more information about the supported setup switches, see Microsoft Knowledge Base Article 197147.

Administrative Deployment Information

To update your administrative installation, follow these steps:

1. Download this security update for Office XP and/or Project 2002 Service Pack 1 and/or Visio 2002 Service Pack 2.
2. Click **Save this program to disk**, and then click **OK**.
3. Click **Save**.
4. Using Windows Explorer, locate the folder that contains the saved file. Click **Start**, click **Run**, type the following command, and then click **OK** to extract the .msp file:

   [path\name of EXE file] /c /t:C:\AdminUpdate

Note Double-clicking the .exe file does not extract the .msp file; it applies the update to the local computer. In order to update an administrative image, you must first extract the .msp file.

5. Click **Yes** to accept the License Agreement.

6. Click **Yes** if you are prompted to create the folder.

7. If you are familiar with the procedure for updating your administrative installation, click **Start**, click **Run**, type the following command, and then click **OK**:

   msiexec /a *Admin Path***MSI File **/p C:\adminUpdate***MSP File* **SHORTFILENAMES=TRUE**

   Note *Admin Path* is the path of your administrative installation point for your application (for example, C:\OfficeXp), *MSI File* is the .msi database package for the application (for example, Data1.msi), and *MSP File* is the name of the administrative update (for example, SHAREDff.msp).

   Note You can append /**qb+** to the command line so that the **Administrative Installation** dialog box and the **End User License Agreement** dialog box do not appear.

8. Click **Next** in the provided dialog box. Do not change your CD key, installation location, or company name in the provided dialog box.

9. Click **I accept the terms in the License Agreement**, and then click **Install**.

At this point, your administrative installation point is updated. Next, you must update the workstation configurations that were originally installed from this administrative installation. To do this, see the "Workstation Deployment Information" section. Any new installations that you run from this administrative installation point will include the update.

Warning Any workstation configuration that was originally installed from this administrative installation before you installed the update cannot use this administrative installation for actions like repairing Office or adding new features until you complete the steps in the "Workstation Deployment Information" section for this workstation.

Workstation Deployment Information

To deploy the update to the client workstations, click **Start**, click **Run**, type the following command, and then click **OK**:

msiexec /I *Admin Path***MSI File **/qb REINSTALL=**Feature List **REINSTALLMODE=vomu**

Note *Admin Path* is the path of your administrative installation point for your application (for example, C:\OfficeXP), *MSI File* is the .msi database package for the application (for example, Data1.msi), and *Feature List* is 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.

Expandable

Product	Feature
ACCESS, FP, OUTLOOK, PPT, ACCESSRT, PUB	ProductFiles
PIPC1, PROPLUS, PRO, SBE, STD, STDEDU	ProductFiles
WORD	WORDNonBootFiles, ProductFiles
EXCEL	EXCELNonBootFiles, ProductFiles
Visio 2002	Program_Files
Project 2002	ProductFiles

Note Administrators working in managed environments can find complete resources for deploying Office updates in an organization on the Office Admin Update Center. On the home page of that site, look under the **Update Strategies** section for the software version you are updating. The Windows Installer Documentation also provides more information about the parameters supported by the Windows Installer.

Administrative Installation File Information

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

Office XP:

Expandable

File Name	Version	Date	Time	Size
Mso.dll	10.0.6825.0	15-Dec-2006	05:59	9,816,840

Visio 2002:

Expandable

File Name	Version	Date	Time	Size
Mso.dll	10.0.6825.0	15-Dec-2006	05:59	9,816,840

Project 2002:

Expandable

File Name	Version	Date	Time	Size
Mso.dll	10.0.6825.0	15-Dec-2006	05:59	9,816,840

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

- **File Version Verification**

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

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

   Note Depending on the version of the operating system or programs installed, some of the files that are listed in the file information table may not be installed.

5. On the **Version** tab, determine the version of the file that is installed on your computer by comparing it to the version that is documented in the appropriate file information table.

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

Office 2003

Prerequisites and Additional Update Details

Important: Before you install this update, make sure that the following requirements have been met:

- To update Office 2003, Office 2003 Service Pack 2 must be installed. Before you install this update, install Office 2003 SP2.
- To install the update for Project 2003 Service Pack 2, Project 2003 Service Pack 2 must be installed. Before you install this update, install Project 2003 SP2. For additional information about how to install Project 2003 Service Pack 2, see Microsoft Knowledge Base Article 887620.
- To install the update for Visio 2003 Service Pack 2, Visio 2003 Service Pack 2 must be installed. Before you install this update, install Visio 2003 SP2. For additional information about how to install Visio 2003 Service Pack 2, see Microsoft Knowledge Base Article 838345.
- To install the update for OneNote 2003 Service Pack 2, OneNote 2003 Service Pack 2 must be installed. Before you install this update, install OneNote SP2. For additional information about how to install OneNote Service Pack 2, see Microsoft Knowledge Base Article 887619.

