2011 年版の Cisco Unity Server Updates ウィザードでインストールされるソフトウェア

Software Installed by the Cisco Unity Server Updates Wizard in 2011

OL-21651-01-J

注意 Cisco Unity 4.x および Cisco Unity Connection 1.x に関するウィザードの開発は、それぞれ 2009 年 7 月 27 日と 2009 年 3 月 12 日に終了しました。詳細については、「ウィザードを実行できるサーバ」（P.4）の最後にある注意を参照してください。

このマニュアルでは、Cisco Unity Server Updates ウィザードを実行すると自動的にインストールされる Microsoft 更新プログラムについて説明します。更新プログラムごとに、更新プログラム番号、関連するサポート技術情報の記事 ID、重大度、および Microsoft のドキュメントのタイトルを示します。更新プログラムの詳細は、Microsoft の Web サイトを参照してください。

また、このマニュアルでは、Cisco Unity Server Updates ウィザードでオプションとしてインストールできる Cisco Security Agent for Cisco Unity のバージョンも示します。

（注） ウィザードをダウンロードして使用する前に、「ウィザードについて知っておくべきこと」（P.2）に記載されている内容を理解してください。

毎月第 2 火曜日に、Microsoft は新しいセキュリティ更新プログラムのリストをリリースします。当社では、リストを確認し、更新プログラムが重要なものであれば、新しいウィザードを作成します（新しいウィザードは、平均して約 2 か月ごとに作成しています）。新しいウィザードには、以前のバージョンに含まれていた既存の更新プログラムと、Cisco Unity 関連サーバにある次のソフトウェアのサポート対象バージョンに該当する新しい更新プログラムが含まれています。

- Windows Server 2003
- Windows 2000 Server
- SQL Server 2005 および SQL Server 2000
- SQL Server 2005 Express および MSDE 2000
- Exchange Server 2003
- Exchange 2000 Server
- Internet Explorer

つまり、最新版のウィザードを実行するだけで、該当するサーバに対して使用するように現在推奨されているすべての更新プログラムを取得することができます。

Microsoft のサービス パックおよび更新プログラムと、Windows 自動更新に対するサポート ポリシー情報については、http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html にある『*Supported Hardware and Software, and Support Policies for Cisco Unity*』を参照してください。

ウィザードについて知っておくべきこと

次の 3 つの項では、Cisco Unity Server Updates ウィザードに関する重要な内容について説明します。

Server Updates ウィザードの実行

Cisco Unity サーバおよび Cisco Unity 関連のサーバにインストールされたサードパーティ アプリケーションのセキュリティを最善の状態に保つために、1 か月おきに次の作業を実行することを推奨します。

1. 最新の Cisco Unity Server Updates ウィザードをダウンロードします。

   http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240 にある [Voice and Unified Communications Downloads] ページにアクセスします。[Downloads] ページのツリー コントロールで、[Unified Communications Applications] > [Voice Mail and Unified Messaging] > [Cisco Unity] の順に展開し、最新版の Cisco Unity をクリックして、Microsoft 更新プログラムのダウンロード ページを参照します。

（注） ソフトウェアをダウンロードするページにアクセスするには、登録ユーザとして Cisco.com にログオンする必要があります。

2. 業務時間外に、コンソールまたは VNC ビューアを使用してサーバにログインします。その他のリモート アクセス アプリケーションはサポートされていません。

   「ウィザードを実行できるサーバ」（P.4）も参照してください。

3. *新しいバージョンの Cisco Security Agent for Cisco Unity を、それがすでにインストールされているサーバにインストールする場合は*、既存のバージョンをアンインストールし、サーバを再起動してから、Server Updates ウィザードを実行します。

（注） 2010 年 1 月より、Server Updates ウィザードによって Cisco Security Agent for Cisco Unity バージョン 3.1(7) がインストールされます。

Cisco Security Agent for Cisco Unity のアンインストールについては、http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html にある、該当するバージョンの『*Release Notes for Cisco Security Agent for Cisco Unity*』を参照してください。

