

openssh3.7p1 chroot patch not work on solaris 7

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-09/0299.html>

From: Tom (tom_at_hottestnet.com)

Date: 09/26/03

Date: 25 Sep 2003 18:22:42 -0700

I downloaded the latest openssh-3.7p1 chroot patch from <http://chrootssh.sourceforge.net> and installed it on my Solaris 7 (Sun Sparc 20), but it doesn't work, after I ssh/sftp to it, it closed the connection immediately.

1. I CAN login to a normal user.
2. I CAN do "chroot /export/home/test /bin/sh".
3. But when I tried to ssh/sftp to a chrooted user, I CAN see etc/motd under /export/home/test, but after that I got "Connection closed" immediately.

Here is the debug from "sshd -ddd" for "sftp test@localhost":

```
debug3: mm_auth_password: user authenticated
Accepted password for tom from 192.168.1.1 port 39156 ssh2
Accepted password for tom from 192.168.1.1 port 39156 ssh2
debug1: monitor_child_preauth: test has been authenticated by privileged process
debug3: mm_get_keystate: Waiting for new keys
debug3: mm_request_receive_expect entering: type 24
debug3: mm_request_receive entering
debug3: mm_send_keystate: Sending new keys: 1171c8 11e578
debug3: mm_newkeys_to_blob: converting 1171c8
debug3: mm_newkeys_to_blob: converting 11e578
debug3: mm_send_keystate: New keys have been sent
debug3: mm_send_keystate: Sending compression state
debug3: mm_request_send entering: type 24
debug3: mm_newkeys_from_blob: 116708(123)
debug2: mac_init: found hmac-sha1
debug3: mm_get_keystate: Waiting for second key
debug3: mm_newkeys_from_blob: 116708(123)
debug2: mac_init: found hmac-sha1
debug3: mm_get_keystate: Getting compression state
debug3: mm_get_keystate: Getting Network I/O buffers
debug3: mm_share_sync: Share sync
debug3: mm_share_sync: Share sync end
debug3: mm_send_keystate: Finished sending state
debug2: User child is on pid 17923
debug3: mm_request_receive entering
```

comp.security.ssh: openssh3.7p1 chroot patch not work on solaris 7

```
debug1: permanently_set_uid: 1005/60000
debug2: set_newkeys: mode 0
debug2: set_newkeys: mode 1
debug1: Entering interactive session for SSH2.
debug2: fd 11 setting O_NONBLOCK
debug2: fd 12 setting O_NONBLOCK
debug1: server_init_dispatch_20
debug1: server_input_channel_open: ctype session rchan 0 win 65536 max 32768
debug1: input_session_request
debug1: channel 0: new [server-session]
debug1: session_new: init
debug1: session_new: session 0
debug1: session_open: channel 0
debug1: session_open: session 0: link with channel 0
debug1: server_input_channel_open: confirm session
debug1: server_input_channel_req: channel 0 request subsystem reply 1
debug1: session_by_channel: session 0 channel 0
debug1: session_input_channel_req: session 0 req subsystem
subsystem request for sftp
debug1: subsystem: exec() /usr/local/libexec/sftp-server
debug1: Received SIGCHLD.
debug2: fd 15 setting O_NONBLOCK
debug2: fd 15 is O_NONBLOCK
debug2: notify_done: reading
debug1: session_by_pid: pid 17925
debug1: session_exit_message: session 0 channel 0 pid 17925
debug2: channel 0: request exit-signal
debug1: session_exit_message: release channel 0
debug2: channel 0: write failed
debug2: channel 0: close_write
debug2: channel 0: output open -> closed
debug1: session_close: session 0 pid 17925
debug2: channel 0: read<=0 rfd 15 len 0
debug2: channel 0: read failed
debug2: channel 0: close_read
debug2: channel 0: input open -> drain
debug2: channel 0: ibuf empty
debug2: channel 0: send eof
debug2: channel 0: input drain -> closed
debug2: channel 0: send close
debug3: channel 0: will not send data after close
debug2: channel 0: rcvd close
debug3: channel 0: will not send data after close
debug2: channel 0: is dead
debug2: channel 0: garbage collecting
debug1: channel 0: free: server-session, nchannels 1
debug3: channel 0: status: The following connections are open:
  #0 server-session (t4 r0 i3/0 o3/0 fd 15/15)

debug3: channel 0: close_fds r 15 w 15 e -1
Connection closed by 192.168.1.1
```

comp.security.ssh: openssh3.7p1 chroot patch not work on solaris 7

Closing connection to 192.168.1.1

debug3: mm_request_send entering: type 54

debug3: monitor_read: checking request 54

debug3: mm_answer_term: tearing down sessions

Any idea?

Thanks.