



Software Installed by the Cisco Unity Server Updates Wizard in 2009

Revised November 25, 2009



Caution

Wizard development related to Cisco Unity 4.x and Cisco Unity Connection 1.x has ceased as of July 27, 2009 and March 12, 2009, respectively. For more information, see the Cautions at the end of the [“Servers on Which the Wizard Can Be Run”](#) section on page 3.

This document lists the Microsoft updates that are installed automatically when you run the Cisco Unity Server Updates wizard. The following information is provided for each update: the update number, related Knowledge Base article ID, severity rating, and Microsoft document title. For more information on an update, refer to the Microsoft website.

In addition, this document lists the version of Cisco Security Agent for Cisco Unity that the Cisco Unity Server Updates wizard can optionally install.



Note

Before you download and use the wizard, familiarize yourself with the information in the [“What You Need to Know About the Wizard”](#) section on page 2.

On the second Tuesday of each month, Microsoft releases its list of new security updates. We review the list and, if the updates are sufficiently important, create a new wizard. (On average, we create a new wizard about every two months.) The new wizard includes the existing updates from previous versions and the new updates that are applicable to any of the servers, including supported versions of the following software:

- Windows Server 2003
- Windows 2000 Server
- SQL Server 2000
- MSDE 2000
- Exchange Server 2003
- Exchange 2000 Server
- Internet Explorer



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

This means that you need to run only the latest wizard version to get all of the updates that are currently recommended for use with any of the applicable servers.

For support-policy information on Microsoft service packs and updates, and on Windows Automatic Updates, see *Supported Hardware and Software, and Support Policies for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

What You Need to Know About the Wizard

The following three sections contain important information about the Cisco Unity Server Updates wizard:

- [Running the Server Updates Wizard, page 2](#)
- [Servers on Which the Wizard Can Be Run, page 3](#)
- [Only English-Language Versions of Updates Provided, page 4](#)

Running the Server Updates Wizard

To ensure the best possible security for the third-party applications installed on Cisco Unity and Cisco Unity–related servers, we recommend that you do the following tasks once a month:

1. Download the latest Cisco Unity Server Updates wizard.
(Go to the Voice and Unified Communications Downloads page at <http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240>. In the tree control on the Downloads page, expand Unified Communications Applications > Voice Mail and Unified Messaging > Cisco Unity, then click the latest version of Cisco Unity and browse to the Microsoft Updates download page.)
2. During nonbusiness hours, log on to the server from the console or by using a VNC viewer. Other remote-access applications are not supported.
See also the “[Servers on Which the Wizard Can Be Run](#)” section on page 3.
3. *If you plan to install a new version of Cisco Security Agent for Cisco Unity on a server on which it is already installed:* Uninstall the existing version and restart the server before you run the Server Updates wizard.
For information on uninstalling Cisco Security Agent for Cisco Unity, see the applicable version of *Release Notes for Cisco Security Agent for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.
4. *If you uninstalled Cisco Security Agent for Cisco Unity version 3.1(5) or earlier in Task 3. and if the Cisco Unity server is running Windows Server 2003:* Check the status of the Windows firewall and, if it is enabled, disable it. In some configurations, uninstalling Cisco Security Agent for Cisco Unity version 3.1(5) or earlier causes the Windows firewall to be enabled, which causes Cisco Unity to function improperly.
5. *If you are running the wizard on a Cisco Unity server:* Use the Cisco Unity tray icon to stop the Cisco Unity software.

6. Stop antivirus services, if any.



Note If you plan to skip installing a new version of Cisco Security Agent for Cisco Unity on a server on which it is already installed, the Server Updates wizard automatically stops the agent before installing the updates.

7. Run the wizard, and follow the on-screen prompts to install updates for the software installed on the server. At the end of the wizard, choose the option to restart the server.

Progress information displayed by the individual updates is sometimes inaccurate. Do not assume that an apparent lack of progress is an indication that the installation of an update has failed. (The wizard saves detailed installation logs to C:\WINDOWS\SUWlogs.)

