Subject: Re: [RFC][PATCH 2/7] RSS controller core
Posted by ebiederm on Fri, 16 Mar 2007 00:55:45 GMT
View Forum Message <> Reply to Message

Alan Cox <alan@lxorguk.ukuu.org.uk> writes:

>> 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 ?"

To create a DOS attack.

- Allocate some memory you know your victim will want in the future,
  (shared libraries and the like).
- Wait until your victim is using the memory you allocated.
- Terminate your memory resource group.
- Victim is pushed over memory limits by your exiting.
- Victim can no longer allocate memory
- Victim dies

It's not quite that easy unless your victim calls mlockall(MCL_FUTURE),
but the potential is clearly there.

Am I missing something? Or is this fundamental to any first touch scenario?

I just know I have problems with first touch because it is darn hard to
reason about.

Eric

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