

MajorRev: v2.0 Microsoft Security Bulletin MS04-014 – Vulnerability in the Microsoft Jet Database Engine Could Allow Code Execution (837001)

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-06/0044.html>

From: Russ Cooper (*Russ.Cooper_at_TRUSECURE.CA*)

Date: 06/15/04

Date: Tue, 15 Jun 2004 17:36:00 -0400
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Microsoft Security Bulletin MS04-014:
Vulnerability in the Microsoft Jet Database Engine Could Allow Code
Execution (837001)

Bulletin URL:

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

Reason for Revision: Microsoft has released a revised version of the
Windows XP security update that contains the correctly localized
optional Jet error strings

Version Number: 2.0

Issued Date: Tuesday, April 13, 2004

Revision Date: Tuesday, May 11, 2004

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: Important

Patch(es) Replaced: None

Caveats: None

Executive Summary:

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.

The following files, on non-English systems only, were updated as part of this update: mswstr10.dll and msjint40.dll. You may see other files with new Date and Time information from the original release – these files remain unchanged, only the 2 files above have been updated.

A buffer overrun vulnerability exists in the Microsoft Jet Database Engine (Jet) that could allow remote code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges.

Tested Software:

Affected Software:

- * Microsoft Windows NT. Workstation 4.0 Service Pack 6a
<<http://tinyurl.com/ysd4d>>
- * Microsoft Windows NT Server 4.0 Service Pack 6a
<<http://tinyurl.com/ysd4d>>
- * Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
<<http://tinyurl.com/ysd4d>>
- * Microsoft Windows 2000 Service Pack 2, Microsoft Windows 2000 Service Pack 3, and Microsoft Windows 2000 Service Pack 4
<<http://tinyurl.com/2ht7z>>
- * Microsoft Windows XP and Microsoft Windows XP Service Pack 1
<<http://tinyurl.com/2lhmb>>
- * Microsoft Windows XP 64-Bit Edition Service Pack 1
<<http://tinyurl.com/2ojxe>>
- * Microsoft Windows XP 64-Bit Edition Version 2003
<<http://tinyurl.com/29wzu>>
- * Microsoft Windows Server(tm) 2003
<<http://tinyurl.com/365ev>>
- * Microsoft Windows Server 2003 64-Bit Edition
<<http://tinyurl.com/29wzu>>
- * Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME) – Review the FAQ section of this bulletin for details about these operating systems.

Affected Components:

* Microsoft Jet Database Engine version 4.0

Technical Description:

* Jet Vulnerability – CAN-2004-0197: A buffer overrun vulnerability exists in the Microsoft Jet Database Engine (Jet) that could allow remote code execution on an affected system. An attacker could exploit the vulnerability by creating a specially crafted database query and sending it through an application that is using Jet on an affected system. An attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges.

Revision History:

* v1.0 – 4/13/2004: Bulletin published
* v2.0 – 5/11/2004: Microsoft has released a revised version of the Windows XP security update that contains the correctly localized optional Jet error strings

This email is sent to NTBugtraq automagically as a service to my subscribers. (v4.01.1625.28734)

Cheers,
Russ – Senior Scientist – TruSecure Corporation/NTBugtraq Editor

NTBugtraq Editor's Note:

Want to reply to the person who sent this message? This list is configured such that just hitting reply is going to result in the message coming to the list, not to the individual who sent the message. This was done to help reduce the number of Out of Office messages posters received. So if you want to send a reply just to the poster, you'll have to copy their email address out of the message and place it in your TO: field.