February 15, 2007

DELAWARE DEPARTMENT OF TECHNOLOGY & INFORMATION

Enabling Excellence In Delaware State Government

SECURITY - Now ...more than ever!

Cyber Security - Disaster Recovery - Continuity of Government

http://dti.delaware.gov/cybersecurity

eSecurity Advisory

FEBRUARY 2007 MICROSOFT SECURITY BULLETIN RELEASE

This alert is to provide you with an overview of Security Bulletins released on 13 February 2007.

New Bulletins

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

MAXIMUM SEVERITY	BULLETIN NUMBER	AFFECTED PRODUCT OR COMPONENT	IMPACT
Important	MS07-005	Step-by-Step Interactive Training	Remote Code Execution
Important	MS07-006	Windows Shell	Elevation of Privilege
Important	MS07-007	Windows Image Acquisition Service	Elevation of Privilege
Critical	MS07-008	HTML Help ActiveX Control	Remote Code Execution
Critical	MS07-009	Microsoft Data Access Components	Remote Code Execution
Critical	MS07-010	Microsoft Malware Protection Engine	Remote Code Execution
Important	MS07-011	Microsoft OLE Dialog	Remote Code Execution
Important	MS07-012	Microsoft MFC	Remote Code Execution
Important	MS07-013	Microsoft RichEdit	Remote Code Execution
Critical	MS07-014	Microsoft Word	Remote Code Execution
Critical	MS07-015	Microsoft Office	Remote Code Execution
Critical	MS07-016	Internet Explorer	Remote Code Execution

Summaries for these new bulletins may be found at the following pages:

1. http://www.microsoft.com/technet/security/bulletin/ms07-Feb.mspx

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

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 today also making the following High-Priority NON-SECURITY updates available on WU, MU, SUS and WSUS:

KB NUMBER	TITLE	Distribution:
931836	**Update for Windows XP (Daylight Savings Time)**	WU, MU
925720	February 2007 CardSpace Update for Windows XP	WU, MU
924885	Update for Outlook Junk Email Filter 2003	MU
924884	Update for Outlook Junk Email Filter 2007	MU
925251	Update for Office 2003	MU
929058	Update for Excel 2003	MU
929060	Update for PowerPoint 2003	MU
926666	**Update for Daylight Saving Time changes in 2007 for Exchange 2003**	MU

RESOURCES RELATED TO THIS ALERT

- **TechNet Webcast:**
- TechNet Webcast: Information about Microsoft's February Security Bulletins (Level 200)
- The on-demand version of the Webcast will be available at:

http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?culture=en-US&EventID=1032323262

TECHNICAL DETAILS

MS07-005

Title: Vulnerability in Step-by-Step Interactive Training Could Allow Remote Code Execution (923723)

Affected Software:

- Step-by-Step Interactive Training when installed on Microsoft Windows 2000 Service Pack 4
- Step-by-Step Interactive Training when installed on Microsoft Windows XP Service Pack 2
- Step-by-Step Interactive Training when installed on Microsoft Windows XP Professional x64 Edition
- Step-by-Step Interactive Training when installed on Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- Step-by-Step Interactive Training when installed on Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- Step-by-Step Interactive Training when installed on Microsoft Windows Server 2003 x64 Edition

Note: The Step-by-Step Interactive Training software is included with many Microsoft Press titles. Use the information in the section, "Frequently Asked Questions (FAQ) Related to This Security Update", to help determine whether you require this security update.

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: Important

Restart Requirement: Please see the Bulletin for further details

Removal Information: Please see the Bulletin for further details

More information on this vulnerability is available at:

http://www.microsoft.com/technet/security/bulletin/MS07-005.mspx

---

MS07-006

Title: Vulnerability in Windows Shell Could Allow Elevation of Privilege (928255)

Affected Software:

- Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- Microsoft Windows Server 2003 x64 Edition

Non-Affected Software:

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows Vista

Impact of Vulnerability: Elevation of Privilege

Maximum Severity Rating: Important

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

Removal Information: To remove this 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.