8. Restart antivirus services, if any.
9. Repeat Task 2. through Task 8. on the remaining servers on which the wizard can be run.

Servers on Which the Wizard Can Be Run

Revised August 25, 2009

The Cisco Unity Server Updates wizard can be run on the following Cisco Unity and Cisco Unity–related servers:

- Cisco Unity 5.x and 7.x servers.
- Cisco Unity voice-recognition servers.
- Cisco Unity Bridge servers.
- In a Cisco Unity Voice Messaging configuration, you can also run the wizard on dedicated Exchange servers and domain controllers/global catalog servers.



Caution

Wizard development related to Cisco Unity 4.x has ceased as of July 27, 2009, as documented in the “End of Software Maintenance Releases Date” milestone in the *EoS and EoL Announcement for Cisco Unity 4.x* document at http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps5745/ps2237/end_of_life_notice_cisco_unity_version_4x.html. The Cisco Unity 4.x support policy for Microsoft service packs and updates allows the installation of all Microsoft updates when they are released. Although using the Cisco Unity Server Updates wizard to install the updates may continue to work, we are no longer testing the wizard with Cisco Unity 4.x. As a result, if you encounter any problems with the wizard, Cisco TAC will not be able to help you resolve them. For the Cisco Unity 4.x support policy for Microsoft service packs and updates, see *Supported Hardware and Software, and Support Policies for Cisco Unity 4.2 and Later* at http://www.cisco.com/en/US/docs/voice_ip_comm/unity/42/support/42lsupp.html.



Caution

Wizard development related to Cisco Unity Connection 1.x has ceased as of March 12, 2009, as documented in the “End of Software Maintenance Releases Date” milestone in the *EoS and EoL Announcement for Cisco Unity Connection 1.x* document at https://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps5745/ps6509/prod_end-of-life_notice_0900aecd806c3d64.html. The Connection 1.x support policy for Microsoft service packs and updates allows the installation of all Microsoft updates when they are released. Although using the Cisco Unity Server Updates wizard to install the updates may continue to work, we are no longer testing the wizard with Connection 1.x. As a result, if you encounter any problems with the wizard, Cisco TAC will not be

able to help you resolve them. For the Connection 1.x support policy for Microsoft service packs and updates, see *Cisco Unity Connection 1.x System Requirements, and Supported Hardware and Software* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/1x/requirements/1xsyrq.html.

Only English-Language Versions of Updates Provided

The Cisco Unity Server Updates wizard contains only the English-language version of Microsoft updates. Therefore, you can use the wizard to update a server only when Windows was installed in one of the following ways:

- By using the Platform Configuration discs that are included with a Cisco Unity server purchased from Cisco.



Note Windows Server 2003 Platform Configuration discs include the Microsoft Multilingual User Interface, which allows you to localize the Windows user interface into the languages supported for use with Cisco Unity.

- By using a retail, English-language Windows disc.

You cannot use the Cisco Unity Server Updates wizard to install Microsoft updates when a localized version of Windows was installed on the server. If you installed a non-English-language version of Windows, we recommend that you use another process to download and install the Microsoft updates listed in this document (for example, Windows Automatic Update).

Wizard Version 3.0(1), November 2009

Cisco Unity Server Updates wizard version 3.0(1) installs the following software:

- Cisco Security Agent for Cisco Unity version 3.1(6).
- The Microsoft security updates listed in the following sections:
 - [Wizard Version 2.0\(19\), September 2009, page 5](#)
 - [Wizard Version 2.0\(18\), August 2009, page 6](#)
 - [Wizard Version 2.0\(17\), July 2009, page 6](#)
 - [Wizard Version 2.0\(16\), April 2009, page 7](#)
 - [Wizard Version 2.0\(15\), March 2009, page 8](#)
 - [Wizard Version 2.0\(13\), January 2009, page 9](#)
 - [Wizard Version 2.0\(12\), December 2008, page 9](#)
- The Microsoft security updates listed below.

