Security Bulletin

Microsoft Security Bulletin MS09-009 - Critical

Vulnerabilities in Microsoft Office Excel Could Cause Remote Code Execution (968557)

Published: April 14, 2009 | Updated: April 22, 2009

Version: 1.1

General Information

Executive Summary

This security update resolves a privately reported vulnerability and a publicly disclosed vulnerability in Microsoft Office Excel. The vulnerabilities could allow remote code execution if the user opens a specially crafted Excel file. An attacker who successfully exploited 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 all supported editions of Microsoft Office Excel 2000. For all supported editions of Microsoft Office Excel 2002, Microsoft Office Excel 2003, Microsoft Office Excel 2007, Microsoft Office 2004 for Mac, and Microsoft Office 2008 for Mac; all supported versions of Microsoft Office Excel Viewer; and Microsoft Office Compatibility Pack Service Pack 1, this security update is rated Important. For more information, see the subsection, **Affected and Non-Affected Software**, in this section.

This security update addresses these vulnerabilities by modifying the way that Microsoft Office Excel opens Excel files. 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 968272.

Recommendation. Microsoft recommends that customers apply the update immediately.

Known Issues. None.

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 Excel 2000 Service Pack 3 (KB959964)	Remote Code Execution	Critical	MS08-074
Microsoft Office XP Service Pack 3	Microsoft Office Excel 2002 Service Pack 3 (KB959988)	Remote Code Execution	Important	MS08-074
Microsoft Office 2003 Service Pack 3	Microsoft Office Excel 2003 Service Pack 3 (KB959995)	Remote Code Execution	Important	MS08-074
2007 Microsoft Office System Service Pack 1	Microsoft Office Excel 2007 Service Pack 1* (KB959997)	Remote Code Execution	Important	MS08-074
Microsoft Office for Mac				
Microsoft Office 2004 for Mac (KB968695)	Not applicable	Remote Code Execution	Important	MS08-074

Office Suite and Other Software	Component	Maximum Security Impact	Aggregate Severity Rating	Bulletins Replaced by this Update
Microsoft Office 2008 for Mac (KB968694)	Not applicable	Remote Code Execution	Important	MS08-074
Other Office Software				
Microsoft Office Excel Viewer 2003 Service Pack 3 (KB959993)	Not applicable	Remote Code Execution	Important	MS08-074
Microsoft Office Excel Viewer (KB960000)	Not applicable	Remote Code Execution	Important	MS08-074
Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Service Pack 1 (KB960003)	Not applicable	Remote Code Execution	Important	MS08-074

*For Microsoft Office Excel 2007 Service Pack 1, in addition to security update package KB959997, customers also need to install the security update for Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Service Pack 1 (KB960003) to be protected from the vulnerabilities described in this bulletin.

Non-Affected Software

Expand table

Office and Other Software
Microsoft Works 8.5
Microsoft Works 9.0
Microsoft Works Suite 2005
Microsoft Works Suite 2006
Open XML File Format Converter for Mac
Microsoft Office File Converter Pack
Microsoft Office SharePoint Server 2003 Service Pack 3

Office and Other Software
Microsoft Office SharePoint Server 2007 and Microsoft Office SharePoint Server 2007 Service Pack 1 (32-bit editions)
Microsoft Office SharePoint Server 2007 and Microsoft Office SharePoint Server 2007 Service Pack 1 (64-bit editions)

Frequently Asked Questions (FAQ) Related to This Security Update

Where are the file information details?

The file information details can be found in Microsoft Knowledge Base Article 968557.

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.

What is the Microsoft Office Excel Viewer?

The Microsoft Office Excel Viewer is a replacement for all previous Excel Viewer versions, including Excel Viewer 97 and Excel Viewer 2003. With Excel Viewer, you can open, view, and print Excel workbooks, even if you don't have Excel installed. You can also copy data from Excel Viewer to another program. However, you cannot edit data, save a workbook, or create a new workbook.

Why is this update Critical for Excel 2000 but only Important for all other affected versions of Excel?

Microsoft Excel 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.

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.

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 April bulletin summary. For more information, see Microsoft Exploitability Index.

Expand table

Affected Software	Memory Corruption Vulnerability - CVE-2009-0100	Memory Corruption Vulnerability - CVE-2009-0238	Aggregate Severity Rating
Microsoft Office Suites and Components			
Microsoft Office Excel 2000 Service Pack 3	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical**
Microsoft Office Excel 2002 Service Pack 3	**Important** Remote Code Execution	**Important** Remote Code Execution	**Important**
Microsoft Office Excel 2003 Service Pack 3	**Important** Remote Code Execution	**Important** Remote Code Execution	**Important**
Microsoft Office Excel 2007 Service Pack 1	**Important** Remote Code Execution	**Important** Remote Code Execution	**Important**
Microsoft Office for Mac			
Microsoft Office 2004 for Mac	**Important** Remote Code Execution	**Important** Remote Code Execution	**Important**
Microsoft Office 2008 for Mac	**Important** Remote Code Execution	**Important** Remote Code Execution	**Important**
Other Office Software			

