



eSecurity Advisory January 2007 MICROSOFT SECURITY BULLETIN RELEASE

The purpose of this update is to provide you with a summary of the Microsoft January 2007 Security Bulletin release.

NEW BULLETINS

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

MAXIMUM SEVERITY	BULLETIN NUMBER	PRODUCTS AFFECTED	IMPACT
Important	MS07-001	Microsoft Office	Remote Code Execution
Critical	MS07-002	Microsoft Office	Remote Code Execution
Critical	MS07-003	Microsoft Office	Remote Code Execution
Critical	MS07-004	Microsoft Windows, IE	Remote Code Execution

Summaries for these new bulletins may be found at:

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

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

Listed below is more technical information that may be helpful to users to protect their work and home computers.

MS07-001

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

Executive Summary:

A remote code execution vulnerability exists in Office 2003 Brazilian Portuguese Grammar Checker. An attacker could exploit this vulnerability when Office opens a file and parses the text.

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

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

Maximum Severity Rating: **Important**

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)

Executive Summary:

Several remote code execution vulnerabilities exist in Microsoft Excel. An attacker could exploit these vulnerabilities when Excel parses a file and processes a malformed regular, IMDATA, string, column, or palette record.

Affected Software:

- Microsoft Excel 2000
- Microsoft Excel 2002
- Microsoft Excel 2003
- Microsoft Excel Viewer 2003
- Microsoft Works Suite 2004
- Microsoft Works Suite 2005
- Microsoft Office 2004 for Mac
- Microsoft Office v.X 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/MS07-002.msp>

MS07-003

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

Executive Summary:

eSecurity Advisory: JANUARY 2007 MICROSOFT SECURITY BULLETIN RELEASE

Delaware Department of Technology and Information
January 09, 2006

- 1) A remote code execution vulnerability exists in Microsoft Outlook. An attacker could exploit this vulnerability when Outlook parses a file and processes a malformed VEVENT record.
- 2) A denial of service vulnerability exists in Outlook in its processing of e-mail header information.
- 3) A remote code execution vulnerability exists in Microsoft Outlook. An attacker could exploit this vulnerability when Outlook parses an .oss file.

Affected Software:

- Microsoft Outlook 2000
- Microsoft Outlook 2002
- Microsoft Outlook 2003

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/MS07-003.msp>

MS07-004

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

Executive Summary:

A remote code execution vulnerability exists in the Vector Markup Language (VML) implementation in Microsoft Windows.

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

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**

eSecurity Advisory: JANUARY 2007 MICROSOFT SECURITY BULLETIN RELEASE

Delaware Department of Technology and Information
January 09, 2006

More information on this vulnerability is available at:

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