

# Neues Microsoft Sicherheits-Bulletin für September – BITTTE BEACHTEN und UPDATES EINSPIELEN

---

*Source:*

<http://www.tech-archive.net/Archive/German/microsoft.public.de.german.visio/2006-09/msg00032.html>

---

- *From:* "Senaj Lelic [DE MVP Visio]" <[Thanks@xxxxxxxxxxxxxxxxxxx](mailto:Thanks@xxxxxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 13 Sep 2006 14:28:43 +0200
- 

\*\*\*\*\*

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

=====

New Security Bulletins for September 2006

=====

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

MAXIMUM SEVERITY BULLETIN NUMBER PRODUCTS AFFECTED IMPACT

Important MS06-052 Windows Remote  
Code Execution

Moderate MS06-053 Windows  
Information Disclosure

Critical MS06-054 Office Remote  
Code Execution

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

.. <http://www.microsoft.com/technet/security/bulletin/ms06-sep.msp>

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

=====

Re-released Security Bulletins

=====

In addition, Microsoft is re-releasing the following security bulletins:

MAXIMUM SEVERITY BULLETIN NUMBER PRODUCTS AFFECTED IMPACT

Critical MS06-040 Windows  
Remote Code Execution

Critical MS06-042 Windows  
Remote Code Execution

Information on this re-released bulletin may be found at the following page:

Windows <http://www.microsoft.com/technet/security/Bulletin/MS06-040.msp>

Windows <http://www.microsoft.com/technet/security/Bulletin/MS06-042.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>

=====

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/or WSUS:

KB NUMBER TITLE Available via:

922582 Update for Windows MU, WU

920872 Update for Windows XP MU, WU

912580 Outlook 2003 Junk E-mail Filter MU

=====

TechNet Webcast: Information about Microsoft September 2006 Security Bulletins

=====

Wednesday, September 13, 2006 11:00 AM Pacific Time (US & Canada)

The on-demand version of the Webcast will be available 24 hours after the live Webcast at:

<http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?EventID=1032305653&EventCategory=4&culture=en>

=====

Security Bulletin Details

=====

MS06-052

Title: Vulnerability in Pragmatic General Multicast (PGM) Could Allow Remote Code Execution (919007)

Affected Software:

.. Microsoft Windows XP Service Pack 1 and 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

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: Important

Restart required: Yes

Update can be uninstalled: Yes

More information on this vulnerability is available at:

<http://www.microsoft.com/technet/security/bulletin/MS06-052.msp>

\*\*\*\*\*

MS06-053

Title: Vulnerability in Indexing Service Could Allow Cross-Site Scripting (920685)

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

Affected Components:

.. Indexing Service

Impact of Vulnerability: Information Disclosure

Maximum Severity Rating: Moderate

Restart required: No

Update can be uninstalled: Yes

More information on this vulnerability is available at:

<http://www.microsoft.com/technet/security/bulletin/MS06-053.msp>

\*\*\*\*\*

MS06-054

Neues Microsoft Sicherheits-Bulletin für September – BITTTE BEACHTEN und UPDATES EINSPIELEN

Title: Vulnerability in Microsoft Publisher Could Allow Remote Code Execution (910729)

Affected Software:

- .. Microsoft Office 2000 Service Pack 3 – (KB894540)
- .. Office Publisher 2000
- .. Microsoft Office XP Service Pack 3 – (KB894541)
- .. Office Publisher 2002
- .. Microsoft Office 2003 Service Pack 1 and Service Pack 2 – (KB894542)
- .. Office Publisher 2003

Affected Components:

- .. Publisher

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: Critical

Restart required: Yes

Update can be uninstalled: No

More information on this vulnerability is available at:  
<http://www.microsoft.com/technet/security/bulletin/MS06-054.mspx>

\*\*\*\*\*

Re-Release Information

MS06-040

Title: Vulnerability in Server Service Could Allow Remote Code Execution (921883)

Affected Software:

- .. Microsoft Windows 2000 Service Pack 4
- .. Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2

Neues Microsoft Sicherheits-Bulletin für September – BITTTE BEACHTEN und UPDATES EINSPIELEN

Neues Microsoft Sicherheits-Bulletin für September – BITTTE BEACHTEN und UPDATES EINSPIELEN

.. 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

Reason for Re-release: This update resolves a privately disclosed vulnerability as well as additional issues discovered through internal investigations.

An attacker who successfully exploited the vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

More information on this re-released bulletin is available at:  
<http://www.microsoft.com/technet/security/bulletin/MS06-040.mspx>

\*\*\*\*\*

MS06-042

Title: Cumulative Security Update for Internet Explorer (918899)

Affected Software (re-release only):

.. 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

Affected Components (re-release only):

.. 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 or on Microsoft Windows XP Service Pack 1

Neues Microsoft Sicherheits-Bulletin für September – BITTTE BEACHTEN und UPDATES EINSPIELEN

Neues Microsoft Sicherheits-Bulletin für September – BITTTE BEACHTEN und UPDATES EINSPIELEN

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

Reason for Re-release: On August 24, 2006 this Security Bulletin and the Internet Explorer 6 Service Pack 1 security updates were updated to address an issue documented in Microsoft Knowledge Base Article 923762. This issue may lead to an additional buffer overrun condition only affecting Internet Explorer 6 Service Pack 1 customers that have applied the original version of that update released August 8th, 2006. The security issue is documented in the Vulnerability Details section as Long URL Buffer Overflow – CVE-2006-3869. Internet Explorer 6 Service Pack 1 Customers should apply the new update immediately. Microsoft Knowledge Base Article 918899 documents this and any other currently known issues that customers may experience when they install this security update. The article also documents recommended solutions for these issues. For more information, see Microsoft Knowledge Base Article 918899.

More information on this re-released bulletin is available at:  
<http://www.microsoft.com/technet/security/bulletin/MS06-042.msp>

\*\*\*\*\*

Notes and Disclaimers

Regarding Affected Software listed above and in the Security Bulletins:

.. The software listed in the sections above has been tested to determine whether the versions are affected. Other versions either no longer include security update support or may not be affected. To determine the support life cycle for your product and version, visit the Microsoft Support Lifecycle Web site:  
[http://support.microsoft.com/default.aspx?scid=fh;\[ln\];lifecycle](http://support.microsoft.com/default.aspx?scid=fh;[ln];lifecycle)

.. Security updates for Microsoft Windows Server 2003, Windows Server 2003 Service Pack 1, and Windows Server 2003 x64 Edition also apply to Windows Server 2003 R2.

Regarding information consistency:

Neues Microsoft Sicherheits-Bulletin für September – BITTTE BEACHTEN und UPDATES EINSPIELEN

.. We strive to provide you with accurate information in static (this mail) and dynamic (web-based) content. Security Bulletins posted to the web are occasionally updated to reflect late-breaking information. If this results in an inconsistency between the information here and the information in the web-based security bulletin, the information in the web-based security bulletin is authoritative.

\*\*\*\*\*

If you have any questions regarding this alert please contact your Technical Account Manager or Application Development Consultant.

Thank you,

Microsoft PSS Security Team

.