

# FW: MinorRev: Microsoft Security Bulletin MS05-031 – Vulnerability in Step-by-Step Interactive Training Could Allow Remote Code Execution (898458)

**Source:** <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2005-06/0024.html>

---

**From:** Cooper, Russ (*russ.cooper\_at\_CYBERTRUST.COM*)

**Date:** 06/15/05

Date: Wed, 15 Jun 2005 17:00:38 -0400  
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Microsoft Security Bulletin MS05-031:  
Vulnerability in Step-by-Step Interactive Training Could Allow Remote  
Code Execution (898458)

Bulletin URL:

<<http://www.microsoft.com/technet/security/Bulletin/MS05-031.mspx>>

Reason for Revision: Bulletin 'Acknowledgments' section revised with  
additional details.

Version Number: 1.1

Issued Date: Tuesday, June 14, 2005

Revision Date: Wednesday, June 15, 2005

Impact of Vulnerability: Remote Code Execution Maximum Severity Rating:

Important

Patch(es) Replaced: None

Caveats: None

Tested Software:

Affected Software:

-----  
\* Microsoft Windows 2000 Service Pack 3 and Microsoft Windows 2000  
Service Pack 4

\* Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service  
Pack 2

\* Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium)

\* Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium)

\* 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

\* Microsoft Windows Server 2003 x64 Edition

\* 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.

\* Step-by-Step Interactive Training (All Versions)

Affected Components:

---

\* Step-by-Step Interactive Training

<<http://tinyurl.com/ck8ry>>

\* Step-by-Step Interactive Training when it is running on Itanium-based systems <<http://tinyurl.com/ck8ry>>

\* Step-by-Step Interactive Training when it is running on x64-based systems <<http://tinyurl.com/ck8ry>>

Technical Description:

---

\* Interactive Training Vulnerability – CAN-2005-1212: A remote code execution vulnerability exists in Step-by-Step Interactive Training because of the way that Step-by-Step Interactive Training handles bookmark link files. An attacker could exploit the vulnerability by constructing a malicious bookmark link file that could potentially allow remote code execution if a user visited a malicious Web site or opened a malicious attachment that was provided in an e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, user interaction is required to exploit this vulnerability.

Revision History:

---

\* v1.0 – 6/14/2005: Bulletin published

\* v1.1 – 6/15/2005: Bulletin 'Acknowledgments' section revised with additional details.

This email is sent to NTBugtraq automagically as a service to my subscribers. (v4.01.1975.38886)

Cheers,

Russ Cooper – Senior Scientist – Cybertrust/NTBugtraq Editor

--

NTBugtraq Editor's Note:

Most viruses these days use spoofed email addresses. As such, using an Anti-Virus product which a

--