4. *作業 3. で、Cisco Security Agent for Cisco Unity バージョン 3.1(5) またはそれ以前のバージョンをアンインストールし、Cisco Unity サーバが Windows Server 2003 を実行している場合*、Windows ファイアウォールのステータスを確認し、イネーブルになっている場合はディセーブルにします。設定によっては、Cisco Security Agent for Cisco Unity バージョン 3.1(5) またはそれ以前をアンインストールすると、Windows ファイアウォールがイネーブルになり、Cisco Unity が適切に動作しなくなります。

5. *ウィザードを Cisco Unity サーバで実行する場合は*、Cisco Unity トレイ アイコンを使用して Cisco Unity ソフトウェアを停止します。

6. アンチウイルス サービスがインストールされている場合は停止します。

（注） 新しいバージョンの Cisco Security Agent for Cisco Unity がすでにインストールされているサーバでインストールを省略する予定の場合は、更新プログラムをインストールする前に、Server Updates ウィザードによってエージェントが自動的に停止されます。

7. ウィザードを実行し、画面上のプロンプトに従って、サーバにインストールされているソフトウェアの更新プログラムをインストールします。ウィザードの最後で、サーバを再起動するためのオプションを選択します。

   個々の更新プログラムによって表示される進行状況の情報は、正確でない場合があります。進行状況が進まないからといって、更新プログラムのインストールが失敗したとは限りません（ウィザードでは、詳細なインストール ログが C:¥WINDOWS¥SUWlogs に保存されます）。

8. アンチウイルス サービスがインストールされている場合は再起動します。

9. ウィザードを実行できる残りのサーバで、作業 2. から作業 8. を繰り返します。

ウィザードを実行できるサーバ

Cisco Unity Server Updates ウィザードは、次の Cisco Unity サーバおよび Cisco Unity 関連のサーバで実行できます。

- Cisco Unity 5.x、7.x、8.x サーバ。
- Cisco Unity 5.x、7.x 音声認識サーバ。

（注） Cisco Unity 8.x 以降は、Linux ベースのサーバ上で Cisco Unity 音声認識アプリケーションを実行できます。

- Cisco Unity Bridge サーバ。
- Cisco Unity 音声メッセージング構成では、専用の Exchange サーバおよびドメイン コントローラ / グローバル カタログ サーバでもウィザードを実行できます。

注意 Cisco Unity 4.x に関するウィザードの開発は、http://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps5745/ps2237/end_of_life_notice_cisco_unity_version_4x.html にある『*EoS and EoL Announcement for Cisco Unity 4.x*』の「End of Software Maintenance Releases Date」マイルストーンに記載されているように、2009 年 7 月 27 日に終了しました。Microsoft サービス パックと更新プログラムに対する Cisco Unity 4.x のサポート ポリシーでは、Microsoft 更新プログラムがリリースされたときに、そのすべてのインストールが許可されています。Cisco Unity Server Updates ウィザードを使用して更新プログラムをインストールすることは引き続き可能ですが、ウィザードを Cisco Unity 4.x でテストすることは行っていません。そのため、ウィザードで問題が発生した場合でも、Cisco TAC は問題の解決を支援できません。Microsoft のサービス パックと更新プログラムに対する Cisco Unity 4.x のサポート ポリシーについては、http://www.cisco.com/en/US/docs/voice_ip_comm/unity/42/support/42lsupp.html にある『*Supported Hardware and Software, and Support Policies for Cisco Unity 4.2 and Later*』を参照してください。

注意 Cisco Unity Connection 1.x に関するウィザードの開発は、https://www.cisco.com/en/US/prod/collateral/voicesw/ps6789/ps5745/ps6509/prod_end-of-life_notice0900aecd806c3d64.html にある『*EoS and EoL Announcement for Cisco Unity Connection 1.x*』の「End of Software Maintenance Releases Date」マイルストーンに記載されているように、2009 年 3 月 12 日に終了しました。Microsoft サービス パックと更新プログラムに対する Connection 1.x のサポート ポリシーでは、Microsoft 更新プログラムがリリースされたときに、そのすべてのインストールが許可されています。Cisco Unity Server Updates ウィザードを使用して更新プログラムをインストールすることは引き続き可能ですが、ウィザードを Connection 1.x でテストすることは行っていません。そのため、ウィザードで問題が発生した場合でも、Cisco TAC は問題の解決を支援できません。Microsoft のサービス パックと更新プログラムに対する Connection 1.x のサポート ポリシーについては、http://www.cisco.com/en/US/docs/voice_ip_comm/connection/1x/requirements/1xsysrq.html にある『*Cisco Unity Connection 1.x System Requirements, and Supported Hardware and Software*』を参照してください。