More information on this vulnerability is available at:

http://www.microsoft.com/technet/security/bulletin/MS07-006.mspx

---

MS07-007

Title: Vulnerability in Windows Image Acquisition Service Could Allow Elevation of Privilege (927802)

Affected Software:

- Microsoft Windows XP Service Pack 2

Non-Affected Software:

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

Impact of Vulnerability: Elevation of Privilege

Maximum Severity Rating: Important

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

Removal Information: To remove this 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.

More information on this vulnerability is available at:

http://www.microsoft.com/technet/security/bulletin/MS07-007.mspx

---

MS07-008

Title: Vulnerability in HTML Help ActiveX Control Could Allow Remote Code Execution (928843)

Affected Software:

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

Non-Affected Software:

- Windows Vista

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: Critical

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

Removal Information: To remove this 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.

More information on this vulnerability is available at:

http://www.microsoft.com/technet/security/bulletin/MS07-008.mspx

---

MS07-009

Title: Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (927779)

Affected Software:

- Microsoft Data Access Components 2.5 Service Pack 3 on Microsoft Windows 2000 Service Pack 4
- Microsoft Data Access Components 2.8 Service Pack 1 on Microsoft Windows XP Service Pack 2
- Microsoft Data Access Components 2.8 on Microsoft Windows Server 2003

- Microsoft Data Access Components 2.8 on Microsoft Windows Server 2003 for Itanium-based Systems

Non-Affected Software:

- Microsoft Data Access Components 2.8 Service Pack 2 on Microsoft Windows XP Professional x64 Edition
- Microsoft Data Access Components 2.8 Service Pack 2 on Microsoft Windows Server 2003 Service Pack 1
- Microsoft Data Access Components 2.8 Service Pack 2 on Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- Microsoft Data Access Components 2.8 Service Pack 2 on Microsoft Windows Server 2003 x64 Edition
- Windows Data Access Components 6.0 on Windows Vista

Tested Microsoft Windows Components:

Affected Components:

- Microsoft Data Access Components 2.7 Service Pack 1 when installed on Microsoft Windows 2000 Service Pack 4
- Microsoft Data Access Components 2.8 when installed on Microsoft Windows 2000 Service Pack 4
- Microsoft Data Access Components 2.8 Service Pack 1 when installed on Microsoft Windows 2000 Service Pack 4

Note: The "Affected Software" section applies to MDAC that shipped with a Microsoft Windows operating system. The "Affected Components" section applies to MDAC that was downloaded and installed onto a Microsoft Windows operating system.

Note: Microsoft strongly recommends that all customers who currently use a version of Windows that does not have Microsoft Data Access Components 2.7 Service Pack 1 or higher upgrade immediately to Microsoft Data Access Components 2.8 Service Pack 1 or another supported version. The only exception to this notice is customers who currently use Windows 2000 Service Pack 4 running Microsoft Data Access Components 2.5 Service Pack 3. See Knowledge Base Article 915387 for more information.

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: Critical

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.

Removal Information: To remove this 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.

More information on this vulnerability is available at:

http://www.microsoft.com/technet/security/bulletin/MS07-009.mspx

---

MS07-010

Title: Vulnerability in Microsoft Malware Protection Engine Could Allow Remote Code Execution (932135)

Affected Software:

- Windows Live OneCare
- Microsoft Antigen for Exchange Server 9.x
- Microsoft Antigen for SMTP Server 9.x
- Microsoft Windows Defender

- Microsoft Windows Defender x64 Edition
- Microsoft Windows Defender in Windows Vista
- Microsoft Forefront Security for Exchange Server 10
- Microsoft Forefront Security for SharePoint Server 10

Affected Components:

- Microsoft Malware Protection Engine

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: **Critical**

Restart Requirement: Varies depending on the component being updated. Please review the security bulletin for further details**.**

Removal Information: Varies depending on the component being updated. Please review the security bulletin for further details.

