

# Neuer Security Alert 11. Mai 2004

**Source:**

<http://www.tech-archive.net/Archive/German/Security/microsoft.public.de.security.heimanwender/2004-05/0428.htm>

---

**From:** Evelyn Ruf \ (MS\ ) ([evelynr\\_at\\_online.microsoft.com](mailto:evelynr_at_online.microsoft.com))

**Date:** 05/11/04

Date: Tue, 11 May 2004 19:30:06 +0200

Folgender Microsoft Security Alert ist gerade erschienen:

**IMPORTANT PRODUCT VULNERABILITY ALERT – MAY 2004  
SECURITY BULLETIN RELEASE**

Today, 11 May 2004 Microsoft is releasing one security update

for a newly discovered vulnerability in Microsoft Windows.

– One Microsoft Security Bulletins affecting Microsoft Windows

with a maximum severity of Important, MS04–015.

Summaries for these new bulletins may be found at the following

page:

– Microsoft Windows

<http://www.microsoft.com/technet/security/bulletin/winmay04.mspx>

In addition, Microsoft is re-releasing updates for Microsoft

Windows.

Information on these re-released bulletins may be found at the following pages:

– <http://www.microsoft.com/technet/security/Bulletin/MS04-014.mspx>

– <http://www.microsoft.com/technet/security/Bulletin/MS01-052.mspx>

Customers are advised to review the information in the bulletins, test

and deploy the updates immediately in their environments, if applicable.

Microsoft will host a webcast tomorrow to address customer questions on

these bulletins. For more information on this webcast please see below:

- Information about Microsoft's May Security Bulletins
- 5/12/2004 10:00 AM – 5/12/2004 11:00 AM
- Language: English–American
- Live Meeting Webcast – (GMT –08:00) Pacific Time
- <http://go.microsoft.com/fwlink/?LinkId=27513>

The on–demand version of the webcast will be available 24 hours after the live webcast at:

- <http://go.microsoft.com/fwlink/?LinkId=27513>

\*\*\*\*\*

#### TECHNICAL DETAILS

MS04–015

Title: Vulnerability in Help and Support Center Could Allow Remote Code Execution (840374)

Affected Software:

- Microsoft Windows XP and Microsoft Windows XP Service Pack 1
- Microsoft Windows XP 64–Bit Edition Service Pack 1
- Microsoft Windows XP 64–Bit Edition Version 2003
- Microsoft Windows ServerT 2003
- Microsoft Windows Server 2003 64–Bit Edition

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: Important

Restart required: In some cases, this update does not require a restart.

The installer stops the needed services, applies the update, and then restarts the services. However, if the needed services cannot be stopped

for any reason or if required files are in use, this update will require

a restart. If this occurs, a message is displayed that advises you to restart.

Update can be uninstalled: Yes

More information on this vulnerability is available at:

<http://www.microsoft.com/technet/security/bulletin/MS04-015.msp>

\*\*\*\*\*

MS04-014

Title: Vulnerability in the Microsoft Jet Database Engine Could Allow

Code Execution

Affected Software:

- Microsoft Windows NT Workstation 4.0 Service Pack 6a
- Microsoft Windows NT Server 4.0 Service Pack 6a
- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
- Microsoft Windows 2000 Service Pack 2
- Microsoft Windows 2000 Service Pack 3
- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP
- Microsoft Windows XP Service Pack 1
- Microsoft Windows XP 64-Bit Edition Service Pack 1
- Microsoft Windows XP 64-Bit Edition Version 2003
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 64-Bit Edition
- Microsoft Windows 98 – Please review the FAQ section of the bulletin

for details about this operating system.

– Microsoft Windows 98 Second Edition (SE) – Please review the FAQ section

of the bulletin for details about this operating system.

– Microsoft Windows Millennium Edition (ME) – Please review the FAQ section

of the bulletin for details about this operating system.

Affected Components:

– Microsoft Jet Database Engine version 4.0

Reason for Re-issue: Microsoft updated this bulletin on May 11, 2004 to

advise on the availability of a revised version of the security update for

non-English versions of Windows XP (as opposed to Windows XP Service Pack 1).

The original update does address the vulnerability in Windows XP for all supported

languages; however, the original update was not fully localized. Specifically,

optional Jet error strings were only being offered in English on Windows XP.

This issue does not affect other operating systems. If you have previously

applied the security update for other operating systems, including Windows

XP Service Pack 1, you need not take any additional action.

If you have previously applied the security update for non-English versions

of Windows XP (as opposed to Windows XP Service Pack 1), you need not take

any additional action as you are already protected from this vulnerability.

However, if you want to have the Jet optional text error information in

the same language as your Windows XP installation, you will need to remove

the original security update MS04-014 (837001) following the Removal

Information procedure located in this document and install the revised

version. Once 837001 is uninstalled, revisiting Windows Update will result

in the revised MS04-014 security update for Windows XP being re-offered

with the correct, localized, optional text error strings.

More information on this re-issued bulletin is available at:

<http://www.microsoft.com/technet/security/bulletin/MS04-014.msp>

\*\*\*\*\*

MS01-052

Title: Invalid RDP Data can Cause Terminal Service Failure

Affected Software:

- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
- Microsoft Windows 2000 Service Pack 2

Reason for Re-issue: Microsoft updated this bulletin on May 11, 2004

to advise on the availability of a revised version of the Windows NT Server 4.0 Terminal Server Edition security update.

Customers need to install the revised update even if they installed the prior version. This issue does not affect other operating systems. If you have previously applied the security updates for other operating systems, this revised update does not need to be installed.

--

Gruss

Evelyn Ruf

Microsoft Deutschland

(Microsoft kann für die Richtigkeit und Vollständigkeit der Inhalte in dieser Newsgroup keine Haftung übernehmen.)