



**eSecurity Advisory**  
**July 2007 MICROSOFT SECURITY BULLETIN RELEASE**

The purpose of this update is to provide you with a summary of Microsoft's July 2007 Security Bulletin releases.

**NEW BULLETINS**

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

MAXIMUM SEVERITY	BULLETIN NUMBER	PRODUCTS AFFECTED	IMPACT
<b>Critical</b>	MS07-036	All currently supported versions of Microsoft Office	Remote Code Execution
<b>Important</b>	MS07-037	Publisher 2007	Remote Code Execution
<b>Moderate</b>	MS07-038	Windows Vista	Information Disclosure
<b>Critical</b>	MS07-039	Windows 2000 servers, Windows Server 2003	Remote Code Execution
<b>Critical</b>	MS07-040	.NET Framework 1.0, 1.1, 2.0	Remote Code Execution
<b>Important</b>	MS07-041	Windows XP SP2 with IIS 5.1 installed	Remote Code Execution

**RE-RELEASED BULLETINS**

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

**MS06-078:** Vulnerability in Windows Media Format Could Allow Remote Code Execution (923689)

- The security update for Windows Media Player 6.4 (KB925398) did not correctly install on Windows Server 2003 Service Pack 2. A revised security update is now available to install on Windows Server 2003 Service Pack 2 (KB925398).
- No changes have been made to the files in the security update. This is a package change only to install on Windows Server 2003 Service Pack 2.
- Microsoft recommends that customers apply the update immediately. No action is required on systems where the security update has been successfully installed.
- Known issues documented in Microsoft Knowledge Base Article 933065 and Microsoft Knowledge Base Article 933066 are resolved. No action is required on systems where the security update has been successfully installed.
- Customers who did experience this known issue and did not install this security update will be reoffered the security update included with this security bulletin

More Information on **MS06-078** - Vulnerability in Windows Media Format Could Allow Remote Code Execution (923689): <http://www.microsoft.com/technet/security/bulletin/MS06-078.mspx>

**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, 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-Jul.msp>.

---

**TechNet Webcast:**

**Information about Microsoft's May Security Bulletin Release**

Microsoft will be discussing today's bulletin during their regularly scheduled July 2007 TechNet Security Bulletin webcast. This month, the webcast will be held Wednesday, July 11, 2007 at 11:00 AM (GMT-08:00) PT. You can register for it here:

<http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?culture=en-US&EventID=1032343783>.

**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=1032343783>.

---

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

**Technical Details**

**MS07-036**

**Title:** Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (936542)

**Summary:**

This critical update resolves one publicly disclosed vulnerability and two privately reported vulnerabilities in addition to other security issues identified during the course of the investigation. These vulnerabilities could allow remote code execution if a user opens a specially crafted Excel file. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

**Affected Software:**

- Microsoft Office

- Microsoft Excel

**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/MS07-036.aspx>

---

#### MS07-037

**Title:** Vulnerability in Microsoft Office Publisher Could Allow Remote Code Execution (936548)

**Summary:**

This important security update resolves one publicly disclosed vulnerability. This vulnerability could allow remote code execution if a user viewed a specially crafted Microsoft Office Publisher file. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. User interaction is required to exploit this vulnerability.

**Affected Software:**

- Microsoft Office
- Microsoft Publisher

**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/MS07-037.aspx>

---

#### MS07-038

**Title:** Vulnerability in Windows Vista Firewall Could Allow Information Disclosure (935807)

**Summary:**

This moderate security update resolves a privately reported vulnerability. This vulnerability could allow incoming unsolicited network traffic to access a network interface. An attacker could potentially gather information about the affected host.

**Affected Software:**

- Windows Vista

**Impact of Vulnerability:** Information Disclosure

**Maximum Severity Rating:** **Moderate**

**More information on this vulnerability is available at:**

<http://www.microsoft.com/technet/security/bulletin/MS07-038.aspx>

**MS07-039**

**Title:** Vulnerability in Windows Active Directory Could Allow Remote Code Execution (926122)

**Summary:**

This critical security update resolves a privately reported vulnerability in implementations of Active Directory on Windows 2000 Server and Windows Server 2003 that could allow remote code execution or a denial of service condition. Attacks attempting to exploit this vulnerability would most likely result in a denial of service condition. However remote code execution could be possible. On Windows Server 2003 an attacker must have valid logon credentials to exploit this vulnerability. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts.

**Affected Software:**

- Microsoft Windows 2000 Service Pack 4
- Windows Server 2003 Service Pack 1
- Windows Server 2003 Service Pack 2
- Windows Server 2003 with SP1 for Itanium-based Systems
- Windows Server 2003 with SP2 for Itanium-based Systems
- Windows Server 2003 x64 Edition
- 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/MS07-039.msp>

---

**MS07-040**

**Title:** Vulnerabilities in .NET Framework Could Allow Remote Code Execution (931212)

**Summary:**

This update resolves three privately reported vulnerabilities. Two of these vulnerabilities could allow remote code execution on client systems with .NET Framework installed, and one could allow information disclosure on Web servers running ASP.NET. In all remote code execution cases, users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

**Affected Software:**

- .NET Framework 1.0
- .NET Framework 1.1
- .NET Framework 2.0

**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/MS07-040.mspx>

---

#### **MS07-041**

**Title:** Vulnerability in Microsoft Internet Information Services Could Allow Remote Code Execution (939373)

**Summary:**

This important security update resolves a privately reported vulnerability. This vulnerability could allow remote code execution if an attacker sent specially crafted URL requests to a Web page hosted by Internet Information Services (IIS) 5.1 on Windows XP Professional Service Pack 2. IIS 5.1 is not part of a default install of Windows XP Professional Service Pack 2. An attacker who successfully exploited this vulnerability could take complete control of the affected system.

**Affected Software:**

- Windows XP Professional 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/MS07-041.mspx>

---

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