



eSecurity Advisory
May 2007 MICROSOFT SECURITY BULLETIN RELEASE

The purpose of this update is to provide you with a summary of Microsoft's May 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	MS07-023	Microsoft Excel	Remote Code Execution
Critical	MS07-024	Microsoft Word 2000,2002, 2003, 2004(Mac)	Remote Code Execution
Critical	MS07-025	Microsoft Office	Remote Code Execution
Critical	MS07-026	Microsoft Exchange	Remote Code Execution
Critical	MS07-027	Internet Explorer	Remote Code Execution
Critical	MS07-028	CAPICOM, BizTalk Server	Remote Code Execution
Critical	MS07-029	Windows 2000, Windows Server 2003	Remote Code Execution

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-May.msp>.

TechNet Webcast:

Information about Microsoft's May Security Bulletin Release

Microsoft will be discussing today's bulletin during their regularly scheduled May 2007 TechNet Security Bulletin webcast. This month, the webcast will be held Wednesday, May 9, 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=1032327015>

The on-demand version: will be available 24 hours after the live Webcast at:

<http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?culture=en-US&EventID=1032327015>

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

Technical Details

MS07-023

Title: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (934233)

Executive Summary:

A remote code execution vulnerability exists in the way Excel handles files with malformed BIFF records, files with specially crafted set font values, and files with specially crafted filter records. Such files might be included in an e-mail attachment or hosted on a malicious Web site. An attacker could exploit the vulnerability by constructing a specially crafted Excel file that could allow remote code execution.

Affected Software:

- Microsoft Excel 2000
- Microsoft Excel 2002
- Microsoft Excel 2003
- Microsoft Excel 2003 Viewer
- Microsoft Office Excel 2007
- Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats
- Microsoft Office 2004 for Mac

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/MS07-023.aspx>

MS07-024

Title: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (934232)

Executive Summary:

A remote code execution vulnerability exists in the way Microsoft Word handles data within an array, handles a specially crafted Word Document stream, and parses certain rich text properties within a file. Such specially crafted files might be included as an e-mail attachment or hosted on a malicious Web site. An attacker could exploit the vulnerability by constructing a specially crafted Word file that could allow remote code execution.

Affected Software:

- Microsoft Word 2000
- Microsoft Word 2002
- Microsoft Word 2003
- Microsoft Word Viewer 2003
- Microsoft Office 2004 for Mac
- Microsoft Works Suite 2004
- Microsoft Works Suite 2005
- Microsoft Works Suite 2006

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/MS07-024.msp>

MS07-025

Title: Vulnerability in Microsoft Office Could Allow Remote Code Execution (934873)

Executive Summary:

A remote code execution vulnerability exists in the way Microsoft Office handles a specially crafted drawing object. An attacker could exploit this vulnerability when Office parses a file and processes a malformed drawing object. Such a specially crafted file might be included as an e-mail attachment or hosted on a malicious Web site. An attacker could exploit the vulnerability by constructing a specially crafted Office file containing a malformed drawing object that could allow remote code execution.

Affected Software:

- Microsoft Office 2000 Service Pack 3:
 - ◆ Microsoft Excel 2000
 - ◆ Microsoft FrontPage 2000
 - ◆ Microsoft Publisher 2000
- Microsoft Office XP Service Pack 3:
 - ◆ Microsoft Excel 2002
 - ◆ Microsoft FrontPage 2002
 - ◆ Microsoft Publisher 2002
- Microsoft Office 2003 Service Pack 2:
 - ◆ Microsoft Excel 2003
 - ◆ Microsoft FrontPage 2003
 - ◆ Microsoft Publisher 2003
 - ◆ Microsoft Excel 2003 Viewer
- 2007 Microsoft Office System:
 - ◆ Microsoft Office Excel 2007
 - ◆ Microsoft Office Publisher 2007
 - ◆ Microsoft Office SharePoint Designer 2007
 - ◆ Microsoft Expression Web
- Microsoft Office 2004 for Mac

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/MS07-025.msp>

MS07-026

Title: Vulnerabilities in Microsoft Exchange Could Allow Remote Code Execution (931832)

Executive Summary:

This update resolves several newly discovered, privately reported 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.