In addition, when version 3.0(1) of the wizard is run on Windows Server 2003 SP1 or SP2, it applies the registry edit described in Microsoft Knowledge Base article KB 928046. The registry edit fixes a known issue in Cisco Unity in which administering the system over remote desktop connections in console mode crashed the Cisco Unity-CM TSP.

November 2009

MS09-066, KB 973309 (Important), *Vulnerability in Active Directory Could Allow Denial of Service*

MS09-065, KB 969947 (Critical), *Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution*

October 2009

MS09-064, KB 974783 (Critical), *Vulnerability in License Logging Server Could Allow Remote Code Execution*

MS09-062, KB 957488 (Critical), *Vulnerabilities in GDI+ Could Allow Remote Code Execution*

MS09-061, KB 974378 (Critical), *Vulnerabilities in the Microsoft .NET Common Language Runtime Could Allow Remote Code Execution*

MS09-059, KB 975467 (Important), *Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service*

MS09-058, KB 971486 (Important), *Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege*

MS09-057, KB 969059 (Important), *Vulnerability in Indexing Service Could Allow Remote Code Execution*

MS09-056, KB 974571 (Important), *Vulnerabilities in Windows CryptoAPI Could Allow Spoofing*

MS09-055, KB 973525 (Critical), *Cumulative Security Update of ActiveX Kill Bits*

MS09-054, KB 974455 (Critical), *Cumulative Security Update for Internet Explorer*

MS09-053, KB 975254 (Important), *Vulnerabilities in FTP Service for Internet Information Services Could Allow Remote Code Execution*

KB 957593, *Error message if you use the NON_CONTENT_INDEXED_SEARCH flag*

Wizard Version 2.0(19), September 2009

Cisco Unity Server Updates wizard version 2.0(19) installs the following software:

- Cisco Security Agent for Cisco Unity version 3.1(6).
- The Microsoft security updates listed in the following sections:
 - [Wizard Version 2.0\(18\), August 2009, page 6](#)
 - [Wizard Version 2.0\(17\), July 2009, page 6](#)
 - [Wizard Version 2.0\(16\), April 2009, page 7](#)
 - [Wizard Version 2.0\(15\), March 2009, page 8](#)
 - [Wizard Version 2.0\(13\), January 2009, page 9](#)
 - [Wizard Version 2.0\(12\), December 2008, page 9](#)
- The Microsoft security updates listed below.

In addition, when version 2.0(19) of the wizard is run on Windows Server 2003 SP1 or SP2, it applies the registry edit described in Microsoft Knowledge Base article KB 928046. The registry edit fixes a known issue in Cisco Unity in which administering the system over remote desktop connections in console mode crashed the Cisco Unity-CM TSP.

September 2009

- MS09-048, KB 967723 (Critical), *Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution*

- MS09-047, KB 973812 (Critical), *Vulnerabilities in Windows Media Format Could Allow Remote Code Execution*
- MS09-046, KB 956844 (Critical), *Vulnerability in DHTML Editing Component ActiveX Control Could Allow Remote Code Execution*
- MS09-045, KB 971961 (Critical), *Vulnerability in JScript Scripting Engine Could Allow Remote Code Execution*

Wizard Version 2.0(18), August 2009

Cisco Unity Server Updates wizard version 2.0(18) installs the following software:

- Cisco Security Agent for Cisco Unity version 3.1(6).
- The Microsoft security updates listed in the following sections:
 - [Wizard Version 2.0\(17\), July 2009, page 6](#)
 - [Wizard Version 2.0\(16\), April 2009, page 7](#)
 - [Wizard Version 2.0\(15\), March 2009, page 8](#)
 - [Wizard Version 2.0\(13\), January 2009, page 9](#)
 - [Wizard Version 2.0\(12\), December 2008, page 9](#)
- The Microsoft security updates listed below.

