

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

*Source:* <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2001-02/0673.html>

---

*From:* Matt Dillon ([dillon@earth.backplane.com](mailto:dillon@earth.backplane.com))

*Date:* 02/01/01

Date: Wed, 31 Jan 2001 23:58:48 -0800 (PST)  
From: Matt Dillon <[dillon@earth.backplane.com](mailto:dillon@earth.backplane.com)>  
To: "Crist J. Clark" <[cjclark@reflexnet.net](mailto:cjclark@reflexnet.net)>

:  
:On Wed, Jan 31, 2001 at 03:27:25PM -0800, Matt Dillon wrote:  
:> :> I think we can easily make it the default.  
:> :  
:> :If it breaks HUP, then not really. :)  
:> :  
:> :I'm not sure how bind handles restarts, but even if it exec(2)s over  
:> :itself it can track the fd open for its socket and shouldn't have to  
:> :rebind it.  
:> :  
:> :You gotta work with what you have. Bind outsmarts itself in a lot  
:> :of places, especially the stupid interface scanning/binding code. The  
:> :last thing I want it to do is hold \*any\* state from the previous  
:> :incarnation across a restart. Frankly, restarting is not a big deal  
:> :even if you have hundreds or thousands of domains. I always restarted  
:> :named at BEST rather than HUP it, because HUPing is simply too  
:> :dangerous when you make random modifications to dozens of primary  
:> :zone files out of thousands.  
:  
:You also loose the cache. Some people may not like that.  
:--  
:Crist J. Clark [cjclark@alum.mit.edu](mailto:cjclark@alum.mit.edu)

Recursive nameservers generally do not need to be HUPd or restarted.  
It's the nameservers handing out primary and secondary zones that  
usually need HUPing/restarting.

Nobody in their right mind runs a primary/secondary zone server  
with any significant number of domains or load in recursive mode.  
Even the smallest ISP with any brains separates the functions out.  
Anyone who does -- well, they get what they deserve, and I guarentee  
you that the fact their cache may have to be reloaded is inconsequential  
relative to all the other fallout.

The plain fact of the matter is that if you want reliable name service, you can't afford even to HUP the recursive nameservers (which take the brunt of your other hosts lookup load and for which there is no easy way to create redundancy in a manner that appears seamless to hosts using said server as a resolver). Even HUPing can result in a few seconds worth of glitches, which in turn can glitch every single host trying to use that server for lookups. This is why you separate functions... DNS servers handing out primary and secondary zones can afford to go offline for minutes, even hours without glitching anyone, as long as there is at least one other NS for the zone(s). Servers handling recursive lookups for hosts can't afford to go offline for even an instant, because the hosts using those servers often take several seconds ON EACH LOOKUP to fall back to a secondary recursive server. If you think specifying multiple recursive servers in `/etc/resolv.conf` will save a heavily loaded host, like a mail box, you will be in for one hellofa surprise when your primary resolver goes down!

Since you typically never have to reload or restart a recursive nameserver that is not primary or secondary for any zones, and since you typically always have to reload or restart a primary zone server (whenever you make a change to a zone)... Well, it should be obvious.

-Matt

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