

# [NT] Vulnerability in Microsoft Color Management Module Could Allow Remote Code Execution (MS05-036)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-07/0034.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 07/13/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 13 Jul 2005 21:14:58 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

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

## SUMMARY

The Microsoft Color Management Module allows the operating system to provide consistent color mappings between different devices and applications. In addition, this module is used to transform colors from one color space to another (for example, RGB to CMYK). For additional information about color management, visit the following <http://www.microsoft.com/whdc/device/display/color/icmwp.msp> Web site.

The International Color Consortium is an organization whose purpose is to provide a standard by which vendors can implement color management to ensure cross vendor compatibility. For additional information about the International Color Consortium (ICC), visit the following <http://www.color.org> Web site

A remote code execution vulnerability exists in the Microsoft Color Management Module because of the way that it handles ICC profile format tag validation.

## DETAILS

[NT] Vulnerability in Microsoft Color Management Module Could Allow Remote Code Execution (MS05-036)

Vulnerable Systems:

- \* Microsoft Windows 2000 Service Pack 4

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=FA8D18EC-EBF4-4C49-AFA0-F6A215B3624F>>

Download the update

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C5BCF2DB-ADCE-42BD-ABEE-1380F258158B>>

Download the update

- \* Microsoft Windows XP Professional x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C54BB4BA-FB9B-4615-9BBE-EF6D3885467D>>

Download the update

- \* Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=44275ECB-2E79-4CE8-8269-E81219CE8F6C>>

Download the update

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

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=97A903BC-90E1-4FDE-9487-1816C4A647BB>>

Download the update

- \* Microsoft Windows Server 2003 x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=52167B42-8790-4965-9F26-DC5EDC2E84F8>>

Download the update

- \* Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1219>>

CAN-2005-1219

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

Mitigating Factors for Color Management Module Vulnerability – CAN-2005-1219:

- \* In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to exploit this vulnerability. An attacker would have no way to force users to visit a malicious Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's Web site.

- \* An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. 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.

FAQ for Color Management Module Vulnerability – CAN-2005-1219:

What is the scope of the vulnerability?

This is a remote code execution vulnerability. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. 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.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could take complete control of the affected system.

Who could exploit the vulnerability?

Any anonymous user who could deliver a specially crafted message to the affected system could try to exploit this vulnerability.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted malicious image and persuading a user to view the image by viewing a local file, by previewing an e-mail message containing the malicious image, or by opening an e-mail attachment that contains a malicious image. These actions could then cause the affected system to execute code.

What systems are primarily at risk from the vulnerability?

Workstations and terminal servers are primarily at risk. Servers could be at more risk if users who do not have sufficient administrative permissions are given the ability to log on to servers and to run programs. However, best practices strongly discourage allowing this.

Are Windows 98, Windows 98 Second Edition or Windows Millennium Edition critically affected by this vulnerability?

No. Although Windows 98, Windows 98 Second Edition, and Windows Millennium Edition do contain the affected component, the vulnerability is not critical because it is not exploitable through critical attack vectors. Additionally, the currently known attack vectors require user interaction to exploit this vulnerability. For more information about severity ratings, visit the following Web site.

What does the update do?

The update removes the vulnerability by modifying the way that the Microsoft Color Management Module validates ICC profile information before passing the data to the allocated buffer.

#### ADDITIONAL INFORMATION

The information has been provided by Microsoft.

The original article can be found at:

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

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

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.