In addition, when version 2.0(18) of the wizard is run on Windows Server 2003 SP1 or SP2, it applies the registry edit described in Microsoft Knowledge Base article KB 928046. The registry edit fixes a known issue in Cisco Unity in which administering the system over remote desktop connections in console mode crashed the Cisco Unity-CM TSP.

August 2009

- MS09-044, KB 970927 (Critical), *Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution*
- MS09-042, KB 960859 (Important), *Vulnerability in Telnet Could Allow Remote Code Execution*
- MS09-041, KB 971657 (Important), *Vulnerability in Workstation Service Could Allow Elevation of Privilege*
- MS09-040, KB 971032 (Important), *Vulnerability in Message Queuing Could Allow Elevation of Privilege*
- MS09-039, KB 969883 (Critical), *Vulnerabilities in WINS Could Allow Remote Code Execution*
- MS09-038, KB 971557 (Critical), *Vulnerabilities in Windows Media File Processing Could Allow Remote Code Execution*
- MS09-037, KB 973908 (Critical), *Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution*

Wizard Version 2.0(17), July 2009

Cisco Unity Server Updates wizard version 2.0(17) installs the following software:

- Cisco Security Agent for Cisco Unity version 3.1(6).

- The Microsoft security updates listed in the following sections:
 - [Wizard Version 2.0\(16\), April 2009, page 7](#)
 - [Wizard Version 2.0\(15\), March 2009, page 8](#)
 - [Wizard Version 2.0\(13\), January 2009, page 9](#)
 - [Wizard Version 2.0\(12\), December 2008, page 9.](#)
- The Microsoft security updates listed below.

In addition, when version 2.0(17) of the wizard is run on Windows Server 2003 SP1 or SP2, it applies the registry edit described in Microsoft Knowledge Base article KB 928046. The registry edit fixes a known issue in Cisco Unity in which administering the system over remote desktop connections in console mode crashed the Cisco Unity-CM TSP.

July 2009

- MS09-032. Replaced by MS09-055, October 2009.
- MS09-029, KB 961371 (Critical), *Vulnerabilities in the Embedded OpenType Font Engine Could Allow Remote Code Execution*
- MS09-028, KB 971633 (Critical), *Vulnerabilities in Microsoft DirectShow Could Allow Remote Code Execution*

June 2009

- MS09-026, KB 970238 (Important), *Vulnerability in RPC Could Allow Elevation of Privilege*
- MS09-025. Replaced by MS09-065, November 2009.
- MS09-022, KB 961501 (Critical), *Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution*
- MS09-020, KB 970483 (Important), *Vulnerabilities in Internet Information Services (IIS) Could Allow Elevation of Privilege*
- MS09-019, KB 969897 (Critical), *Cumulative Security Update for Internet Explorer*
- MS09-018. Replaced by MS09-066, November 2009.

Wizard Version 2.0(16), April 2009

Cisco Unity Server Updates wizard version 2.0(16) installs the following software:

- Cisco Security Agent for Cisco Unity version 3.1(6).
- The Microsoft security updates listed in the following sections:
 - [Wizard Version 2.0\(15\), March 2009, page 8](#)
 - [Wizard Version 2.0\(13\), January 2009, page 9](#)
 - [Wizard Version 2.0\(12\), December 2008, page 9.](#)
- The Microsoft security updates listed below.

In addition, when version 2.0(16) of the wizard is run on Windows Server 2003 SP1 or SP2, it applies the registry edit described in Microsoft Knowledge Base article KB 928046. The registry edit fixes a known issue in Cisco Unity in which administering the system over remote desktop connections in console mode crashed the Cisco Unity-CM TSP.

