

Re: [Fwd: cvs commit: ports/dns/bind9 Makefile distinfo ports/dns/bind94 Makefile distinfo ports/dns/bind95 Makefile distinfo]

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2008-07/msg00067.html>

- *From:* Matthew Seaman <m.seaman@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 11 Jul 2008 17:28:11 +0100
-

Alan Clegg wrote:

Jeremy Chadwick wrote:

On Fri, Jul 11, 2008 at 08:54:48AM -0600, Brett Glass wrote:

Is there a way to restrict the ports which BIND selects -- perhaps at the expense of a small amount of entropy -- such that it doesn't try to use UDP ports which are administratively blocked (e.g. ports used by worms, or insecure Microsoft network utilities)? We don't dare turn these port blocks off, or naive users will fall prey to security holes in Microsoft products. But if BIND doesn't know to work around them, lookups will occasionally (and infuriatingly!) fail.

query-source has an argument called "port" which will do what you want. That option **only** affects UDP queries, however; TCP queries are always random.

While query-source allows you to lock down to a single port, you DO NOT WANT TO DO THIS -- if you do, you will be vulnerable to the very thing that the patch made you immune (well, safer) from.

What Brett (and others) need to do is risk the waters with the new beta code (9.4.3b2 and 9.5.1b1) which includes additional "fine-grained"

Re: [Fwd: cvs commit: ports/dns/bind9 Makefile distinfo ports/dns/bind94 Makefile distinfo ports/dns/bind95 Makefile dist

control for the UDP ports to be used.

Please, PLEASE, do not introduce "query-source port XX" into your configurations.

Probably what Brett is looking for are the avoid-v4-udp-ports and avoid-v6-udp-ports options -- these just contain lists of UDP ports to avoid as the source of any DNS traffic. Details are available here (for bind95) <http://www.isc.org/sw/bind/arm95/Bv9ARM.ch06.html#options> but it's the same for all 9.x versions of BIND.

Cheers,

Matthew

Dr Matthew J Seaman MA, D.Phil. 7 Priory Courtyard
Flat 3
PGP: <http://www.infracaninophile.co.uk/pgpkey> Ramsgate
Kent, CT11 9PW

Attachment: signature.asc

Description: OpenPGP digital signature

Re: [Fwd: cvs commit: ports/dns/bind9 Makefile distinfo ports/dns/bind94 Makefile distinfo ports/dns/2bind95