

## Re: FreeBSD Security Advisory: FreeBSD-SA-01:18.bind

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2001-02/0662.html>

---

**From:** Doug Barton ([DougB@gorean.org](mailto:DougB@gorean.org))

**Date:** 02/01/01

Date: Wed, 31 Jan 2001 18:15:50 -0800 (PST)

From: Doug Barton <[DougB@gorean.org](mailto:DougB@gorean.org)>

To: Alfred Perlstein <[bright@wintelcom.net](mailto:bright@wintelcom.net)>

On Wed, 31 Jan 2001, Alfred Perlstein wrote:

> *Since named supports a command line option for chroot as well  
> as user flags (-t) it would be trivial to have it the default.*

Actually, it's not trivial to do the chroot version properly. There are several files, directories, and one device that have to be created in the chroot environment. Also, /etc/ is not a good choice for the chroot, it really should be something like /usr/named, or /usr/local/named since the quantity of zone files could be quite large, and variable in nature.

> *It's pretty much a toss-up between usability and security.*

When done properly (with appropriate compiled-in defaults) the only functionality you lose is the ability to bind new interfaces while named is running. As Matt pointed out, this "feature" is of dubious value at best.

> *I guess this is the final blow for me, and I think we should  
> run bind in a sandbox at this point, I'm just worried about  
> confusing newbies who wish to set it up.*  
>  
> *If anyone has a proposal on doing it by default that doesn't  
> impact ease of use (or if already doesn't impact it) then I'm  
> for it.*

Jeroen and I are kicking around some ideas. I'm thinking of a make.conf variable that will specify the location of the chroot dir. Something like BIND\_CHROOT=/usr/local/named. Questions to be resolved are; location, default to on or off, etc. So far there is pretty good support for at least providing the option to do this in the base, so I think it will happen sometime "soon," depending on how soon the two of us (or someone else) can get to it.

FreeBSD-Security: Re: FreeBSD Security Advisory: FreeBSD-SA-01:18.bind

- > *What I'm worrying about specifically is ndc and other utilities*
- > *basically are unix domain sockets not in the expected place all of*
- > *sudden?*

That's one of the things you compile in. Let's say that you want your chroot to be /usr/local/named. You set DESTRUN in the bind makefile to /usr/local/named/var so named knows where to write it's FIFO when it starts up, and you make that var directory rw for the bind user. QED.

BTW, just running with -u bind -g bind does not constitute "running in a sandbox." It does help to have bind drop privs, but the chroot stuff is what constitutes a true sandbox.

Doug

--

"Pain heals. Chicks dig scars. Glory . . . lasts forever."  
-- Keanu Reeves as Shane Falco in "The Replacements"  
Do YOU Yahoo!?

To Unsubscribe: send mail to [majordomo@FreeBSD.org](mailto:majordomo@FreeBSD.org)  
with "unsubscribe freebsd-security" in the body of the message