April 2009

- MS09-015, KB 959426 (Moderate), *Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege*
- MS09-014. Replaced by MS09-019, June 2009.
- MS09-013, KB 960803 (Critical), *Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution*
- MS09-012, KB 959454, KB952004, and KB956572 (Important), *Vulnerabilities in Windows Could Allow Elevation of Privilege*
- MS09-011. Replaced by MS09-028, July 2009.
- MS09-010, KB 960477 (Critical), *Vulnerabilities in WordPad and Office Text Converters Could Allow Remote Code Execution*. (In the Add or Remove Programs control panel, the application is listed as KB 923561.)

Wizard Version 2.0(15), March 2009

Cisco Unity Server Updates wizard version 2.0(15) installs the following software:

- Cisco Security Agent for Cisco Unity version 3.1(6).
- The Microsoft security updates listed in the following sections:
 - [Wizard Version 2.0\(13\), January 2009, page 9](#)
 - [Wizard Version 2.0\(12\), December 2008, page 9](#).
- The Microsoft security updates listed below.

In addition, when version 2.0(15) of the wizard is run on Windows Server 2003 SP1 or SP2, it applies the registry edit described in Microsoft Knowledge Base article KB 928046. The registry edit fixes a known issue in Cisco Unity in which administering the system over remote desktop connections in console mode crashed the Cisco Unity-CM TSP.

March 2009

- MS09-008. Replaced by MS09-039, August 2009.
- MS09-007, KB 960225 (Important), *Vulnerability in SChannel Could Allow Spoofing*
- MS09-006. Replaced by MS09-025, June 2009.

February 2009

- MS09-004, KB 959420 (Important), *Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution*. (KB 959420 is the main article for this update. However, in the Add or Remove Programs control panel, the application is listed as “Security Update for SQL Server 2000 Service Pack 4 and MSDE 2000 (KB960083)”.)
- MS09-003, KB 959239 (Critical), *Vulnerabilities in Microsoft Exchange Could Allow Remote Code Execution*. (KB 959239 is the main article for this update. However, in the Add or Remove Programs control panel, the application is listed as “Security Update for Exchange 2000 Server (KB959897)”.)
- MS09-002. Replaced by MS09-014, April 2009.

December 2008

- MS08-078. Replaced by MS09-014, April 2009.

[Wizard Version 2.0(14) Was Not Released]

Wizard Version 2.0(13), January 2009

Cisco Unity Server Updates wizard version 2.0(13) installs the following software:

- Cisco Security Agent for Cisco Unity version 3.1(6).
- The Microsoft security updates listed in the [“Wizard Version 2.0\(12\), December 2008” section on page 9](#).
- The Microsoft security updates listed below.

In addition, when version 2.0(13) of the wizard is run on Windows Server 2003 SP1 or SP2, it applies the registry edit described in Microsoft Knowledge Base article KB 928046. The registry edit fixes a known issue in Cisco Unity in which administering the system over remote desktop connections in console mode crashed the Cisco Unity-CM TSP.

January 2009

- MS09-001, KB 958687 (Critical), *Vulnerabilities in SMB Could Allow Remote Code Execution*

Wizard Version 2.0(12), December 2008

Microsoft security updates included in Cisco Unity Server Updates wizard version 2.0(12), by month of their release:

December 2008

- MS08-073. Replaced by MS09-014, April 2009.
- MS08-071, KB 956802 (Critical), *Vulnerabilities in GDI Could Allow Remote Code Execution*

November 2008

- MS08-069, KB 955218, (Critical), *Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution* (KB 955218 is the main article for this update. However, in the Add or Remove Programs control panel, for Windows Server 2003 with service pack 1 or 2, two applications are listed: KB 955069 and KB 954430. For Windows 2000 Server with service pack 4, the application is listed as KB 955069.)
- MS08-068, KB 957097 (Important), *Vulnerability in SMB Could Allow Remote Code Execution*

October 2008

- MS08-067, KB 958644 (Critical), *Vulnerability in Server Service Could Allow Remote Code Execution*
- MS08-066. Replaced by MS09-008, March 2009.
- MS08-065. Replaced by MS09-040, August 2009.
- MS08-064. Replaced by MS09-012, April 2009.
- MS08-063. Replaced by MS09-001, January 2009.
- MS08-062, KB 953155 (Important), *Vulnerability in Windows Internet Printing Service Could Allow Remote Code Execution*

- MS08-061. Replaced by MS09-006, March 2009.
- MS08-060. Replaced by MS09-018, June 2009.

