
Subject: Re: /proc/*/pagemap BUG: sleeping function called from invalid context
Posted by [Matt Mackall](#) on Mon, 09 Apr 2007 21:43:19 GMT
[View Forum Message](#) <> [Reply to Message](#)

On Mon, Apr 09, 2007 at 12:25:54PM +0400, Alexey Dobriyan wrote:

```
> After
> cat /proc/self/pagemap
>
> BUG: sleeping function called from invalid context at include/asm/uaccess.h:453
> in_atomic():1, irqs_disabled():0
> 1 lock held by cat/14183:
> #0: (&mm->mmap_sem){----}, at: [<c017d17b>] pagemap_read+0x11f/0x21b
> [<c01b7bc7>] copy_to_user+0x37/0x4c
> [<c017cf92>] add_to_pagemap+0x49/0x6f
> [<c017d034>] pagemap_pte_range+0x56/0x7e
> [<c017cfde>] pagemap_pte_range+0x0/0x7e
> [<c01b481d>] walk_page_range+0xf1/0x1a0
> [<c017d1e3>] pagemap_read+0x187/0x21b
> [<c01fdafa>] tty_write+0x1bb/0x1cc
> [<c017d05c>] pagemap_read+0x0/0x21b
> [<c01589b0>] vfs_read+0x72/0x95
> [<c0158cce>] sys_read+0x41/0x67
> [<c0103d96>] sysenter_past_esp+0x8f/0x99
> [<c0103d66>] sysenter_past_esp+0x5f/0x99
> =====
```

This looks like it was caused by CONFIG_HIGHPTE making pte_offset_map call kmap_atomic. The message about mm->mmap_sem is spurious. Looking at a fix.

--

Mathematics is the supreme nostalgia of our time.