Restart Requirement:

This update does not require a restart. The installer stops the required services, applies the update, and then restarts the services. However, if the required services cannot be stopped for any reason, or if required files are being used, this update will require a restart. If this behavior occurs, a message appears that advises you to restart. For more information about the reasons why you may be prompted to restart your computer, see [Microsoft Knowledge Base Article 887012](#).

Removal Information:

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

Affected Software:

- Microsoft Exchange 2000 Server Service Pack 3 with the Exchange 2000 Post-Service Pack 3 Update Rollup of August 2004
- Microsoft Exchange Server 2003 Service Pack 1
- Microsoft Exchange Server 2003 Service Pack 2
- Microsoft Exchange Server 2007

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/MS07-026.msp>

MS07-027

Title: Cumulative Security Update for Internet Explorer (931768)

Executive Summary:

A remote code execution vulnerability exists in the way Internet Explorer instantiates COM objects that are not intended to be instantiated in Internet Explorer. A remote code execution vulnerability exists in the way Internet Explorer accessing a object when it is not initiated or already deleted. A remote code execution vulnerability exists in the way Internet Explorer handles a property method. Several remote code execution vulnerabilities exist in Internet Explorer due to attempts to access uninitialized memory in certain situations. An attacker could exploit these vulnerabilities by constructing a specially crafted Web page. If a user viewed the Web page, these vulnerabilities could allow remote code execution. An attacker who successfully exploited these vulnerabilities could take complete control of an affected system.

Restart Requirement: You must restart your system after you apply this security update.

Affected Software:

- Microsoft Internet Explorer 5.01 Service Pack 4 on Windows 2000 Service Pack 4
- Microsoft Internet Explorer 6 Service Pack 1 when installed on Windows 2000 Service Pack 4
- Microsoft Internet Explorer 6 for Windows XP Service Pack 2
- Microsoft Internet Explorer 6 for Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2
- Microsoft Internet Explorer 6 for Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2
- Microsoft Internet Explorer 6 for Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems
- Microsoft Internet Explorer 6 for Windows Server 2003 x64 Edition Service Pack 1 and Windows Server 2003 x64 Edition Service Pack 2
- Windows Internet Explorer 7 for Windows XP Service Pack 2
- Windows Internet Explorer 7 for Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2
- Windows Internet Explorer 7 for Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2
- Windows Internet Explorer 7 for Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems
- Windows Internet Explorer 7 for Windows Server 2003 x64 Edition Service Pack 1 and Windows Server 2003 x64 Edition Service Pack 2
- Windows Internet Explorer 7 in Windows Vista
- Windows Internet Explorer 7 in Windows Vista x64 Edition

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

Caveats:

[Microsoft Knowledge Base Article 931768](#) documents the currently known issues that customers may experience when they install this security update. The article also documents recommended solutions for these issues. For more information, see [Microsoft Knowledge Base Article 931768](#).

Maximum Severity Rating: **Critical**

More information on this vulnerability is available at:

<http://www.microsoft.com/technet/security/bulletin/MS07-027.msp>

MS07-028

Title: Vulnerability in CAPICOM Could Allow Remote Code Execution (931906)

Executive Summary: A remote code execution vulnerability exists in Cryptographic API Component Object Model (CAPICOM) that could allow an attacker who successfully exploited this vulnerability to take complete control of the affected system.

Restart Requirement: You must restart your system after you apply this security update.

Affected Software:

- CAPICOM
- Platform SDK Redistributable: CAPICOM
- BizTalk Server 2004 Service Pack 1
- BizTalk Server 2004 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/MS07-028.msp>

MS07-029

Title: Vulnerability in Windows DNS RPC Interface Could Allow Remote Code Execution (935966)

Executive Summary:

Restart Requirement: You must restart your system after you apply this security update.

Affected Software:

- Microsoft Windows 2000 Server Service Pack 4
- Microsoft Windows Server 2003 Service Pack 1 and Microsoft Windows Server 2003 Service Pack 2
- Microsoft Windows Server 2003 with SP1 for Itanium-based Systems and Microsoft Windows Server 2003 with SP2 for Itanium-based Systems
- Microsoft Windows Server 2003 x64 Edition Service Pack 1 and Microsoft 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/MS07-029.msp>

eSecurity Advisory: MAY 2007 MICROSOFT SECURITY BULLETIN RELEASE

Delaware Department of Technology and Information

May 8, 2007

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