September 2008

- MS08-052. Replaced by MS09-062, October 2009.

August 2008

- MS08-049, KB 950974 (Important), *Vulnerabilities in Event System Could Allow Remote Code Execution*
- MS08-046, KB 952954 (Critical), *Vulnerability in Microsoft Windows Image Color Management System Could Allow Remote Code Execution*

July 2008

- MS08-039, KB 953747 (Important), *Vulnerabilities in Outlook Web Access for Exchange Server Could Allow Elevation of Privilege*
- MS08-037. Replaced by MS09-008, March 2009.

June 2008

- MS08-036, KB 950762 (Important), *Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service*
- MS08-034. Replaced by MS09-008, March 2009.
- MS08-033. Replaced by MS09-011, April 2009.
- MS08-032. Replaced by MS09-032, July 2009.

April 2008

- MS08-022, KB 944338 (Critical), *Vulnerability in VBScript and JScript Scripting Engines Could Allow Remote Code Execution*
- MS08-021, KB 948590 (Critical), *Vulnerabilities in GDI Could Allow Remote Code Execution*
- MS08-020, KB 945553 (Important), *Vulnerability in DNS Client Could Allow Spoofing*

February 2008

- MS08-008, KB 947890 and KB 943055 (Critical), *Vulnerability in OLE Automation Could Allow Remote Code Execution*
- MS08-007, KB 946026 (Critical), *Vulnerability in WebDAV Mini-Redirector Could Allow Remote Code Execution*
- MS08-006, KB 942830 (Important), *Vulnerability in Internet Information Services Could Allow Remote Code Execution*
- MS08-005, KB 942831 (Important), *Vulnerability in Internet Information Services Could Allow Elevation of Privilege*
- KB 928046, *A custom wave driver is unloaded when a remote client computer connects to a Windows Server 2003-based computer that is running a TAPI program*

January 2008

- MS08-002. Replaced by MS09-012, April 2009.

- MS08-001, KB 941644 (Critical), *Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution*

December 2007

- MS07-067, KB 944653 (Important), *Vulnerability in Macrovision Driver Could Allow Local Elevation of Privilege*

November 2007

- MS07-062, KB 941672 (Important), *Vulnerability in DNS Could Allow Spoofing* (only installed when DNS is installed on the server)
- MS07-061, KB 943460 (Critical), *Vulnerability in Windows URI Handling Could Allow Remote Code Execution*

October 2007

- MS07-058. Replaced by MS09-026, June 2009.
- MS07-051, KB 938827 (Critical), *Vulnerability in Microsoft Agent Could Allow Remote Code Execution*
- KB 933360 (none) *August 2007 Cumulative Time Zone Update for Microsoft Windows Operating Systems*

August 2007

- MS07-047. Replaced by MS09-037, August 2009.
- MS07-045, KB 937143 (Critical), *Cumulative Security Update for Internet Explorer*

July 2007

- MS07-040. Replaced by MS09-061, October 2009.

June 2007

- MS07-035. Replaced by MS09-015, April 2009.
- MS07-034, KB929123 (Critical), *Cumulative Security Update for Outlook Express and Windows Mail*
- MS07-031. Replaced by MS09-007, March 2009.

May 2007

- MS07-026, KB931832 (Critical), *Vulnerabilities in Microsoft Exchange Could Allow Remote Code Execution*

After you install MS07-026, Cisco Unity may not be able to deliver voice messages to subscribers whose Active Directory accounts belong to one or more administrative groups. For information on a workaround, refer to the tech note *Cisco Unity for Exchange Cannot Deliver Messages to Some Subscribers After MS06-019 or MS07-026 Is Installed* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_tech_notes_list.html.