For more information about how to determine the version of Office 2003 that is installed on your computer, see Microsoft Knowledge Base Article 821549. For more information about the version information displayed in the **About** dialog box, see Microsoft Knowledge Base Article 328294.

Inclusion in Future Service Packs:

The fix for this issue will be included in a future service pack.

Restart Requirement

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 .

Removal Information

To remove this security update, use Add or Remove Programs 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 Add or Remove Programs in Control Panel. There are several possible causes for this issue. For more information about the removal, see Microsoft Knowledge Base Article 903771 .

Automated Client Installation Information

Microsoft Update Web Site

This update will be available through the Microsoft Update Web site . Microsoft Update consolidates updates that are provided by Windows Update and Office Update into one location and lets you choose automatic delivery and installation of high-priority and security updates. We recommend that you install this update by using the Microsoft Update Web site. The Microsoft Update Web site detects your particular installation and prompts you to install exactly what you must have to make sure that your installation is completely up to date.

To have the Microsoft Update Web site detect the required updates that you must install on your computer, visit the Microsoft Update Web site. You will be given the choice of **Express (Recommended)** or **Custom**. After detection is complete, you will receive a list of recommended updates for your approval. Click **Install Updates** or **Review and Install Updates** to complete the process.

Manual Client Installation Information

For detailed information about how to manually install this update, review the following section.

Installation Information

The security update supports the following setup switches.

Expandable

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	Override install command defined by author. Specifies the path and name of the Setup.inf or .exe file.
/r:n	Never restarts the computer after installation.
/r:l	Prompts the user to restart the computer if a restart is required, except when used with **/q:a**.
/r:a	Always restarts the computer after installation.
/r:s	Restarts the computer after installation without prompting the user.
/n:v	No version checking - Install the program over any earlier version.

Note These switches do not necessarily work with all updates. If a switch is not available, that functionality is required for the correct installation of the update. Also, using the **/n:v** switch is unsupported and may result in an unbootable system. If the installation is unsuccessful, you should contact your support professional to understand why it could not install.

For more information about the supported setup switches, see Microsoft Knowledge Base Article 197147.

Note The full file office update is intended for both client and administrative deployment scenarios.

Client Deployment Information

1. Download the security update for Office 2003.
2. Click **Save this program to disk**, and then click **OK**.
3. Click **Save**.
4. Using Windows Explorer, find the folder that contains the saved file, and then double-click the saved file.

5. If you are prompted to install the update, click **Yes**.
6. Click **Yes** to accept the License Agreement.
7. Insert your original source CD-ROM when you are prompted to do so, and then click **OK**.
8. When you receive a message that states the installation was successful, click **OK**.

Note If the security update is already installed on your computer, you receive the following error message: **This update has already been applied or is included in an update that has already been applied**.

Client Installation File Information

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

Office 2003:

E pand able

File Name	Version	Date	Time	Size
Ietag.dll	11.0.6550.0	17-Mar-2005	21:36	161,984
Mso.dll	11.0.8122.0	27-Dec-2006	23:18	12,257,032

Administrative Installation Information

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 computer.

Installation Information

The following setup switches are relevant to administrative installations as they allow an administrator to customize how the files are extracted from within the security update.

E pand able

Switch	Description
/?	Displays the command-line options.

Switch	Description
/q	Specifies quiet mode, or suppresses prompts, when files are being extracted.
/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	Override install command defined by author. Specifies the path and name of the Setup.inf or .exe file.

For more information about the supported setup switches, see Microsoft Knowledge Base Article 197147.

Administrative Deployment Information

To update your administrative installation, follow these steps:

1. Download the security update for Office 2003.
2. Click **Save this program to disk**, and then click **OK**.
3. Click **Save**.
4. Using Windows Explorer, locate the folder that contains the saved file. Click **Start**, click **Run**, type the following command, and then click **OK** to extract the .msp file:

   [path\name of EXE file] /c /t:C:\AdminUpdate

   Note Double-clicking the .exe file does not extract the .msp file; it applies the update to the local computer. In order to update an administrative image, you must first extract the .msp file.
5. Click **Yes** to accept the License Agreement.
6. Click **Yes** if you are prompted to create the folder.
7. If you are familiar with the procedure for updating **your** administrative installation**,** click **Start**, click **Run**, type the following command, and then click **OK**:

   msiexec /a *Admin Path*****MSI File **/p C:\adminUpdate***MSP File* **SHORTFILENAMES=TRUE**

Note *Admin Path* is the path of your administrative installation point for your application (for example, C:\Office2003), *MSI File* is the .msi database package for the application (for example, Data1.msi), and *MSP File* is the name of the administrative update (for example, SHAREDff.msp).

