

---

Subject: Re: [PATCH 11/11] protect architectures where THREAD\_SIZE >= PAGE\_SIZE against fork bombs

Posted by [Glauber Costa](#) on Tue, 26 Jun 2012 08:44:13 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

On 06/26/2012 12:45 PM, David Rientjes wrote:

> On Tue, 26 Jun 2012, Glauber Costa wrote:

>

>>>> diff --git a/include/linux/thread\_info.h b/include/linux/thread\_info.h

>>>> index ccc1899..914ec07 100644

>>>> --- a/include/linux/thread\_info.h

>>>> +++ b/include/linux/thread\_info.h

>>>> @@ -61,6 +61,12 @@ extern long do\_no\_restart\_syscall(struct restart\_block

>>>> \*parm);

>>>> # define THREADINFO\_GFP (GFP\_KERNEL | \_\_GFP\_NOTRACK)

>>>> #endif

>>>>

>>>> #ifdef CONFIG\_CGROUP\_MEM\_RES\_CTLR\_KMEM

>>>> # define THREADINFO\_GFP\_ACCOUNTED (THREADINFO\_GFP | \_\_GFP\_KMEMCG)

>>>> #else

>>>> # define THREADINFO\_GFP\_ACCOUNTED (THREADINFO\_GFP)

>>>> #endif

>>>> +

>>>

>>> This type of requirement is going to become nasty very quickly if nobody

>>> can use \_\_GFP\_KMEMCG without testing for

CONFIG\_CGROUP\_MEM\_RES\_CTLR\_KMEM.

>>> Perhaps define \_\_GFP\_KMEMCG to be 0x0 if it's not enabled, similar to how

>>> kmemcheck does?

>>>

>> That is what I've done in my first version of this patch. At that time,

>> Christoph wanted it to be this way so we would make sure it would never be

>> used with #CONFIG\_CGROUP\_MEM\_RES\_CTLR\_KMEM defined. A value of zero will

>> generate no errors. Undefined value will.

>>

>> Now, if you ask me, I personally prefer following what kmemcheck does here...

>>

>

> Right, because I'm sure that \_\_GFP\_KMEMCG will be used in additional

> places outside of this patchset and it will be a shame if we have to

> always add #ifdef's. I see no reason why we would care if \_\_GFP\_KMEMCG

> was used when CONFIG\_CGROUP\_MEM\_RES\_CTLR\_KMEM=n with the semantics that it

> as in this patchset. It's much cleaner by making it 0x0 when disabled.

>

What I can do, instead, is to WARN\_ON conditionally to the config option in the page allocator, and make sure no one is actually passing the flag in that case.

---