Subject: Re: [RFC][PATCH 2/7] RSS controller core
Posted by Dave Hansen on Tue, 13 Mar 2007 20:28:26 GMT
View Forum Message <> Reply to Message

On Tue, 2007-03-13 at 19:09 +0000, Alan Cox wrote:
> > stuff is happening by comparing page->count and page->_mapcount, but it
> > certainly wouldn't be conclusive. But, does this kind of nonsense even
> > happen in practice?
>
> "Is it useful for me as a bad guy to make it happen ?"

A very fine question. ;)

To exploit this, you'd need to:
1. need to access common data with another user
2. be patient enough to wait
3. determine when one of those users had actually pulled
   a page in from disk, which sys_mincore() can do, right?

I guess that might be a decent reason to not charge the guy who brings
the page in for the page's entire lifetime.

So, unless we can change page ownership after it has been allocated,
anyone accessing shared data can get around resource limits if they are
patient.

-- Dave

_____
Containers mailing list
Containers@lists.osdl.org
https://lists.osdl.org/mailman/listinfo/containers