英語版の更新プログラムだけを提供

Cisco Unity Server Updates ウィザードには、英語版の Microsoft 更新プログラムだけが含まれています。そのため、このウィザードを使用してサーバを更新できるのは、次のいずれかの方法で Windows がインストールされている場合だけです。

- シスコから購入した Cisco Unity サーバに付属している Platform Configuration ディスクを使用した場合。

（注） Windows Server 2003 Platform Configuration ディスクには、Microsoft Multilingual User Interface が含まれています。これを使用すると、Windows ユーザ インターフェイスを、Cisco Unity で使用できる言語にローカライズできます。

- リテール版の英語の Windows ディスクを使用した場合。

ローカライズされたバージョンの Windows がサーバにインストールされている場合は、Cisco Unity Server Updates ウィザードを使用した Microsoft 更新プログラムのインストールはできません。英語版以外のバージョンの Windows がインストールされている場合は、本書に記載されている Microsoft 更新プログラムを別の手順でダウンロードおよびインストールすることを推奨します（たとえば Windows の自動更新）。

ウィザード バージョン 3.0(11)（2011 年 3 月）

Cisco Unity Server Updates ウィザード バージョン 3.0(11) では次のソフトウェアがインストールされます。

- Cisco Security Agent for Cisco Unity バージョン 3.1(7)
- 次に示す Microsoft セキュリティ更新プログラム

また、このバージョンのウィザードが Windows Server 2003 SP1 または SP2 で動作している場合、Microsoft サポート技術情報の記事 KB 928046 に記載されているレジストリ編集を適用します。このレジストリ編集により、Cisco Unity での、コンソール モードのリモート デスクトップ接続経由でシステムを管理すると Cisco Unity-CM TSP がクラッシュするという、既知の問題が修正されます。

2011 年 3 月

- MS11-017、KB 2508062（重要）、*リモート デスクトップ クライアントの脆弱性により、リモートでコードが実行される*

2010 年 12 月

- MS10-101、KB 2207559（重要）、*Windows Netlogon サービスの脆弱性により、サービス拒否が起こる*
- MS10-099、KB 2440591（重要）、*ルーティングとリモート アクセスの脆弱性により、特権が昇格される*
- MS10-098、KB 2436673（重要）、*Windows カーネル モード ドライバの脆弱性により、特権が昇格される*
- MS10-097、KB 2443105（重要）、*インターネット接続のサインアップ ウィザードの安全でないライブラリのロードにより、リモートでコードが実行される*
- MS10-096、KB 2423089（重要）、*Windows アドレス帳の脆弱性により、リモートでコードが実行される*

- MS10-091、KB 2296199（緊急）、*OpenType フォント（OTF）ドライバの脆弱性により、リモートでコードが実行される*
- MS10-090、KB 2416400（緊急）、*Internet Explorer 用の累積的なセキュリティ更新プログラム*

2010 年 10 月

- MS10-084、KB 2360937（重要）、*Windows ローカル プロシージャ コールの脆弱性により、特権が昇格される*
- MS10-083、KB 2405882（重要）、*Windows シェルおよびワードパッドの COM の検証の脆弱性により、リモートでコードが実行される*
- MS10-081、KB 2296011（重要）、*Windows コモン コントロール ライブラリの脆弱性により、リモートでコードが実行される*
- MS10-076、KB 982132（緊急）、*Embedded OpenType フォント エンジンの脆弱性により、リモートでコードが実行される*
- MS10-074、KB 2387149（警告）、*Microsoft Foundation Classes の脆弱性により、リモートでコードが実行される*
- MS10-070、KB 2418042（重要）、*ASP.NET の脆弱性により、情報漏えいが起こる*

