Subject: Re: [RFC][PATCH 2/7] RSS controller core
Posted by Dave Hansen on Fri, 16 Mar 2007 16:31:00 GMT
View Forum Message <> Reply to Message

On Thu, 2007-03-15 at 18:55 -0600, Eric W. Biederman wrote:
> 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.

I think it's fundamental to any case where two containers share the use
of the page, but either one _can_ be charged but does not receive a
full charge for it.

I don't think it's uniquely associated with first-touch schemes.

The software zones approach where there would be a set of "shared" zones
would not have this problem, because any sharing would have to occur on
data on which neither one was being charged.

http://linux-mm.org/SoftwareZones

-- Dave

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