



eSecurity Advisory OCTOBER 2006 MICROSOFT SECURITY BULLETIN RELEASE

The purpose of this update is to provide you with a summary of the Microsoft October 2006 Security Bulletin release.

NEW BULLETINS

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

MAXIMUM SEVERITY	BULLETIN NUMBER	PRODUCTS AFFECTED	IMPACT
Low	MS06-064	Microsoft Windows	Denial of Service
Moderate	MS06-056	Microsoft Windows	Information Disclosure
Moderate	MS06-065	Microsoft Windows	Remote Code Execution
Important	MS06-063	Microsoft Windows	Remote Code Execution
Critical	MS06-057	Microsoft Windows	Remote Code Execution
Critical	MS06-058	Microsoft Office (PowerPoint)	Remote Code Execution
Critical	MS06-059	Microsoft Office (Excel)	Remote Code Execution
Critical	MS06-060	Microsoft Office (Word)	Remote Code Execution
Critical	MS06-061	Microsoft Windows	Remote Code Execution
Critical	MS06-062	Microsoft Office	Remote Code Execution

Summaries for these new bulletins may be found at:
<http://www.microsoft.com/technet/security/bulletin/ms06-oct.mspx>.

Customers are advised to review the information in the eSecurity bulletin and to test and deploy the updates immediately in their environments, if applicable. These updates can be obtained manually from the Microsoft Update web site at <http://update.microsoft.com> or automatically using Microsoft's Automatic Update.

See http://www.microsoft.com/athome/security/update/msupdate_keep_current.mspx for more information on keeping your system current using Microsoft's Update features.

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

MS06-064

Title: Vulnerabilities in TCP/IP Could Allow Denial of Service (922819)

Executive Summary:

This update resolves several vulnerabilities in Windows, the most critical of which could allow denial of service.

Affected Software:

- Microsoft Windows XP Service Pack 1 and 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

Impact of Vulnerability: Denial of Service

Maximum Severity Rating: Low

More information on this vulnerability is available at:

<http://www.microsoft.com/technet/security/bulletin/ms06-064.mspx>

MS06-056

Title: Vulnerability in ASP.NET Could Allow Information Disclosure (922770)

Executive Summary:

A cross-site scripting vulnerability exists in a server running a vulnerable version of the .Net Framework 2.0 that could inject a client side script in the user's browser. The script could spoof content, disclose information, or take any action that the user could take on the affected web site. Attempts to exploit this vulnerability require user interaction.

Affected Software:

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

Affected Components:

- Microsoft .NET Framework 2.0

Impact of Vulnerability: Information Disclosure

Maximum Severity Rating: Moderate

More information on this vulnerability is available at:

<http://www.microsoft.com/technet/security/bulletin/ms06-056.mspx>

MS06-065

Title: Vulnerability In Windows Object Packager Could Allow Remote Code Execution (924496)

Executive Summary:

A remote code execution vulnerability exists in Windows Object Packager because of the way that file extensions are handled. An attacker could exploit the vulnerability by constructing a specially crafted file that could potentially allow remote code execution if a user visited a specially crafted Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, significant user interaction is required to exploit this vulnerability.

Affected Software:

- Microsoft Windows XP Service Pack 1 and 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

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: **Moderate**

More information on this vulnerability is available at:

<http://www.microsoft.com/technet/security/bulletin/ms06-065.mspx>

MS06-063

Title: Vulnerability in Server Service Could Allow Denial of Service and Remote Code Execution (923414)

Executive Summary:

A denial of service vulnerability exists in the Server service because of the way it handles certain network messages. An attacker could exploit the vulnerability by sending a specially crafted network message to a computer running the Server service. An attacker who successfully exploited this vulnerability could cause the computer to stop responding.

A remote code execution vulnerability exists in the Server service because of the way it handles certain network messages. An attacker could exploit the vulnerability by sending a specially crafted network message to a system running the Server service as an authenticated user. While an attacker who successfully exploited this vulnerability could take complete control of the affected system, attempts to exploit this vulnerability will most probably result in a Denial of Service condition.