2010 年 9 月

- MS10-069、KB 2121546（重要）、*Windows クライアント/サーバ ランタイム サブシステムの脆弱性により、特権が昇格される*
- MS10-068、KB 983539（重要）、*Local Security Authority Subsystem Service の脆弱性により、特権が昇格される*
- MS10-067、KB 2259922（重要）、*ワードパッドのテキスト コンバーターの脆弱性により、リモートでコードが実行される*
- MS10-065、KB 2267960（重要）、*Microsoft Internet Information Service（IIS; インターネット インフォメーション サービス）の脆弱性により、リモートでコードが実行される*
- MS10-063、KB 2320113（緊急）、*Unicode スクリプト プロセッサの脆弱性により、リモートでコードが実行される*
- MS10-062、KB 975558（緊急）、*MPEG-4 コーデックの脆弱性により、リモートでコードが実行される*
- MS10-061、KB 2347290（緊急）、*印刷スプーラ サービスの脆弱性により、リモートでコードが実行される*

2010 年 8 月

- MS10-060、KB 2265906（緊急）、*Microsoft .NET 共通言語ランタイムおよび Microsoft Silverlight の脆弱性により、リモートでコードが実行される*
- MS10-054、KB 982214（緊急）、*SMB サーバの脆弱性により、リモートでコードが実行される*
- MS10-052、KB 2115168（緊急）、*Microsoft MPEG Layer-3 コーデックの脆弱性により、リモートでコードが実行される*
- MS10-051、KB 2079403（緊急）、*Microsoft XML コア サービスの脆弱性により、リモートでコードが実行される*
- MS10-049、KB 980436（緊急）、*SChannel の脆弱性により、リモートでコードが実行される*
- MS10-046、KB 2286198（緊急）、*Windows Shell の脆弱性により、リモートでコードが実行される*

2010 年 7 月

- MS10-042、KB 2229593（緊急）、*ヘルプとサポート センターの脆弱性により、リモートでコードが実行される*

2010 年 6 月

- MS10-041、KB 981343（重要）、*Microsoft .NET Framework の脆弱性により、改ざんが起こる*
- MS10-040、KB 982666（重要）、*インターネット インフォメーション サービスの脆弱性により、リモートでコードが実行される*
- MS10-034、KB 980195（緊急）、*ActiveX の Kill Bit の累積的なセキュリティ更新プログラム*

2010 年 4 月

- KB 948496、*デフォルトの SNP 機能をオフにする更新プログラムが、Windows Server 2003 ベースのコンピュータおよび Small Business Server 2003 ベースのコンピュータで利用可能*

2008 年 12 月

- KB 955839、*Microsoft Windows オペレーティング システム用の 2008 年 12 月の累積的なタイム ゾーン更新プログラム*

2008 年 7 月

- KB 953988、*IEnumVARIANT インターフェイスを使用するアプリケーションが原因でメモリ リークが発生し、Windows Server 2003 ベースのコンピュータでシステムのパフォーマンスが低下する*

2010 年 2 月

- MS10-015、KB 977165（重要）、*Windows カーネルの脆弱性により、特権が昇格される*
- MS10-014、KB 977290（重要）、*Kerberos の脆弱性により、サービス拒否が起こる*
- MS10-013、KB 977935（緊急）、*Microsoft DirectShow の脆弱性により、リモートでコードが実行される*
- MS010-012、KB 971468（重要）、*SMB サーバの脆弱性により、リモートでコードが実行される*
- MS010-011、KB 978037（重要）、*Windows クライアント/サーバ ランタイム サブシステムの脆弱性により、特権が昇格される*
- MS010-008、KB 978262（緊急）、*ActiveX の Kill Bit の累積的なセキュリティ更新プログラム*
- MS010-007、KB 975713（緊急）、*Windows Shell ハンドラーの脆弱性により、リモートでコードが実行される*
- MS010-006、KB 978251（緊急）、*SMB クライアントの脆弱性により、リモートでコードが実行される*
- MS010-005、KB 978706（警告）、*Microsoft ペイントの脆弱性により、リモートでコードが実行される*

