

# Alert: Microsoft Security Bulletin MS05-036 – Vulnerability in Microsoft Color Management Module Could Allow Remote Code Execution (901214)

**Source:** <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2005-07/0003.html>

---

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

**Date:** 07/12/05

Date: Tue, 12 Jul 2005 13:47:05 -0400  
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Microsoft Security Bulletin MS05-036:  
Vulnerability in Microsoft Color Management Module Could Allow Remote  
Code Execution (901214)

Bulletin URL:

<<http://www.microsoft.com/technet/security/Bulletin/MS05-036.msp>>

Version Number: 1.0

Issued Date: Tuesday, July 12, 2005

Impact of Vulnerability: Remote Code Execution Maximum Severity Rating:

Critical

Patch(es) Replaced: None

Caveats: None

Tested Software:

Affected Software:

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

<<http://tinyurl.com/dvgc4>>

\* Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service  
Pack 2 <<http://tinyurl.com/77xdh>>

\* Microsoft Windows XP Professional x64 Edition

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

\* Microsoft Windows Server 2003 and Microsoft Windows Server 2003  
Service Pack 1 <<http://tinyurl.com/8wc5j>>

\* Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft  
Windows Server 2003 with SP1 for Itanium-based Systems

<<http://tinyurl.com/ch2mn>>

\* 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. Windows Server 2003 (all

Alert: Microsoft Security Bulletin MS05-036 – Vulnerability in Microsoft Color Management Module Could Allow Remote Co

versions) <<http://tinyurl.com/8369z>>

Technical Description:

-----  
\* Color Management Module Vulnerability – CAN-2005-1219: A remote code execution vulnerability exists in the Microsoft Color Management Module because of the way that it handles ICC profile format tag validation. An attacker could exploit the vulnerability by constructing a malicious image file that could potentially allow remote code execution if a user visited a malicious Web site or viewed a malicious e-mail message. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

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

Cheers,  
Russ Cooper – Cybertrust/NTBugtraq Editor

--

NTBugtraq Editor's Note:

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

--

Alert: Microsoft Security Bulletin MS05-036 – Vulnerability in Microsoft Color Management Module Could Al