
Subject: [PATCH] proc: check vma->vm_file before dereferencing
Posted by [Stanislav Kinsbursky](#) on Mon, 15 Oct 2012 15:30:03 GMT
[View Forum Message](#) <> [Reply to Message](#)

It can be equal to NULL.

Signed-off-by: Stanislav Kinsbursky <skinsbursky@parallels.com>

fs/proc/base.c | 5 +++--

1 files changed, 3 insertions(+), 2 deletions(-)

diff --git a/fs/proc/base.c b/fs/proc/base.c

index 144a967..74fc562 100644

--- a/fs/proc/base.c

+++ b/fs/proc/base.c

@@ -1770,8 +1770,9 @@ static struct dentry *proc_map_files_lookup(struct inode *dir,
if (!vma)
goto out_no_vma;

- result = proc_map_files_instantiate(dir, dentry, task,
- (void *) (unsigned long) vma->vm_file->f_mode);
+ if (vma->vm_file)
+ result = proc_map_files_instantiate(dir, dentry, task,
+ (void *) (unsigned long) vma->vm_file->f_mode);

out_no_vma:

up_read(&mm->mmap_sem);

Subject: Re: [PATCH] proc: check vma->vm_file before dereferencing
Posted by [akpm](#) on Mon, 15 Oct 2012 21:40:48 GMT
[View Forum Message](#) <> [Reply to Message](#)

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

Stanislav Kinsbursky <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?

Thanks.

Subject: Re: [PATCH] proc: check vma->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> 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> 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.

Subject: Re: [PATCH] proc: check vma->vm_file before dereferencing
Posted by [Stanislav Kinsbursky](#) on Tue, 16 Oct 2012 07:26:33 GMT

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

> On Mon, 15 Oct 2012 19:30:03 +0400
> Stanislav Kinsbursky <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?
>

Sure. Sorry.

> Thanks.
>

--

Best regards,
Stanislav Kinsbursky