2010 年 1 月

- MS10-001、KB 972270（緊急）、*Embedded OpenType フォント エンジンの脆弱性により、リモートでコードが実行される*

2009 年 12 月

- MS09-073、KB 975539（重要）、*ワードパッドおよび Office テキスト コンバーターの脆弱性により、リモートでコードが実行される*
- MS09-071、KB 974318（緊急）、*インターネット認証サービスの脆弱性により、リモートでコードが実行される*
- MS09-070、KB 971726（重要）、*Active Directory フェデレーション サービスの脆弱性により、リモートでコードが実行される*
- MS09-069、KB 974392（重要）、*Local Security Authority Subsystem Service の脆弱性により、サービス拒否が起こる*

2009 年 10 月

- MS09-064、KB 974783（緊急）、*ライセンス ログ サーバーの脆弱性により、リモートでコードが実行される*
- MS09-062、KB 957488（緊急）、*GDI+ の脆弱性により、リモートでコードが実行される*
- MS09-059、KB 975467（重要）、*Local Security Authority Subsystem Service の脆弱性により、サービス拒否が起こる*
- MS09-057、KB 969059（重要）、*インデックス サービスの脆弱性により、リモートでコードが実行される*
- MS09-056、KB 974571（重要）、*Windows CryptoAPI の脆弱性により、スプーフィングが行われる*
- MS09-053、KB 975254（重要）、*インターネット インフォメーション サービスの FTP サービスの脆弱性により、リモートでコードが実行される*
- KB 957593、*NON_CONTENT_INDEXED_SEARCH フラグを使用するとエラー メッセージが表示される*

2009 年 9 月

- MS09-048、KB 967723（緊急）、*Windows TCP/IP の脆弱性により、リモートでコードが実行される*
- MS09-047、KB 973812（緊急）、*Windows Media Format の脆弱性により、リモートでコードが実行される*
- MS09-046、KB 956844（緊急）、*DHTML 編集コンポーネントの ActiveX コントロールの脆弱性により、リモートでコードが実行される*
- MS09-045、KB 971961（緊急）、*JScript スクリプト エンジンの脆弱性により、リモートでコードが実行される*

2009 年 8 月

- MS09-044、KB 970927（緊急）、*リモート デスクトップ接続の脆弱性により、リモートでコードが実行される*
- MS09-042、KB 960859（重要）、*Telnet の脆弱性により、リモートでコードが実行される*
- MS09-041、KB 971657（重要）、*ワークステーション サービスの脆弱性により、特権が昇格される*
- MS09-040、KB 971032（重要）、*メッセージ キューの脆弱性により、特権が昇格される*
- MS09-039、KB 969883（緊急）、*WINS の脆弱性により、リモートでコードが実行される*
- MS09-037、KB 973908（緊急）、*Microsoft Active Template Library（ATL）の脆弱性により、リモートでコードが実行される*

2009 年 6 月

- MS09-022、KB 961501（緊急）、*Windows 印刷スプーラーの脆弱性により、リモートでコードが実行される*
- MS09-020、KB 970483（重要）、*Internet Information Service（IIS; インターネット インフォメーション サービス）の脆弱性により、特権の昇格が起こる*
- MS09-019、KB 969897（緊急）、*Internet Explorer 用の累積的なセキュリティ更新プログラム*

2009 年 4 月

- MS09-015、KB 959426（警告）、*SearchPath の複合的な攻撃の脆弱性により、特権が昇格される*
- MS09-013、KB 960803（緊急）、*Windows HTTP サービスの脆弱性により、リモートでコードが実行される*
- MS09-012、KB 959454、KB952004、および KB956572（重要）、*Windows の脆弱性により、特権が昇格される*
- MS09-010、KB 960477（緊急）、*ワードパッドおよび Office テキスト コンバーターの脆弱性により、リモートでコードが実行される*（コントロール パネルのプログラムの追加と削除では、このアプリケーションは KB 923561 と表示されます）