Affected Software	Memory Corruption Vulnerability - CVE-2009-0100	Memory Corruption Vulnerability - CVE-2009-0238	Aggregate Severity Rating
Microsoft Office Excel Viewer 2003 Service Pack 3	**Important** Remote Code Execution	**Important** Remote Code Execution	**Important**
Microsoft Office Excel Viewer	**Important** Remote Code Execution	**Important** Remote Code Execution	**Important**
Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Service Pack 1	**Important** Remote Code Execution	**Important** Remote Code Execution	**Important**

Memory Corruption Vulnerability - CVE-2009-0100

A remote code execution vulnerability exists in Microsoft Office Excel that could allow remote code execution if a user opens a specially crafted Excel file that includes a malformed object. 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.

To view this vulnerability as a standard entry in the Common Vulnerabilities and Exposures list, see CVE-2009-0100 .

Mitigating Factors for Memory Corruption Vulnerability - CVE-2009-0100

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:

- 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.
- 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 later editions of Office.

Workarounds for Memory Corruption Vulnerability - CVE-2009-0100

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 un-trusted 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 .xls, .xlt, and .xla file formats. The following table describes the command to enable or to disable MOICE for the .xls, .xlt, and .xla 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 .XLS=oice.excel.sheet	ASSOC .xls=Excel.Sheet.8
ASSOC .XLT=oice.excel.template	ASSOC .xlt=Excel.Template

Command to use to enable MOICE to be the registered handler	Command to use to disable MOICE as the registered handler
ASSOC .XLA=oice.excel.addin	ASSOC .xla=Excel.Addin

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\Excel\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.

  - **For 2007 Office system**

    Windows Registry Editor Version 5.00

    [HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Security\FileOpenBlock]

    "BinaryFiles"=dword:00000001

Note In order to use 'FileOpenBlock' with the 2007 Microsoft Office system, all of the latest security updates for the 2007 Microsoft Office system 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 922848 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\Excel\Security\FileOpenBlock]

  "BinaryFiles"=dword:00000000

- **For 2007 Office system**
  Windows Registry Editor Version 5.00

  [HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security\FileOpenBlock]

  "BinaryFiles"=dword:00000000

FAQ for Memory Corruption Vulnerability - CVE-2009-0100

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 remotely. An attacker could then install programs or view, change, or delete data; or create new accounts with full user rights.

What causes the vulnerability?
The vulnerability exists in the way that Microsoft Office Excel parses the Excel spreadsheet file format that could allow remote code execution when opening a specially crafted Excel spreadsheet.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could run arbitrary code as the logged-on

user. If a user is logged on with administrative user rights, an attacker could take complete control of the 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.

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

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

In a Web-based attack scenario, an attacker would have to host a Web site that contains an Office 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 specially crafted Web site. Instead, an attacker would have to convince them to visit the Web site, typically by getting them to click a link that takes them to the attacker's site, and then convince them to open the specially crafted Excel file.

What systems are primarily at risk from the vulnerability?
Systems where Microsoft Office Excel is used, including 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 removes the vulnerability by changing the way that Microsoft Office Excel opens specially crafted Excel files.

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 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-2009-0238

A remote code execution vulnerability exists in Microsoft Office Excel that could allow remote code execution if a user opens a specially crafted Excel file that includes a malformed object. 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.

To view this vulnerability as a standard entry in the Common Vulnerabilities and Exposures list, see CVE-2009-0238.

Mitigating Factors for Memory Corruption Vulnerability - CVE-2009-0238

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.
- 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-2009-0238

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 un-trusted 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 .xls, .xlt, and .xla file formats. The following table describes the command to enable or to disable MOICE for the .xls, .xlt, and .xla 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 .XLS=oice.excel.sheet	ASSOC .xls=Excel.Sheet.8
ASSOC .XLT=oice.excel.template	ASSOC .xlt=Excel.Template
ASSOC .XLA=oice.excel.addin	ASSOC .xla=Excel.Addin

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\Excel\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.

  - **For 2007 Office system**
    Windows Registry Editor Version 5.00

    [HKEY_CURRENT_USER\Software\Microsoft\Office\12.0\Excel\Security\FileOpenBlock]

    "BinaryFiles"=dword:00000001

    Note In order to use 'FileOpenBlock' with the 2007 Microsoft Office system, all of the latest security updates for the 2007 Microsoft Office system 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 922848 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\Excel\Security\FileOpenBlock]

"BinaryFiles"=dword:00000000

- **For 2007 Office system**
  Windows Registry Editor Version 5.00

  [HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security\FileOpenBlock]

  "BinaryFiles"=dword:00000000

FAQ for Memory Corruption Vulnerability - CVE-2009-0238

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 remotely. An attacker could then install programs or view, change, or delete data; or create new accounts with full user rights.

