



eSecurity Advisory April 2007 MICROSOFT SECURITY BULLETIN RELEASE

The purpose of this update is to provide you with a summary of Microsoft's April 2007 Security Bulletin releases.

NEW BULLETINS

Microsoft is releasing the following security bulletins for newly discovered vulnerabilities:

| MAXIMUM SEVERITY | BULLETIN NUMBER | PRODUCTS AFFECTED | IMPACT |
|------------------|-----------------|---|------------------------|
| Critical | MS07-018 | Content Management Server 2001 and Content Management Server 2002 | Remote Code Execution |
| Critical | MS07-019 | Microsoft Windows XP | Remote Code Execution |
| Critical | MS07-020 | Windows 2000, Windows XP, Windows Server 2003 | Remote Code Execution |
| Critical | MS07-021 | All current versions of Microsoft Windows | Remote Code Execution |
| Important | MS07-022 | Windows 2000, Windows XP, Windows Server 2003 | Elevation of Privilege |

Microsoft Windows Malicious Software Removal Tool

Microsoft is releasing an updated version of the Microsoft Windows Malicious Software Removal Tool on Windows Server Update Services (WSUS), Windows Update (WU) and the Download Center. Note that this tool will NOT be distributed using Software Update Services (SUS). Information on the Microsoft Windows Malicious Software Removal Tool can be located here:

<http://go.microsoft.com/fwlink/?LinkId=40573>

High-Priority Non-Security Updates on Microsoft Update (MU), Windows Update (WU), Windows Server Update Services (WSUS) and Software Update Services (SUS)

Microsoft is also releasing High-Priority NON-SECURITY updates today on WU, MU, SUS and WSUS. For complete details on non-security updates being released today please review the following KB Article: <http://support.microsoft.com/?id=894199>

A summary for this new bulletin may be found at:

<http://www.microsoft.com/technet/security/bulletin/ms07-apr.msp>.

TechNet Webcast:

Information about Microsoft's April Security Bulletin Release

Microsoft will be discussing today's bulletin during their regularly scheduled April 2007 TechNet Security Bulletin webcast. This month, the webcast will be held Wednesday, 11 April 2007 11:00 AM (GMT-08:00) PT.

You can register for it here: <http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?culture=en-US&EventID=1032327017>.

Agencies are advised to review the information in the bulletins, test and deploy the updates immediately in their environments, if applicable.

Technical Details

MS07-018

Title: Vulnerabilities in Microsoft Content Management Server Could Allow Remote Code Execution (925939)

Executive Summary:

This update resolves two newly discovered, privately reported vulnerabilities. Each vulnerability is documented in the "Vulnerability Details" section of this bulletin. We recommend that customers apply the update immediately.

Restart Requirement: To help reduce the chance that a restart will be required, stop all affected services and close all applications that may use the affected files prior to installing the security update. For more information about the reasons why you may be prompted to restart your computer, see Microsoft Knowledge Base Article 887012 (<http://support.microsoft.com/kb/887012>).

Removal Information: After you install the update, you cannot remove it. To revert to an installation before the update was installed; you must remove the application, and then install it again from the original CD-ROM.

Affected Software:

- Microsoft Content Management Server 2001 Service Pack 1
- Microsoft Content Management Server 2002 Service Pack 2

Impact of Vulnerability: [Remote Code Execution](#)

Maximum Severity Rating: **Critical**

More information on this vulnerability is available at:

<http://www.microsoft.com/technet/security/bulletin/MS07-018.msp>

MS07-019

Title: Vulnerability in Universal Plug and Play Could Allow Remote Code Execution (931261)

Executive Summary:

This update resolves a newly discovered, privately reported vulnerability. The vulnerability is documented in its own subsection in the Vulnerability Details section of this bulletin. We recommend that customers apply the update immediately.

Restart Requirement: You must restart your system after you apply this security update. For more information about the reasons why you may be prompted to restart your computer, see Microsoft Knowledge Base Article 887012 (<http://support.microsoft.com/kb/887012>).

Removal Information: To remove this security update, use the Add or Remove Programs tool in Control Panel. System administrators can also use the Spuninst.exe utility to remove this security update.