2009 年 3 月

- MS09-007、KB 960225（重要）、*SChannel の脆弱性により、スプーフィングが行われる*

2009 年 2 月

- MS09-004、KB 959420（重要）、*Microsoft SQL Server の脆弱性により、リモートでコードが実行される*（KB 959420 は、この更新プログラムの主な記事です。ただし、コントロール パネルの [Add or Remove Programs] では、アプリケーションは「Security Update for SQL Server 2000 Service Pack 4 and MSDE 2000 (KB960083)」と表示されます）
- MS09-003、KB 959239（緊急）、*Microsoft Exchange の脆弱性により、リモートでコードが実行される*（KB 959239 は、この更新プログラムの主な記事です。ただし、コントロール パネルの [Add or Remove Programs] では、アプリケーションは「Security Update for Exchange 2000 Server (KB959897)」と表示されます）

2008 年 12 月

- MS08-071、KB 956802（緊急）、*GDI の脆弱性により、リモートでコードが実行される*

2008 年 11 月

- MS08-068、KB 957097（重要）、*SMB の脆弱性により、リモートでコードが実行される*

2008 年 10 月

- MS08-067、KB 958644（緊急）、*Server サービスの脆弱性により、リモートでコードが実行される*
- MS08-062、KB 953155（重要）、*Windows インターネット印刷サービスの脆弱性により、リモートでコードが実行される*

2008 年 8 月

- MS08-049、KB 950974（重要）、*イベント システムの脆弱性により、リモートでコードが実行される*
- MS08-046、KB 952954（緊急）、*Microsoft Windows イメージ カラー管理モジュールの脆弱性により、リモートでコードが実行される*

2008 年 7 月

- MS08-039、KB 953747（重要）、*Exchange Server の Outlook Web Access の脆弱性により、特権が昇格される*

2008 年 6 月

- MS08-036、KB 950762（重要）、*Pragmatic General Multicast（PGM）の脆弱性により、サービス拒否が起こる*

2008 年 4 月

- MS08-022、KB 944338（緊急）、*VBScript および JScript スクリプト エンジンの脆弱性により、リモートでコードが実行される可能性がある*
- MS08-021、KB 948590（緊急）、*GDI の脆弱性により、リモートでコードが実行される*
- MS08-020、KB 945553（重要）、*DNS クライアントの脆弱性により、スプーフィングが行われる*

2008 年 2 月

- MS08-008、KB 947890 および KB 943055（緊急）、*OLE オートメーションの脆弱性により、リモートでコードが実行される*
- MS08-007、KB 946026（緊急）、*WebDAV Mini-Redirector の脆弱性により、リモートでコードが実行される*
- MS08-005、KB 942831（重要）、*インターネット インフォメーション サービスの脆弱性により、特権の昇格が起こる*
- KB 928046、*リモート クライアント コンピュータが、TAPI プログラムを実行中の Windows Server 2003 ベースのコンピュータに接続すると、カスタム WAVE ドライバがアンロードされる*

2008 年 1 月

- MS08-001、KB 941644（緊急）、*Windows TCP/IP の脆弱性により、リモートでコードが実行される*

2007 年 12 月

- MS07-067、KB 944653（重要）、*Macrovision ドライバの脆弱性により、ローカルで特権が昇格される*

2007 年 11 月

- MS07-062、KB 941672（重要）*DNS の脆弱性により、スプーフィングが行われる*（サーバに DNS がインストールされている場合にだけインストールされます）
- MS07-061、KB 943460（緊急）、*Windows URI 処理の脆弱性により、リモートでコードが実行される*