April 2007

- MS07-021. Replaced by MS09-022, June 2009.
- MS07-020, KB 932168 (Critical), *Vulnerability in Microsoft Agent Could Allow Remote Code Execution*
- MS07-017, KB 925902 (Critical), *Vulnerabilities in GDI Could Allow Remote Code Execution*

February 2007

- MS07-013, KB 918118 (Important), *Vulnerability in Microsoft RichEdit Could Allow Remote Code Execution*
- MS07-012, KB 924667 (Important), *Vulnerability in Microsoft MFC Could Allow Remote Code Execution*
- MS07-011, KB 926436 (Important), *Vulnerability in Microsoft OLE Dialog Could Allow Remote Code Execution*
- MS07-009, KB 927779 (Critical), *Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution*
- MS07-008, KB 928843 (Critical), *Vulnerability in HTML Help ActiveX Control Could Allow Remote Code Execution*
- MS07-006, KB 928255 (Important), *Vulnerability in Windows Shell Could Allow Elevation of Privilege*
- KB 931836 (none), *February 2007 cumulative time zone update for Microsoft Windows operating systems*

December 2006

- MS06-078, KB925398 (Critical), *Vulnerability in Windows Media Format Could Allow Remote Code Execution*
- MS06-074, KB 926247 (Important), *Vulnerability in SNMP Could Allow Remote Code Execution*

November 2006

- MS06-070, KB 924270 (Critical), *Vulnerability in Workstation Service Could Allow Remote Code Execution*
- MS06-068, KB 920213 (Critical), *Vulnerability in Microsoft Agent Could Allow Remote Code Execution*
- MS06-066, KB 923980 (Important), *Vulnerabilities in Client Service for NetWare Could Allow Remote Code Execution*

October 2006

- MS06-065, KB 924496 (Moderate), *Vulnerability in Windows Object Packager Could Allow Remote Execution*
- MS06-064, KB 922819 (Low), *Vulnerabilities in TCP/IP IPv6 Could Allow Denial of Service*
- MS06-063, KB 923414 (Important), *Vulnerability in Server Service Could Allow Denial of Service and Remote Code Execution*
- MS06-057, KB 923191 (Critical), *Vulnerability in Windows Explorer Could Allow Remote Execution*

September 2006

- MS06-053. Replaced by MS09-057, October 2009.

August 2006

- MS06-050, KB 920670 (Important), *Vulnerabilities in Microsoft Windows Hyperlink Object Library Could Allow Remote Code Execution*

- MS06-046, KB 922616 (Critical), *Vulnerability in HTML Help Could Allow Remote Code Execution*
- MS06-044, KB 917008 (Critical), *Vulnerability in Microsoft Management Console Could Allow Remote Code Execution*
- MS06-041, KB 920683 (Critical), *Vulnerabilities in DNS Resolution Could Allow Remote Code Execution*

July 2006

- MS06-036, KB 914388 (Critical), *Vulnerability in DHCP Client Service Could Allow Remote Code Execution*
- MS06-035, KB 917159 (Critical), *Vulnerability in Server Service Could Allow Remote Code Execution*
- MS06-034, KB 917537 (Important), *Vulnerability in Microsoft Internet Information Services using Active Server Pages Could Allow Remote Code Execution*

June 2006

- MS06-031, KB 917736 (Moderate), *Vulnerability in RPC Mutual Authentication Could Allow Spoofing*
- MS06-025, KB 911280 (Critical), *Vulnerability in Routing and Remote Access Could Allow Remote Code Execution*
- MS06-022, KB 918439 (Critical), *Vulnerability in ART Image Rendering Could Allow Remote Code Execution*

