

Re: WU-FTPD, Solaris 8, anon user, chroot() question

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-sun/2001-11/0026.html>

From: Jan-Philip Velders (jp@jpv.xs4all.nl)

Date: 11/16/01

Date: Fri, 16 Nov 2001 22:56:27 +0100 (CET)
From: Jan-Philip Velders <jp@jpv.xs4all.nl>
To: Mansel P Bell <Mansel_P_Bell@raytheon.com>
Subject: Re: WU-FTPD, Solaris 8, anon user, chroot() question
Message-ID: <Pine.LNX.4.05.10111162214420.11715-100000@jp-gp.vsi.nl>

> *Date:* Fri, 16 Nov 2001 12:24:13 -0600
> *From:* Mansel P Bell <Mansel_P_Bell@raytheon.com>
> *Subject:* WU-FTPD, Solaris 8, anon user, chroot() question

> *I am working on a anonymous-only wu-ftp design and
> need some help with logging via syslog from within
> an anonymous user's chroot()ed home directory.*

Ehm... you may need to clarify that the *daemon* itself is chrooted,
and will probably then perform a chroot into the anonymous-ftp space.

> *Configuration info:*
> [...]
> - *Successfully chroot()ed the Solaris 8 syslogd server:*
> --> *running from \$CHROOT/usr/sbin/syslogd*
> --> *logging to \$CHROOT/var/adm/messages*
> - *Successfully chroot()ed the wuftp server:*
> --> *running from \$CHROOT/sbin/in.ftpd*
> --> *getting anon ftp user info from \$CHROOT/etc/passwd*
> --> *anon ftp user home of \$CHROOT/home*
> --> *each anon class has home of \$CHROOT/home/anon{1..N}*
> --> *all syslog() calls from the parent in.ftpd instance*
> *log fine to \$CHROOT/var/adm/messages*

> *Problem:*
> -----
> *Once an anonymous user logs on, a new child process is
> forked, and the user is chroot()ed according to his/her
> anon class, all logging ceases for the child process
> b/c \$CHROOT/home/anon{1..N}/var/run/syslog_door does not
> exist...the dreaded "syslog_door" problem all over again.*
>

SecurityFocus SUN: Re: WU-FTPD, Solaris 8, anon user, chroot()

- > *Does anyone know how to deal with Solaris doors in this*
- > *situation, short of rebuilding a version of syslog.o that*
- > *uses /dev/log instead?*

Ehm... I found something on the wu ftpd mailinglist, albeit for Solaris 2.6 and 7 ...

<http://www.landfield.com/wu-ftp/mail-archive/wu-ftp/1999/May/0027.html>

They specify that the syslog_door is **not** used for logging, but for finding out if a proces is still running (/var/run after all !).

Perhaps you could fiddle with placing some stuff in \$CHROOT/dev ...

On a Solaris 8 E250:

```
bash-2.03: root / $ strings /usr/sbin/syslogd | egrep -i 'dev/[a-z]' | sort | uniq
/dev/console
/dev/log
/dev/sysmsg
bash-2.03: root / $ ls -al /dev/console /dev/sysmsg /dev/log
lrwxrwxrwx 1 root other 30 Feb 10 2001 /dev/console -> ../devices/pseudo/cn@0:console
lrwxrwxrwx 1 root other 27 Feb 10 2001 /dev/log -> ../devices/pseudo/log@0:log
lrwxrwxrwx 1 root other 33 Feb 10 2001 /dev/sysmsg -> ../devices/pseudo/sysmsg@0:sysmsg
bash-2.03: root / $ ls -al /devices/pseudo/cn@0:console
crw--w----- 1 root tty 0, 0 Nov 16 22:00 /devices/pseudo/cn@0:console
bash-2.03: root / $ ls -al /devices/pseudo/log@0:log
crw-r----- 1 root sys 21, 5 Feb 10 2001 /devices/pseudo/log@0:log
bash-2.03: root / $ ls -al /devices/pseudo/sysmsg@0:sysmsg
crw----- 1 root sys 97, 0 Nov 13 14:12 /devices/pseudo/sysmsg@0:sysmsg
bash-2.03: root / $ cat /etc/release
```

Solaris 8 s28_38shwp2 SPARC

Copyright 2000 Sun Microsystems, Inc. All Rights Reserved.

Assembled 21 January 2000

Solaris 8 Maintenance Update 5 applied

- > *Does anyone otherwise have any ideas on how I can circumvent*
- > *this problem in my design?*

I think that your main problem is caused by your wu-ftp daemon process running chroot. I'm guessing your main reason is to confine a remote root-hole risk ?

Perhaps you should look at other ftp servers. Very well known are ProFTPD and BeroFTPD. BeroFTPD has been recommended to me by various people as an excellent choice for anon-ftp... And those people know their security stuff ;)

- > *Any help is sincerely appreciated.*
- > *-Mansel*

Regards,
JP Velders

- **Previous message:** Mansel P Bell: "WU-FTPD, Solaris 8, anon user, chroot() question"
- **In reply to:** Mansel P Bell: "WU-FTPD, Solaris 8, anon user, chroot() question"
- **Messages sorted by:** [date] [thread] [subject] [author] [attachment]