More information on this vulnerability is available at:

http://www.microsoft.com/technet/security/bulletin/MS07-010.mspx

---

MS07-011

Title: Vulnerability in Microsoft OLE Dialog Could Allow Remote Code Execution (926436)

Affected Software:

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

Non-Affected Software:

- Windows Vista

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: **Important**

Restart Requirement: 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.

Removal Information: To remove this 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.

More information on this vulnerability is available at:

http://www.microsoft.com/technet/security/bulletin/MS07-011.mspx

---

MS07-012

Title: Vulnerability in Microsoft MFC Could Allow Remote Code Execution (924667)

Affected Software:

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- Microsoft Windows Server 2003 x64 Edition
- Microsoft Visual Studio .NET 2002
- Microsoft Visual Studio .NET 2002 Service Pack 1
- Microsoft Visual Studio .NET 2003
- Microsoft Visual Studio .NET 2003 Service Pack 1

Non-Affected Software:

- Windows Vista
- Microsoft Visual Studio 2005

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: Important

Restart Requirement: Varies depending on the component being updated. Please review the security bulletin for further details**.**

Removal Information: To remove this update, use the Add or Remove Programs tool in Control Panel.

More information on this vulnerability is available at:

http://www.microsoft.com/technet/security/bulletin/MS07-012.mspx

---

MS07-013

Title: Vulnerability in Microsoft RichEdit Could Allow Remote Code Execution (918118)

Tested Software and Security Update Download Locations:

Affected Software:

Windows Software:

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

Office Software:

- Microsoft Office 2000 Service Pack 3
  - Microsoft Access 2000
  - Microsoft Excel 2000
  - Microsoft FrontPage 2000
  - Microsoft Outlook 2000
  - Microsoft PowerPoint 2000
  - Microsoft Publisher 2000
  - Microsoft Word 2000

- Microsoft Office XP Service Pack 3
  - Microsoft Access 2002
  - Microsoft Excel 2002
  - Microsoft FrontPage 2002
  - Microsoft Outlook 2002
  - Microsoft PowerPoint 2002
  - Microsoft Publisher 2002
  - Microsoft Word 2002

- Microsoft Office 2003 Service Pack 2
  - Microsoft Access 2003
  - Microsoft Excel 2003
  - Microsoft FrontPage 2003
  - Microsoft InfoPath 2003
  - Microsoft OneNote 2003
  - Microsoft Outlook 2003
  - Microsoft PowerPoint 2003
  - Microsoft Project 2003
  - Microsoft Publisher 2003
  - Microsoft Visio 2003
  - Microsoft Word 2003
  - Microsoft Word 2003 Viewer

- Microsoft Project 2000 Service Release 1
- Microsoft Office 2000 Multilanguage Packs
- Microsoft Project 2002 Service Pack 1
- Microsoft Visio 2002 Service Pack 2
- Microsoft Learning Essentials 1.0, 1.1, and 1.5 for Microsoft Office
- Microsoft Global Input Method Editor for Office 2000 (Japanese)
- Microsoft Office 2004 for Mac

Non-Affected Software:

- Windows Vista
- 2007 Microsoft Office System
- Microsoft Office 2003 Service Pack 2
  - Microsoft Excel 2003 Viewer
  - Microsoft PowerPoint 2003 Viewer

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: Important

Restart Requirement: Varies depending on the component being updated. Please review the security bulletin for further details**.**

Removal Information: Varies depending on the component being updated. Please review the security bulletin for further details.