2007 年 10 月

- MS07-051、KB 938827（緊急）、*Microsoft エージェントの脆弱性により、リモートでコードが実行される*

2007 年 8 月

- MS07-045、KB 937143（緊急）、*Internet Explorer 用の累積的なセキュリティ更新プログラム*

2007 年 6 月

- MS07-034、KB929123（緊急）、*Outlook Express および Windows メール用の累積的なセキュリティ更新プログラム*

2007 年 5 月

- MS07-026、KB931832（緊急）、*Microsoft Exchange の脆弱性により、リモートでコードが実行される*

  MS07-026 をインストールした後、Cisco Unity で、サブスクライバの Active Directory アカウントが 1 つ以上の管理グループに属している場合、そのサブスクライバに音声メッセージを配信できなくなることがあります。回避策については、http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_tech_notes_list.html にある技術資料『*Cisco Unity for Exchange Cannot Deliver Messages to Some Subscribers After MS06-019 or MS07-026 Is Installed*』を参照してください。

2007 年 4 月

- MS07-020、KB 932168（緊急）、*Microsoft エージェントの脆弱性により、リモートでコードが実行される*
- MS07-017、KB 925902（緊急）、*GDI の脆弱性により、リモートでコードが実行される*

2007 年 2 月

- MS07-013、KB 918118（重要）、*Microsoft リッチ エディットの脆弱性により、リモートでコードが実行される*
- MS07-011、KB 926436（重要）、*Microsoft OLE ダイアログの脆弱性により、リモートでコードが実行される*
- MS07-009、KB 927779（緊急）、*Microsoft Data Access Components の脆弱性により、リモートでコードが実行される*
- MS07-008、KB 928843（緊急）、*HTML ヘルプの ActiveX コントロールの脆弱性により、リモートでコードが実行される*
- MS07-006、KB 928255（重要）、*Windows シェルの脆弱性により、特権が昇格される*
- KB 931836（なし）、*Microsoft Windows オペレーティング システム用の 2007 年 2 月の累積的なタイム ゾーン更新プログラム*

2006 年 12 月

- MS06-078、KB925398（緊急）、*Windows Media Format の脆弱性により、リモートでコードが実行される*
- MS06-074、KB 926247（重要）、*SNMP の脆弱性により、リモートでコードが実行される*

2006 年 11 月

- MS06-070、KB 924270（緊急）、*Workstation サービスの脆弱性により、リモートでコードが実行される*
- MS06-066、KB 923980（重要）、*Netware 用クライアント サービスの脆弱性により、リモートでコードが実行される*

2006 年 10 月

- MS06-065、KB 924496（警告）、*Windows オブジェクト パッケージャの脆弱性により、リモートでコードが実行される*
- MS06-064、KB 922819（注意）*TCP/IP IPv6 の脆弱性により、サービス拒否が起こる*
- MS06-063、KB 923414（重要）、*Server サービスの脆弱性により、サービス拒否およびリモートでのコードの実行が起こる*
- MS06-057、KB 923191（緊急）、*Windows Explorer の脆弱性により、リモートでコードが実行される*

2006 年 8 月

- MS06-050、KB 920670（重要）、*Microsoft Windows ハイパーリンク オブジェクト ライブラリの脆弱性により、リモートでコードが実行される*
- MS06-046、KB 922616（緊急）、*HTML ヘルプの脆弱性により、リモートでコードが実行される*
- MS06-044、KB 917008（緊急）、*Microsoft 管理コンソールの脆弱性により、リモートでコードが実行される*
- MS06-041、KB 920683（緊急）、*DNS 解決の脆弱性により、リモートでコードが実行される*

2006 年 7 月

- MS06-036、KB 914388（緊急）、*DHCP クライアント サービスの脆弱性により、リモートでコードが実行される*
- MS06-035、KB 917159（緊急）、Server サービスの脆弱性により、リモートでコードが実行される
- MS06-034、KB 917537（重要）、*Active Server Pages を使用した Microsoft インターネット インフォメーション サービスの脆弱性により、リモートでコードが実行される*

2006 年 6 月

- MS06-031、KB 917736（警告）*RPC の相互認証の脆弱性により、スプーフィングが行われる*
- MS06-022、KB 918439（緊急）、*ART の画像表示の脆弱性により、リモートでコードが実行される*

2006 年 5 月

- MS06-018、KB 913580（警告）、*Microsoft Distributed Transaction Coordinator の脆弱性によりサービス拒否が起こる*