Affected Software:

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 and 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

Impact of Vulnerability: Denial of Service and Remote Code Execution

Maximum Severity Rating: **Important**

More information on this vulnerability is available at:

<http://www.microsoft.com/technet/security/bulletin/ms06-063.mspx>

MS06-057

Title: Vulnerability in ASP.NET Could Allow Information Disclosure (922770)

Executive Summary:

A remote code execution vulnerability exists in Windows Shell due to improper validation of input parameters when invoked by the WebViewFolderIcon ActiveX control (Web View). This vulnerability could potentially allow remote code execution if a user visited a specially crafted Web site or viewed a specially crafted e-mail message. An attacker could exploit the vulnerability by hosting a web site that contained a web page that was used to exploit this vulnerability. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Affected Software:

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 or Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows XP Tablet PC Edition
- Microsoft Windows XP Media Center Edition
- Microsoft Windows Server 2003 or Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 for Itanium-based Systems or Windows Server 2003 with SP1 for Itanium-based Systems
- Microsoft Windows Server 2003 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/ms06-057.mspx>

MS06-058

Title: Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (924163)

Executive Summary:

Several remote code execution vulnerabilities exist in PowerPoint. An attacker could exploit these vulnerabilities when PowerPoint parsed a file that included a malformed object pointer, parsed a file that included a malformed Data record, or opened a specially crafted file. Such a file might be included in an e-mail attachment or hosted on a malicious web site.

Affected Software:

- Microsoft Office 2000 Service Pack 3

- Microsoft PowerPoint 2000
- Microsoft Office XP Service Pack 3
- Microsoft PowerPoint 2002
- Microsoft Office 2003 Service Pack 1 or Service Pack 2
- Microsoft Office PowerPoint 2003
- Microsoft Office 2004 for Mac
- Microsoft PowerPoint 2004 for Mac
- Microsoft Office v. X for Mac
- Microsoft PowerPoint 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/ms06-058.mspx>

MS06-059

Title: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (924164)

Executive Summary:

This update addresses several newly discovered, privately reported and public vulnerabilities. Remote code execution vulnerabilities exist in Excel. An attacker could exploit these vulnerabilities when Excel parses a file and processes a malformed DATETIME record, parses a file and processes a malformed STYLE record, handles a Lotus 1-2-3 file, or parses a file and processes a malformed COLINFO record.

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 1 or Service Pack 2
- Microsoft Office Excel 2003
- Microsoft Office Excel Viewer 2003
- Microsoft Office 2004 for Mac
- Microsoft Excel 2004 for Mac
- Microsoft Office v. X for Mac
- Microsoft Excel v. X for Mac
- Microsoft Works Suites: 2004, 2005, 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/ms06-059.mspx>

MS06-060

Title: Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (924554)

Executive Summary:

Remote code execution vulnerabilities exist in Word. An attacker could exploit these vulnerabilities when Word parses a file that contains a malformed string, opens a specially crafted mail-merge file, or opens a specially crafted Word file. Such specially crafted files might be included as e-mail attachments or hosted on a malicious web site.

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 1 or Service Pack 2
- Microsoft Office Word 2003
- Microsoft Office Word 2003 Viewer
- Microsoft Works Suites: 2004, 2005, 2006
- 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/ms06-060.mspx>

MS06-061

Title: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (924191)

Executive Summary:

A vulnerability exists in Microsoft XML Core Services that could allow for information disclosure because the XMLHTTP ActiveX control incorrectly interprets an HTTP server-side redirect. An attacker could exploit the vulnerability by constructing a specially crafted Web page that could potentially lead to information disclosure if a user visited that page or clicked a link in a specially crafted e-mail message. An attacker who successfully exploited this vulnerability could access content from another domain retrieved using the credentials of the user browsing the Web at the client. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. However, user interaction is required to exploit this vulnerability.

A vulnerability exists in XSLT processing that could allow remote code execution on an affected system. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited that page. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Affected Software:

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 or Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows XP Media Center Edition
- Microsoft Windows Server 2003 or Microsoft Windows Server 2003 Service Pack 1

eSecurity Advisory: OCTOBER 2006 MICROSOFT SECURITY BULLETIN RELEASE

Delaware Department of Technology and Information
October 11, 2006

- Microsoft Windows Server 2003 for Itanium-based Systems or Windows Server 2003 with SP1 for Itanium-based Systems
- Microsoft Windows Server 2003 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/ms06-061.mspx>

MS06-062

Title: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (922581)

Executive Summary:

Remote code execution vulnerabilities exist in Office. An attacker could exploit these vulnerabilities when Office parses a file with a malformed string., parses a file with a malformed chart record, parses a file with a malformed record, or parses a malformed Smart Tag.

Affected Software:

- Microsoft Office 2000 Service Pack 3
- Microsoft Office XP Service Pack 3
- Microsoft Office 2003 Service Pack 1 or Service Pack 2
- Microsoft Project 2000 Service Release 1
- Microsoft Project 2002 Service Pack 1
- Microsoft Visio 2002 Service Pack 2
- 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/ms06-062.mspx>