

Microsoft Security Bulletin Review

January 9, 2007

Overview

Microsoft confirmed vulnerabilities in various products in their product portfolio and released patches on January 9, 2007 to minimize risks posed by the vulnerabilities in question. The purpose of this meeting is to analyze and categorize the new vulnerabilities relative to the overall security posture of PHS IS Infrastructure.

Agenda

- Discuss impact of MS vulnerabilities.
- Discuss patch deployment timelines.
- Action Items for follow-up
- Question and Comments

Vulnerabilities

MAXIMUM SEVERITY	BULLETIN NUMBER	PRODUCTS AFFECTED	IMPACT
Important	MS07-001	Vulnerability in Microsoft Office 2003 Brazilian Portuguese Grammar Checker	Remote Code Execution
Critical	MS07-002	Vulnerabilities in Microsoft Excel mac issue, can't uninstall patch, must install excel again	Remote Code Execution
Critical	MS07-003	Vulnerabilities in Microsoft Outlook	Remote Code Execution
Critical	MS07-004	Vulnerability in Vector Markup Language	Remote Code Execution

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

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

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>

MS07-001

Title: Vulnerability in Microsoft Office 2003 Brazilian Portuguese Grammar Checker Could Allow Remote Code Execution (921585)

Affected Software:

- Microsoft Office 2003 Service Pack 2 (Brazilian Portuguese Version)
 - Microsoft Word 2003
 - Microsoft Excel 2003
 - Microsoft Outlook 2003
 - Microsoft Access 2003
 - Microsoft OneNote 2003
 - Microsoft PowerPoint 2003
 - Microsoft Publisher 2003
 - Microsoft Access 2003
 - Microsoft InfoPath 2003
 - Microsoft FrontPage 2003
 - Microsoft Visio 2003
 - Microsoft Visio Enterprise Architects 2003
- Microsoft Office Multilingual User Interface 2003 Service Pack 2
- Microsoft Project Multilingual User Interface 2003 Service Pack 2
- Microsoft Visio Multilingual User Interface 2003 Service Pack 2
- Microsoft Office Proofing Tools 2003 Service Pack 2

Non-Affected Software:

- Microsoft Office 2000
- Microsoft Office XP
- Microsoft Office 2007
- Microsoft Office v.X for Mac
- Microsoft Office 2004 for Mac

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: **Important**

Security Update Replacement: None

Caveats: None

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, see [Microsoft Knowledge Base Article 887012](#).

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

More information on this vulnerability is available at:
<http://www.microsoft.com/technet/security/bulletin/MS07-001.msp>

MS07-002

Title: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (927198)

Affected Software:

- Microsoft Office 2000 Service Pack 3
 - Microsoft Excel 2000
- Microsoft Office XP Service Pack 3
 - Microsoft Excel 2002
- Microsoft Office 2003 Service Pack 2
 - Microsoft Excel 2003
 - Microsoft Office Excel Viewer 2003
- Microsoft Works Suites:
 - Microsoft Works Suite 2004
 - Microsoft Works Suite 2005
- Microsoft Office 2004 for Mac
- Microsoft Office v. X for Mac
- **Mac users: (NOTE: the patch cannot be uninstalled without a complete re-install of Office)**

Non-Affected Software:

- 2007 Microsoft Office system
 - Microsoft Office Excel 2007
- Microsoft Works Suites:
 - Microsoft Works Suite 2006

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: **Critical**

Security Update Replacement: This bulletin replaces a prior security update. See the frequently asked questions (FAQ) section of this bulletin for the complete list.

Caveats: None

Restart Requirement: Varies depending on which product version is being updated. Please see the bulletin's *Security Update Information* section for more details.

Removal Information: Varies depending on which product version is being updated. Please see the bulletin's *Security Update Information* section for more details.

More information on this vulnerability is available at:

<http://www.microsoft.com/technet/security/bulletin/MS07-002.msp>

MS07-003

Title: Vulnerabilities in Microsoft Outlook Could Allow Remote Code Execution (925938)

Affected Software:

- Microsoft Office 2000 Service Pack 3

- Microsoft Outlook 2000
- Microsoft Office XP Service Pack 3
- Microsoft Outlook 2002
- Microsoft Office 2003 Service Pack 2
- Microsoft Outlook 2003

Non-Affected Software:

- Microsoft Office 2007
- Microsoft Office Outlook 2007

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: **Critical**

Security Update Replacement: This bulletin replaces a prior security update. See the frequently asked questions (FAQ) section of this bulletin for the complete list.

Caveats: [Microsoft Knowledge Base Article 925938](#) documents the currently known issues that customers may experience when they install this security update. The article also documents recommended solutions for these issues.

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, see [Microsoft Knowledge Base Article 887012](#).

Removal Information: Varies depending on which product version is being updated. Please see the bulletin's *Security Update Information* section for more details.

More information on this vulnerability is available at:
<http://www.microsoft.com/technet/security/bulletin/MS07-003.mspx>

MS07-004

Title: Vulnerability in Vector Markup Language Could Allow Remote Code Execution (929969)

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

Affected Components:

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

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 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.

More information on this vulnerability is available at:

<http://www.microsoft.com/technet/security/bulletin/MS07-004.msp>