More information on this vulnerability is available at:

http://www.microsoft.com/technet/security/bulletin/MS07-013.mspx

---

MS07-014

Title: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (929434)

Tested Software and Security Update Download Locations:

Affected Software:

- Microsoft Office 2000 Service Pack 3
  - Microsoft Word 2000
- Microsoft Office XP Service Pack 3
  - Microsoft Word 2002
- Microsoft Office 2003 Service Pack 2
  - Microsoft Word 2003
  - Microsoft Word Viewer 2003
- Microsoft Works Suites:
  - Microsoft Works Suite 2004
  - Microsoft Works Suite 2005
  - Microsoft Works Suite 2006
- Microsoft Office 2004 for Mac

Non-Affected Software:

- 2007 Microsoft Office System
  - Microsoft Office Word 2007

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: **Critical**

Restart Requirement: Varies depending on the component being updated. Please review the security bulletin for further details**.**

Removal Information: Varies depending on the component being updated. Please review the security bulletin for further details.

More information on this vulnerability is available at:

http://www.microsoft.com/technet/security/bulletin/MS07-014.mspx

---

MS07-015

Title: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (932554)

Tested Software and Security Update Download Locations:

Affected Software:

Microsoft Office 2000 Service Pack 3

- Microsoft Access 2000
- Microsoft Excel 2000
- Microsoft FrontPage 2000
- Microsoft Outlook 2000
- Microsoft PowerPoint 2000
- Microsoft Publisher 2000
- Microsoft Word 2000

Microsoft Office XP Service Pack 3

- Microsoft Access 2002
- Microsoft Excel 2002
- Microsoft FrontPage 2002
- Microsoft Outlook 2002
- Microsoft PowerPoint 2002
- Microsoft Publisher 2002
- Microsoft Visio 2002
- Microsoft Word 2002

Microsoft Office 2003 Service Pack 2

- Microsoft Access 2003
- Microsoft Excel 2003
- Microsoft Excel 2003 Viewer
- Microsoft FrontPage 2003
- Microsoft InfoPath 2003
- Microsoft OneNote 2003
- Microsoft Outlook 2003
- Microsoft PowerPoint 2003
- Microsoft Project 2003
- Microsoft Publisher 2003
- Microsoft Visio 2003
- Microsoft Word 2003
- Microsoft Excel 2003 Viewer
- Microsoft Word 2003 Viewer

- Microsoft Project 2000 Service Release 1
- Microsoft Project 2002 Service Pack 1
- Microsoft Visio 2002 Service Pack 2
- Microsoft Office 2004 for Mac

Non-Affected Software:

- 2007 Microsoft Office System

- Microsoft Office 2003 Service Pack 2
  - Microsoft PowerPoint 2003 Viewer

Microsoft Works Suites:
- Microsoft Works Suite 2004
- Microsoft Works Suite 2005
- Microsoft Works Suite 2006

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: **Critical**

Restart Requirement: Varies depending on the component being updated. Please review the security bulletin for further details**.**

Removal Information: Varies depending on the component being updated. Please review the security bulletin for further details.

More information on this vulnerability is available at:

http://www.microsoft.com/technet/security/bulletin/MS07-015.mspx

---

MS07-016

Title: Cumulative Security Update for Internet Explorer (928090)

Tested Software and Security Update Download Locations:

Affected Software:

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

Non-Affected Software:

- Windows Vista

Tested Microsoft Windows Components:

Affected Components:

- 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
- Microsoft Internet Explorer 6 for Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- Microsoft Internet Explorer 6 for Windows Server 2003 for Itanium-based Systems and Windows Server 2003 with SP1 for Itanium-based Systems
- Microsoft Internet Explorer 6 for Windows Server 2003 x64 Edition
- Windows Internet Explorer 7 for Windows XP Service Pack 2

- Windows Internet Explorer 7 for Windows XP Professional x64 Edition
- Windows Internet Explorer 7 for Windows Server 2003 Service Pack 1
- Windows Internet Explorer 7 for Windows Server 2003 with SP1 for Itanium-based Systems
- Windows Internet Explorer 7 for Windows Server 2003 x64 Edition

Non-Affected Components:

- Windows Internet Explorer 7 in Windows Vista

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: **Critical**

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

Removal Information: To remove this 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.

More information on this vulnerability is available at:

http://www.microsoft.com/technet/security/bulletin/MS07-016.mspx

---

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