2006 年 4 月

- MS06-015、KB 908531（重要）、*Windows エクスプローラの脆弱性により、リモートでコードが実行される*
- MS06-014、KB 911562（緊急）、*Microsoft Data Access Components（MDAC）の機能の脆弱性により、コードが実行される可能性がある*

2006 年 3 月

- SQL Server 2000 Service Pack 4 ビルド 2187 用に入手できる累積的な修正プログラム パッケージ、KB 916287

2006 年 2 月

- MS06-009、KB 901190（重要）、*韓国語版 Input Method Editor の脆弱性により、特権が昇格される*（韓国語版 Input Method Editor がインストールされている場合だけ必要）
- MS06-008、KB 911927（重要）、*WebClient サービスの脆弱性により、リモートでコードが実行される*

2006 年 1 月

- MS06-003、KB 902412（緊急）、*Microsoft Outlook および Microsoft Exchange の TNEF デコードの脆弱性により、リモートでコードが実行される*

2005 年 12 月

- MS05-055、KB 908523（重要）、Windows カーネルの脆弱性により、特権が昇格される
- MS05-053、KB 896424（緊急）、*Graphics Rendering Engine の脆弱性によりコードが実行される可能性がある*

2005 年 10 月

- MS05-051、KB 902400（緊急）、*MSDTC および COM+ の脆弱性により、リモートでコードが実行される*
- MS05-049、KB 900725（重要）、*Windows シェルの脆弱性により、リモートでコードが実行される*
- MS05-048、KB 907245（重要）、*Microsoft Collaboration Data Objects の脆弱性により、リモートでコードが実行される*
- MS05-047、KB 905749（重要）、*プラグ アンド プレイの脆弱性により、リモートでコードが実行され、ローカルで特権の昇格が行われる*
- MS05-046、KB 899589（重要）、*NetWare 用クライアント サービスの脆弱性により、リモートでコードが実行される*
- MS05-045、KB 905414（警告）、*ネットワーク接続マネージャの脆弱性により、サービス拒否が起こる*
- MS05-044、KB 905495（警告）、*Windows FTP クライアントの脆弱性により、ファイルの転送場所が改ざんされる*

2005 年 8 月

- MS05-043、KB 896423（緊急）、*印刷スプーラの脆弱性により、リモートでコードが実行される*
- MS05-042、KB 899587（警告）、*Kerberos の脆弱性により、サービス拒否、情報漏えいおよびスプーフィングが行われる*
- MS05-041、KB 899591（警告）、*リモート デスクトップ プロトコルの脆弱性により、サービス拒否が起こる*
- MS05-040、KB 893756（重要）、*テレフォニー サービスの脆弱性により、リモートでコードが実行される*
- MS05-039、KB 899588（緊急）、*プラグアンド プレイの脆弱性により、リモートでコードが実行され、特権の昇格が行われる*

2005 年 7 月

- MS05-036、KB 901214（緊急）、*マイクロソフト カラー管理モジュールの脆弱性によりリモートでコードが実行される*
- MS05-032、KB 890046（警告）、*Microsoft エージェントの脆弱性により、スプーフィングが行われる*

2005 年 6 月

- Windows 2000 Service Pack 4 対応の更新プログラム ロールアップ 1、KB 900345
- MS05-026、KB 896358（緊急）、*HTML ヘルプの脆弱性により、リモートでコードが実行される*

2005 年 4 月

- MS05-021、KB 894549（緊急）、*Exchange Server の脆弱性により、リモートでコードが実行される*

2005 年 2 月

- MS05-014、KB 867282（緊急）、*Internet Explorer 用の累積的なセキュリティ更新プログラム*

2004 年 10 月

- MS04-036、KB 883935（緊急）、*NNTP の脆弱性により、コードが実行される*

2004 年 8 月

- Microsoft .NET Framework 1.1 Service Pack 1、KB 867460
- Exchange 2000 Server Service Pack 3 以降の更新プログラムのロールアップ、KB 870540（なし）、*2004 年 8 月公開の Exchange 2000 Server Service Pack 3 以降の更新プログラムのロールアップ*