What causes the vulnerability?
A vulnerability exists in Microsoft Office Excel that could allow remote code execution when opening a specially crafted Excel spreadsheet. The vulnerability exists in the way that Microsoft Office Excel parses the Excel spreadsheet file format.

What might an attacker use the vulnerability to do?
An attacker who successfully exploited this vulnerability could run arbitrary code as the logged-on user. If a user is logged on with administrative user rights, an attacker could take complete control of the 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.

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

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

In a Web-based attack scenario, an attacker would have to host a Web site that contains an Office 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 specially crafted Web site. Instead, an attacker would have to convince them to visit the Web site, typically by getting them to click a link that takes them to the attacker's site and then convince them to open the specially crafted Excel 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.

What systems are primarily at risk from the vulnerability?
Systems where Microsoft Office Excel is used, including 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 removes the vulnerability by changing the way that Microsoft Excel opens specially crafted Excel 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-2009-0238. This vulnerability was first described in Microsoft Security Advisory 968272.

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.

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
Excel 2000 Service Pack 3	No

Software	MBSA 2.1
Excel 2002 Service Pack 3	Yes
Excel 2003 Service Pack 3	Yes
Excel 2007 Service Pack 1	Yes
Microsoft Office Excel Viewer 2003 Service Pack 3	Yes
Microsoft Office Excel Viewer	Yes
Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Service Pack 1	Yes
Microsoft Office 2004 for Mac	No
Microsoft Office 2008 for Mac	No

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
Excel 2000 Service Pack 3	Yes	Yes	No	No
Excel 2002 Service Pack 3	Yes	Yes	Yes	Yes
Excel 2003 Service Pack 3	Yes	Yes	Yes	Yes
Excel 2007 Service Pack 1	No	No	Yes	Yes
Microsoft Office Excel Viewer 2003 Service Pack 3	Yes	Yes	Yes	Yes
Microsoft Office Excel Viewer	No	No	Yes	Yes
Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Service Pack 1	No	No	Yes	Yes
Microsoft Office 2004 for Mac	No	No	No	No
Microsoft Office 2008 for Mac	No	No	No	No

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:

Excel 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-kb959964-fullfile-enu /q:a
Installing without	office2000-kb959964-fullfile-enu /r:n

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.**
restarting	
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 968557
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
O9EXL, O9PRM, O9PRO, O9SBE, O9PIPC1, O9PIPC2, O9STD	ExcelFiles

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**.
/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.

Excel 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	

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 user intervention	officeXP-kb959988-fullfile-enu /q:a
Installing without restarting	officeXP-kb959988-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 968557
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
PIPC1, PROPLUS, PRO, SBE, STD, STDEDU	EXCELFiles, WordNonBootFiles
EXCEL	EXCELFile

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.

Excel 2003 and Excel Viewer 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 Excel 2003:\ office2003-kb959995-fullfile-enu /q:a\ \ For Excel Viewer 2003:\ office2003-kb959993-fullfile-enu /q:a
Installing without restarting	For Excel 2003:\ office2003-kb959995-fullfile-enu /r:n\ \ For Excel Viewer 2003:\ office2003-kb959993-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 968557
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, BASIC11, PERS11, PROI11, PRO11, STDP11, EXCEL11, PRO11SB	All
XLVIEW	ExcelViewer

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.

Excel 2007, Excel Viewer, and Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats (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 Excel 2007:\ excel2007-kb959997-fullfile-x86-glb /passive\ \ For Excel Viewer:\ excelviewer2007-kb960000-fullfile-x86-glb /passive\ \ For Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Service Pack 1:\ office2007-kb960003-fullfile-x86-glb /passive\
Installing without restarting	For Excel 2007:\ excel2007-kb959997-fullfile-x86-glb /norestart\ \ For Excel Viewer:\ excelviewer2007-kb960000-fullfile-x86-glb /norestart\ \ For Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats Service Pack 1:\ office2007-kb960003-fullfile-x86-glb /norestart\
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.
File Information	See Microsoft Knowledge Base Article 968557
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.

Switch	Description
/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 11.5.4 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 11.5.4 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 11.5.4 Update volume window, double-click the Microsoft Office 2004 for Mac 11.5.4 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 Mac 11.5.4 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 **11.5.4**, 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 12.1.7 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 12.1.7 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 12.1.7 Update volume window, double-click the Microsoft Office 2008 for Mac 12.1.7 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 12.1.7 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 **12.1.7**, 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.

Other Information

Acknowledgments

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

- Haifei Li of Fortinet's FortiGuard Global Security Research Team for reporting the Memory Corruption Vulnerability (CVE-2009-0100)

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 (April 14, 2009): Bulletin published.
- V1.1 (April 22, 2009): Added Excel Viewer 2003 Service Pack 3 to the MBSA and SMS tables in the section, Detection and Deployment Tools and Guidance. This is an informational change only. There were no changes to the security update binaries or detection logic.

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

Last updated on 06/08/2023