

---

Subject: Re: [PATCH] proc: check vma-&gt;vm\_file before dereferencing

Posted by [akpm](#) on Mon, 15 Oct 2012 22:04:28 GMT

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

---

On Tue, 16 Oct 2012 01:52:30 +0400

Cyrill Gorcunov <[gorcunov@openvz.org](mailto:gorcunov@openvz.org)> wrote:

> On Mon, Oct 15, 2012 at 02:40:48PM -0700, Andrew Morton wrote:

> > On Mon, 15 Oct 2012 19:30:03 +0400

> > Stanislav Kinsbursky <[skinsbursky@parallels.com](mailto:skinsbursky@parallels.com)> wrote:

> >

> > > It can be equal to NULL.

> > >

> >

> > Please write better changelogs, so people do not have to ask questions

> > such as:

> >

> > - Under what conditions does this bug trigger?

> >

> > - In which kernel version(s)?

> >

> > - Is it a post-3.6 regression?

>

> Andrew, would the following changelog be enough?

>

> The commit 7b540d0646ce122f0ba4520412be91e530719742 switched

> proc\_map\_files\_readdir to use @f\_mode directly instead of grabbing

> @file reference, but same time the test for @vm\_file presence was

> lost leading to nil dereference. The patch brings the test back.

>

> The all proc\_map\_files feature is CONFIG\_CHECKPOINT\_RESTORE wrapped

> (which is set to 'n' by default) so the bug doesn't affect regular

> kernels.

>

> The regression is 3.7-rc1 only as far as I can tell.

Ah, I see, great, thanks.

---