Affected Software:

- Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition and Microsoft Windows XP Professional x64 Edition

Impact of Vulnerability: [Remote Code Execution](#)

Maximum Severity Rating: **Critical**

More information on this vulnerability is available at:

<http://www.microsoft.com/technet/security/bulletin/MS07-019.mspx>

MS07-020

Title: Vulnerability in Microsoft Agent Could Allow Remote Code Execution (932168)

Executive Summary:

This update resolves a newly discovered, privately reported vulnerability. The vulnerability is documented in its own subsection in the Vulnerability Details section of this bulletin. We recommend that customers apply the update immediately.

Restart Requirement: You must restart your system after you apply this security update. For more information about the reasons why you may be prompted to restart your computer, see Microsoft Knowledge Base Article 887012 (<http://support.microsoft.com/kb/887012>).

Removal Information: To remove this security update, use the Add or Remove Programs tool in Control Panel. System administrators can also use the Spuninst.exe utility to remove this security update.

Affected Software:

- Windows 2000 Service Pack 4
- Windows XP Service Pack 2
- Windows XP Professional x64 Edition
- Windows XP Professional x64 Edition Service Pack 2
- Windows Server 2003
- Windows Server 2003 Service Pack 1
- Windows Server 2003 Service Pack 2
- Windows Server 2003 for Itanium-based Systems
- Windows Server 2003 with SP1 for Itanium-based Systems
- Windows Server 2003 with SP2 for Itanium-based Systems
- Windows Server 2003 x64 Edition
- Windows Server 2003 x64 Edition Service Pack 2

Impact of Vulnerability: [Remote Code Execution](#)

Maximum Severity Rating: **Critical**

More information on this vulnerability is available at:

<http://www.microsoft.com/technet/security/bulletin/MS07-020.msp>

MS07-021

Title: Vulnerabilities in CSRSS Could Allow Remote Code Execution (930178)

Executive Summary:

This update resolves several newly discovered, privately and publicly disclosed vulnerabilities. Each vulnerability is documented in its own subsection in the Vulnerability Details section of this bulletin. An attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. We recommend that customers apply the update immediately.

Restart Requirement: You must restart your system after you apply this security update. For more information about the reasons why you may be prompted to restart your computer, see Microsoft Knowledge Base Article 887012 (<http://support.microsoft.com/kb/887012>).

Removal Information:

- **Windows 2000, Windows XP and Windows Server 2003:** To remove this security update use the Add or Remove Programs tool in Control Panel. System administrators can also use the Spuninst.exe utility to remove this security update.
- **Windows Vista:** To remove this update, click Control Panel, click Security, then under Windows Update, click *View installed updates* and select from the list of updates.

Affected Software:

- Windows 2000 Service Pack 4
- Windows XP Service Pack 2
- Windows XP Professional x64 Edition
- Windows XP Professional x64 Edition Service Pack 2
- Windows Server 2003
- Windows Server 2003 Service Pack 1
- Windows Server 2003 Service Pack 2
- Windows Server 2003 for Itanium-based Systems
- Windows Server 2003 with SP1 for Itanium-based Systems
- Windows Server 2003 with SP2 for Itanium-based Systems
- Windows Server 2003 x64 Edition
- Windows Server 2003 x64 Edition Service Pack 2
- Windows Vista
- Windows Vista x64 Edition

Impact of Vulnerability: [Remote Code Execution](#)

Maximum Severity Rating: **Critical**

More information on this vulnerability is available at:

<http://www.microsoft.com/technet/security/bulletin/MS07-021.msp>

MS07-022

Title: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (931784)

Executive Summary:

This update resolves a newly discovered, privately reported vulnerability. The vulnerability is documented in its own subsection in the Vulnerability Details section of this bulletin. 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. We recommend that customers apply the update at the earliest opportunity.

Restart Requirement: You must restart your system after you apply this security update. For more information about the reasons why you may be prompted to restart your computer, see Microsoft Knowledge Base Article 887012 (<http://support.microsoft.com/kb/887012>).

Removal Information: To remove this security update, use the Add or Remove Programs tool in Control Panel. System administrators can also use the Spuninst.exe utility to remove this security update.

Affected Software:

- Windows 2000 Service Pack 4
- Windows XP Service Pack 2
- Windows Server 2003
- Windows Server 2003 Service Pack 1
- Windows Server 2003 Service Pack 2

Impact of Vulnerability: Elevation of Privilege

Maximum Severity Rating: **Important**

More information on this vulnerability is available at:

<http://www.microsoft.com/technet/security/bulletin/MS07-022.mspx>

PLEASE VISIT <http://www.microsoft.com/technet/security> FOR THE MOST CURRENT INFORMATION ON THESE ALERTS.