Subject: Re: [PATCH] struct file leakage
Posted by Trond Myklebust on Wed, 12 Jul 2006 00:26:02 GMT
View Forum Message <> Reply to Message

On Tue, 2006-07-11 at 16:32 -0700, Andrew Morton wrote:
> Trond Myklebust <trond.myklebust@fys.uio.no> wrote:
> >
> > > > - if (error)
> > > > + if (error) {
> > > > + /* Does someone understand code flow here? Or it is only
> > > > +   * me so stupid? Anathema to whoever designed this non-sense
> > > > +   * with "intent.open".
> > > > +   */
> > > > + if (!IS_ERR(nd->intent.open.file))
> > > > +   release_open_intent(nd);
> > > >   return error;
> > > > + }
> > > >   nd->flags &= ~LOOKUP_PARENT;
> > > >   if (nd->last_type == LAST_BIND)
> > > >   goto ok;
> > > >
> > >
> > > It's good to have some more Alexeycomments in the tree.
> > >
> > > I wonder if we're also needing a path_release() here. And if not, whether
> > > it is still safe to run release_open_intent() against this nameidata?
> > >
> > > Hopefully Trond can recall what's going on in there...
> >
> > The patch looks correct, except that I believe we can skip the IS_ERR()
> > test there: if we're following links then we presumably have not tried
> > to open any files yet, so the call to release_open_intent(nd) can be
> > made unconditional.
>
> Sorry, but phrases like "looks correct" and "I believe" don't inspire
> confidence. (Although what you say looks correct ;)) Are you sure?

We do need the call to release_open_intent(), since otherwise we will
leak a struct file. The question is whether we can optimise away the
IS_ERR() test. In my opinion, we can.

> And do we also need a path_release(nd) in there?

No. do_follow_link() should release the path for us on error. Replacing
with a 'goto exit' would therefore be a mistake.

Cheers,
  Trond