May 2006

- MS06-018, KB 913580 (Moderate), *Vulnerability in Microsoft Distributed Transaction Coordinator Could Allow Denial of Service*

April 2006

- MS06-015, KB 908531 (Important), *Vulnerability in Windows Explorer Could Allow Remote Code Execution*
- MS06-014, KB 911562 (Critical), *Vulnerability in the Microsoft Data Access Components (MDAC) Function Could Allow Code Execution*

March 2006

- Cumulative Hotfix for SQL Server 2000 Service Pack 4 - Build 2187, KB 916287

February 2006

- MS06-009, KB 901190 (Important), *Vulnerability in the Korean Input Method Editor Could Allow Elevation of Privilege* (necessary only if the Korean Input Method Editor is installed)
- MS06-008, KB 911927 (Important), *Vulnerability in Web Client Service Could Allow Remote Code Execution*

January 2006

- MS06-003, KB 902412 (Critical), *Vulnerability in TNEF Decoding in Microsoft Outlook and Microsoft Exchange Could Allow Remote Code Execution*
- MS06-002. Replaced by MS09-029, July 2009.

December 2005

- MS05-055, KB 908523 (Important), *Vulnerability in Windows Kernel Could Allow Elevation of Privilege*
- MS05-053, KB 896424 (Critical), *Vulnerabilities in Graphics Rendering Engine Could Allow Code Execution*

October 2005

- MS05-051, KB 902400 (Critical), *Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution*
- MS05-049, KB 900725 (Important), *Vulnerabilities in Windows Shell Could Allow Remote Code Execution*
- MS05-048, KB 907245 (Important), *Vulnerability in the Microsoft Collaboration Data Objects Could Allow Remote Code Execution*
- MS05-047, KB 905749 (Important), *Vulnerability in Plug and Play Could Allow Remote Code Execution and Local Elevation of Privilege*
- MS05-046, KB 899589 (Important), *Vulnerability in the Client Service for NetWare Could Allow Remote Code Execution*
- MS05-045, KB 905414 (Moderate), *Vulnerability in Network Connection Manager Could Allow Denial of Service*
- MS05-044, KB 905495 (Moderate), *Vulnerability in the Windows FTP Client Could Allow File Transfer Location Tampering*

August 2005

- MS05-043, KB 896423 (Critical), *Vulnerability in Print Spooler Service Could Allow Remote Code Execution*
- MS05-042, KB 899587 (Moderate), *Vulnerabilities in Kerberos Could Allow Denial of Service, Information Disclosure, and Spoofing*
- MS05-041, KB 899591 (Moderate), *Vulnerability in Remote Desktop Protocol Could Allow Denial of Service*
- MS05-040, KB 893756 (Important), *Vulnerability in Telephony Service Could Allow Remote Code Execution*
- MS05-039, KB 899588 (Critical), *Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege*

July 2005

- MS05-036, KB 901214 (Critical), *Vulnerability in Microsoft Color Management Module Could Allow Remote Code Execution*
- MS05-032, KB 890046 (Moderate), *Vulnerability in Microsoft Agent Could Allow Spoofing*

June 2005

- Microsoft Update Rollup 1 for Windows 2000 SP4, KB 900345.
- MS05-026, KB 896358 (Critical), *Vulnerability in HTML Help Could Allow Remote Code Execution*

April 2005

- MS05-021, KB 894549 (Critical), *Vulnerability in Exchange Server Could Allow Remote Code Execution*

February 2005

- MS05-014, KB 867282 (Critical), *Cumulative Security Update for Internet Explorer*

October 2004

- MS04-036, KB 883935 (Critical), *Vulnerability in NNTP Could Allow Remote Code Execution*

August 2004

- Microsoft .NET Framework 1.1 Service Pack 1, KB 867460
- Exchange 2000 Server Post-Service Pack 3 Update Rollup, KB 870540 (None), *Availability of the August 2004 Exchange 2000 Server Post-Service Pack 3 Update Rollup*

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.

