

FreeBSD-Security: Re: /var partition overflow (due to spyware?) in FreeBSD default install

## Re: /var partition overflow (due to spyware?) in FreeBSD default install

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2003-10/0111.html>

---

**From:** Pete Ehlke ([pde\\_at\\_ehlke.net](mailto:pde_at_ehlke.net))

**Date:** 10/27/03

Date: Mon, 27 Oct 2003 06:08:38 -0800

To: [security@freebsd.org](mailto:security@freebsd.org)

On Thu, Oct 23, 2003 at 08:46:46PM -0600, David G. Andersen wrote:

> *Garance A Drosihn just mooded:*  
> > *newsyslog for the past year. I am pretty familiar with it.*  
> >  
> > *What I meant was that in circumstances where "once per hour"*  
> > *is not fast enough, then I do not believe the right solution*  
> > *is to rotate files every five minutes. Just MO.*  
>  
> *the problem is very obviously an excess of messages from bind.*  
> *This bug report should go to the ISC folks. No daemon should*  
> *be spewing out log messages at the \_incredible\_ rate that*  
> *bind does when it decides it doesn't like what it's getting*  
> *in this context. The same bug can be triggered by using a*  
> *forwarding nameserver that bind doesn't like.*

It logs messages at the rate that it sees errors.

> *The immediate question to ask is, "is this fixed in bind9?"*

>

Well, no. The immediate question to ask is "why are you sending bind messages to syslogd in the first place?"

see <http://www.isc.org/products/BIND/docs/config/logging.html> for how to configure bind to do sane logging, including size-based autorotation of log files.

-Pete

---

[freebsd-security@freebsd.org](mailto:freebsd-security@freebsd.org) mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "[freebsd-security-unsubscribe@freebsd.org](mailto:freebsd-security-unsubscribe@freebsd.org)"