

Neue Sicherheits-Bulletins – KRITISCHE UPDATES – Bitte beachten

Source:

<http://www.tech-archive.net/Archive/German/microsoft.public.de.german.visio/2007-09/msg00026.html>

- *From:* "Senaj Lelic [DE MVP Visio]" <visio@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 12 Sep 2007 15:16:36 +0200
-

Hallo,

anbei das Bulletin

--

Mit freundlichen Grüßen/ with kind regards
Senaj Lelic
DE MVP Visio

Bulletin Anfang.

=====
New Security Bulletins
=====

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

Bulletin Number: MS07-051
Maximum Severity: Critical
Affected Products: Microsoft Windows 2000
Impact: Remote Code Execution

Bulletin Number: MS07-052
Maximum Severity: Important
Affected Products: Microsoft Visual Studio
Impact: Remote Code Execution

Bulletin Number: MS07-053
Maximum Severity: Important
Affected Products: Windows Services for UNIX, Subsystem for UNIX-based Applications
Impact: Elevation of Privilege

Neue Sicherheits-Bulletins – KRITISCHE UPDATES – Bitte beachten

Bulletin Number: MS07-054
Maximum Severity: Important
Affected Products: MSN Messenger, Windows Live Messenger
Impact: Remote Code Execution

Summaries for these new bulletins may be found at the following page:
<http://www.microsoft.com/technet/security/bulletin/ms07-sep.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
=====

High priority non-security updates Microsoft releases to be available on Microsoft Update (MU), Windows Update (WU) or Windows Server Update Services (WSUS) will be detailed in the following KB Article: <http://support.microsoft.com/?id=894199>

=====
TechNet Webcast
=====

Microsoft will host a Webcast to address customer questions on these bulletins:
Title: Information about Microsoft September Security Bulletins (Level 200)
Date: Wednesday, September 12, 2007 11:00 AM Pacific Time (US & Canada)
URL: <http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?culture=en-US&EventID=1032344690>
Replay: Available 24 hours after webcast – same URL

=====
New Security Bulletin Technical Details
=====

In the following tables of affected and non-affected software, software editions that are not listed are past their support lifecycle. To determine the support lifecycle for your product and edition, visit Microsoft Support Lifecycle: <http://support.microsoft.com/lifecycle/>

=====
Microsoft Security Bulletin MS07-051
=====

Bulletin Title: Vulnerability in Microsoft Agent Could Allow Remote Code Execution (938827)

Executive Summary: This critical security update resolves a privately reported vulnerability. A remote code execution vulnerability exists in Microsoft Agent in the way that it handles certain specially crafted URLs. The vulnerability could allow an attacker to remotely execute code on the affected system. Users whose

Neue Sicherheits-Bulletins – KRITISCHE UPDATES – Bitte beachten

accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Maximum Severity Rating: Critical

Impact of Vulnerability: Remote Code Execution

Detection: Microsoft Baseline Security Analyzer can detect whether your computer system requires this update.

Affected Software: Windows. For more information, see the Affected Software and Download Locations section of the bulletin at the link below.

Restart Requirement: You must restart your system after you apply this security update.

Removal Information: Use Add or Remove Programs tool in Control Panel or the Spuninst.exe utility.

Full Details: <http://www.microsoft.com/technet/security/bulletin/MS07-051.msp>

=====

Microsoft Security Bulletin MS07-052

=====

Bulletin Title: Vulnerability in Crystal Reports for Visual Studio Could Allow Remote Code Execution (941522)

Executive Summary: This important security update resolves a publicly disclosed vulnerability. This vulnerability could allow remote code execution if a user opens a specially crafted RPT 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.

Maximum Severity Rating: Important

Impact of Vulnerability: Remote Code Execution

Detection: Microsoft Baseline Security Analyzer and Enterprise Update Scan Tool can detect whether your computer system requires this update.

Affected Software: Visual Studio. For more information, see the Affected Software and Download Locations section of the bulletin at the link below.

Restart Requirement: In some cases, this update does not require a restart. If the required files are being used, this update will require a restart. If this behavior occurs, a message appears that advises you to restart. 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: Use Add or Remove Program tool in Control Panel.

Full Details: <http://www.microsoft.com/technet/security/bulletin/MS07-052.msp>

=====

Neue Sicherheits-Bulletins – KRITISCHE UPDATES – Bitte beachten

Microsoft Security Bulletin MS07-053

=====
Bulletin Title: Vulnerability in Windows Services for UNIX Could Allow Elevation of Privilege (939778)

Executive Summary: This important security update resolves one publicly reported vulnerability. A vulnerability exists in Windows Services for UNIX 3.0, Windows Services for UNIX 3.5, and Subsystem for UNIX-based Applications where running certain setuid binary files could allow an attacker to gain elevation of privilege.

Maximum Severity Rating: Important

Impact of Vulnerability: Elevation of Privilege

Detection: Microsoft Baseline Security Analyzer and Enterprise Update Scan Tool can detect whether your computer system requires this update.

Affected Software: Windows Services for UNIX, Subsystem for UNIX-based Applications. For more information, see the Affected Software and Download Locations section of the bulletin at the link below.

Restart Requirement: The update will require a restart.

Removal Information: Varies depending on which component is installed. For more details see the "Security Update Deployment" section within the bulletin at the link below.

Full Details: <http://www.microsoft.com/technet/security/bulletin/MS07-053.msp>

=====
Microsoft Security Bulletin MS07-054

=====
Bulletin Title: Vulnerability in MSN Messenger and Windows Live Messenger could allow Remote Code Execution (942099)

Executive Summary: This security update resolves a publicly disclosed vulnerability in MSN Messenger and Windows Live Messenger. The vulnerability could allow remote code execution when a user accepts a video chat invitation from an attacker. An attacker who successfully exploited this vulnerability could take complete control of the affected system. 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.

Maximum Severity Rating: Important

Impact of Vulnerability: Remote Code Execution

Detection: These products provide built-in mechanisms for automatic detection and deployment of updates.

Affected Software: MSN Messenger, Windows Live Messenger. For more information, see the Affected Software and Download Locations section of the bulletin at the link below.

Restart Requirement: You may need to restart your system after upgrading if, during the upgrade, you have users with multiple MSN Messenger or Windows Live Messenger sessions active on the system.

Removal Information: Use Add or Remove Programs tool in Control Panel.

Neue Sicherheits-Bulletins – KRITISCHE UPDATES – Bitte beachten

Neue Sicherheits-Bulletins – KRITISCHE UPDATES – Bitte beachten

Full Details: <http://www.microsoft.com/technet/security/bulletin/MS07-054.msp>

=====

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

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

Thank you,

Microsoft CSS Security Team

.