

# [NT] Windows FTP Client Allows File Transfer Location Tampering (MS05-044)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-10/0040.html>

---

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

**Date:** 10/12/05

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

Date: 12 Oct 2005 09:38:11 +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>

-----

Windows FTP Client Allows File Transfer Location Tampering (MS05-044)

---

## SUMMARY

A tampering vulnerability exists in the Windows FTP client. This vulnerability could allow an attacker to modify the intended destination location for a file transfer, when a client has manually chosen to transfer a file by using FTP. This vulnerability could allow the attacker to write the file to any file system that is located on an affected system.

## DETAILS

### Affected Software:

\* Microsoft Windows XP Service Pack 1 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=351C63A3-AB62-418D-8678-3AF791D73A29>>

Download the update

\* Microsoft Windows Server 2003 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=4940CF64-E1FD-4E88-8980-3106BE03BF12>>

Download the update

\* Microsoft Windows Server 2003 for Itanium-based Systems –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=B715147B-DE2D-4F14-9548-AFF18641D0F3>>

Download the update

## Securiteam: [NT] Windows FTP Client Allows File Transfer Location Tampering (MS05-044)

### Affected Components:

- \* Internet Explorer 6 Service Pack 1 on Microsoft Windows 2000 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=FCEA60E5-9EA8-4216-BA4D-C85054892DBB>>  
Download the update

### Non-Affected Software:

- \* Microsoft Windows 2000 Service Pack 4
- \* Microsoft Windows XP Service Pack 2
- \* Microsoft Windows XP Professional x64 Edition
- \* Microsoft Windows Server 2003 Service Pack 1
- \* Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- \* Microsoft Windows Server 2003 x64 Edition
- \* Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)

### Non-Affected Components:

- \* Internet Explorer 5.01 Service Pack 4 on Microsoft Windows 2000 Service Pack 4

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2126>>  
CAN-2005-2126

### Mitigating Factors for FTP Client Vulnerability:

- \* If an attacker successfully persuades users to visit an FTP server hosting files with specially-crafted file names, the attacker would have no way of forcing files to be transferred. User interaction is required before the file can be transferred to the affected system.

- \* If the malicious FTP transfer tries to overwrite an existing file on the affected system, the user receives an Overwrite File warning message. The file is saved only if the user selects to allow it to save when they receive the warning message.

- \* By default, the Enable Folder View for FTP Sites Internet Explorer setting is disabled on all affected operating system versions. An attacker would only be successful if the user manually enables the Enable Folder View for FTP Sites Internet Explorer setting on the affected system.

### What is the scope of the vulnerability?

This is a tampering vulnerability. This vulnerability could allow an attacker to modify the intended destination location for a file transfer when a client has manually chosen to transfer a file by using FTP.

### What causes the vulnerability?

The Windows FTP client does not properly validate file names that are received from FTP servers.

### What might an attacker use the vulnerability to do?

An attacker who exploited this vulnerability could save files to specific

## Securiteam: [NT] Windows FTP Client Allows File Transfer Location Tampering (MS05-044)

locations on an affected system. These files could allow other attacks. For example, an attacker could save an executable file in the Startup folder. Then, the transferred file would run the next time the user logs on.

Who could exploit the vulnerability?

Anyone who could persuade a user to visit and transfer files from an FTP server that hosts files that have specially-crafted file names.

How could an attacker exploit the vulnerability?

An attacker could exploit this vulnerability by hosting a file on an FTP server that has a specially-crafted file name. The file name must be constructed in such a way that it bypasses the file name validation that the FTP client provides and that it maps to a valid location on the users computer. An attacker must then persuade a user to download this file.

Can the vulnerability be exploited automatically by visiting an FTP server?

No. User interaction is required for the file to be transferred and saved by using FTP.

What systems are primarily at risk from the vulnerability?

The vulnerability requires that a user connect to an FTP server and transfer files from the FTP server. Therefore, any systems where FTP transfers occur frequently, such as workstations, are at the most risk from this vulnerability. Systems that are not typically used to visit FTP servers, such as most server systems, are at a reduced risk.

What does the update do?

The update removes the vulnerability by modifying the way the Windows FTP client validates file names that it receives from FTP servers.

When this security bulletin was issued, had this vulnerability been publicly disclosed?

Yes. This vulnerability has been publicly disclosed. It has been assigned Common Vulnerability and Exposure number CAN-2005-2126

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers. However, examples of proof of concept code had been published when this security bulletin was originally issued.

Does applying this security update help protect customers from the code that has been published publicly that tries to exploit this vulnerability?

Yes. This security update addresses the vulnerability for which proof of concept code has been published.

ADDITIONAL INFORMATION

Securiteam: [NT] Windows FTP Client Allows File Transfer Location Tampering (MS05-044)

The information has been provided by Microsoft Product Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/MS05-044.mspx>>

<http://www.microsoft.com/technet/security/Bulletin/MS05-044.mspx>

=====

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

In order to subscribe to the mailing list, simply forward this email to: 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.