Note You can append /**qb+** to the command line so that the **Administrative Installation** dialog box and the **End User License Agreement** dialog box do not appear.

8. Click **Next** in the provided dialog box. Do not change your CD key, installation location, or company name in the provided dialog box.

9. Click **I accept the terms in the License Agreement**, and then click **Install**.

At this point, your administrative installation point is updated. Next, you must update the workstations configurations that were originally installed from this administrative installation. To do this, please review the "Workstation Deployment Information" section. Any new installations that you run from this administrative installation point will include the update.

Warning Any workstation configuration that was originally installed from this administrative installation before you installed the update cannot use this administrative installation for actions such as repairing Office or adding new features until you complete the steps in the "Workstation Deployment Information" section.

Workstation Deployment Information

To deploy the update to the client workstations, click **Start**, click **Run**, type the following command, and then click **OK**:

Msiexec /I *Admin Path*****MSI File **/qb REINSTALL=**Feature List **REINSTALLMODE=vomu**

Note *Admin Path* is the path of your administrative installation point for your application (for example, C:\Office2003), *MSI File* is the .msi database package for the application (for example, Data1.msi), and *Feature List* is 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:

Expandable

Product	Feature
RMS	RMSFiles, ProductFiles

Product	Feature
ACCESSRT, ACC11	ACCESSNonBootFiles, ProductFiles
STD11, BASIC11, PERS11, STDP11	WORDNonBootFiles, EXCELNonBootFiles, ProductFiles
FP11, OUTLS11, OUTL11, PPT11, INF11, OUTLSM11	ProductFiles
PROI11, PRO11, PRO11SB	WORDNonBootFiles, ACCESSNonBootFiles, EXCELNonBootFiles, ProductFiles
WORD11	WORDNonBootFiles, ProductFiles
EXCEL11	EXCELNonBootFiles, ProductFiles

Note Administrators working in managed environments can find complete resources for deploying Office updates in an organization on the Office Admin Update Center. On the home page of that site, look under the **Update Strategies** section for the software version you are updating. The Windows Installer Documentation also provides more information about the parameters supported by the Windows Installer.

Administrative Installation File Information

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

Office 2003:

Expandable

File Name	Version	Date	Time	Size
Ietag.dll	11.0.6550.0	17-Mar-2005	21:36	161,984
Mso.dll	11.0.8122.0	27-Dec-2006	23:18	12,257,032

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

- **File Version Verification**

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

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

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

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

Office 2004 for Mac

Installation Information

Restart Requirement

This update does not require you to restart your computer.

Removal Information

This update cannot be uninstalled.

Installation Information:

1. 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.
2. Open the **Microsoft Office 2004 for Mac 11.3.4 Update** volume on your desktop. This step might have been performed for you.
3. To start the update process, in the **Microsoft Office 2004 for Mac 11.3.4 Update** volume window, double-click the **Microsoft Office 2004 for Mac 11.3.4 Update** application, and follow the instructions on the screen.
4. If the installation finishes successfully, you can remove the update installer from your hard disk. To verify that the installation finished successfully, see the "Verifying Update Installation" section. To remove the update installer, first drag the **Microsoft Office 2004 for Mac 11.3.4 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 **11.3.4**, the update has been successfully installed.

Other Information

Acknowledgments

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

- Chris Ries of VigilantMinds Inc. for reporting the PowerPoint Malformed Record Memory Corruption Vulnerability (CVE-2006-3877).

Obtaining Other Security Updates:

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

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

Support:

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

Security Resources:

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

Software Update Services:

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

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

Windows Server Update Services:

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

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

Systems Management Server:

Microsoft Systems Management Server (SMS) delivers a highly configurable enterprise solution for managing updates. By using SMS, administrators can identify Windows-based systems that require security updates and can perform controlled deployment of these updates throughout the enterprise with minimal disruption to end users. For more information about how administrators can use SMS 2003 to deploy security updates, visit the SMS 2003 Security Patch Management Web site. SMS 2.0 users can also use Software Updates Service Feature Pack to help deploy security updates. For information about SMS, visit the SMS Web site.

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

Disclaimer:

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

Revisions:

- V1.0 (February 13, 2007): Bulletin published.
- V1.1 (February 28, 2007) Bulletin updated: “Prerequisites and Additional Update” for Office 2003 in the “Security Update Information” section.
- V1.2 (April 23, 2008) Bulletin updated: Microsoft Visio 2002 removed from Microsoft Office XP Service Pack 3 section of Affected Software table. Microsoft Visio 2002 Service Pack 2 is

listed separately in the Affected Software table.

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

Last updated on 03/01/2023