Linux kernel client - Bug #65

crash in tcp_sendpage

04/23/2010 04:13 PM - Sage Weil

Status:	Resolved	**Start date:**	04/23/2010
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	v2.6.34	**Spent time:**	0.00 hour
Source:		**Reviewed:**	
Tags:		**Affected Versions:**	
Backport:		**ceph-qa-suite:**	
Regression:	No	**Crash signature:**	
Severity:	3 - minor		

Description

on issdm. master branch (standalone).

[2900.360800] ceph: osd16 weight 0x10000 (in)
[2900.360802] ceph: osd17 weight 0x10000 (in)
[2900.360804] ceph: osd19 weight 0x10000 (in)
[2900.360806] ceph: osd20 weight 0x10000 (in)
[2900.360808] ceph: osd25 weight 0x10000 (in)
[2900.360810] ceph: osd14 up
[2900.360811] ceph: osd18 up
[2900.360813] ceph: osd37 up
[2900.360815] ceph: osd14 weight 0x10000 (in)
[2900.360817] ceph: osd18 weight 0x10000 (in)
[2900.360818] ceph: osd37 weight 0x10000 (in)
[3260.360025] ceph: tid 1538 timed out on osd6, will reset osd
[3263.786024] BUG: unable to handle kernel paging request at 000000000002a348
[3263.786063] IP: [<ffffffff8146f4d5>] do_tcp_sendpages+0x425/0x520
[3263.786098] PGD 216865067 PUD 2114f4067 PMD 0
[3263.786126] Oops: 0000 [#1] SMP
[3263.786150] last sysfs file: /sys/module/libcrc32c/initstate
[3263.786177] CPU 3
[3263.786197] Modules linked in: ceph btrfs zlib_deflate crc32c libcrc32c nfs lockd nfs_acl auth_rpcgss sunrpc radeon ttm drm ib_mthca lp psmouse iptable_filter k8temp ib_mad ip_tables i2c_algo_bit i2c_nforce2 amd64_edac_mod ib_core edac_core shpchp serio_raw parport x_tables joydev floppy e1000 usbhid forcedeth
[3263.786346] Pid: 2696, comm: ceph-msgr/3 Not tainted 2.6.31-19-server #56 H8DMR-82
[3263.786390] RIP: 0010:[<ffffffff8146f4d5>] [<ffffffff8146f4d5>] do_tcp_sendpages+0x425/0x520
[3263.786436] RSP: 0018:ffff88011a4e3be0 EFLAGS: 00010246
[3263.786461] RAX: ffffffff817f66c0 RBX: ffff8800d61ae180 RCX: ffff8801dfba1000
[3263.786490] RDX: ffff88017bdd4140 RSI: 000000000000017f RDI: 0000000000000000
[3263.786519] RBP: ffff88011a4e3c80 R08: 0000000000000000 R09: 000000000002a348
[3263.786548] R10: 000000000000017f R11: 0000000000000000 R12: 000000000000c040
[3263.786576] R13: 0000000000000000 R14: ffff88011a4e3c4c R15: 0000000000000e81
[3263.786606] FS: 00007fc9797fa910(0000) GS:ffffc90000600000(0000) knlGS:0000000000000000
[3263.786650] CS: 0010 DS: 0018 ES: 0018 CR0: 000000008005003b
[3263.786676] CR2: 000000000002a348 CR3: 00000002115a6000 CR4: 00000000000006e0
[3263.786705] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
[3263.786734] DR3: 0000000000000000 DR6: 00000000ffff0ff0 DR7: 0000000000000400
[3263.786763] Process ceph-msgr/3 (pid: 2696, threadinfo ffff88011a4e2000, task ffff88011991dac0)
[3263.786807] Stack:
[3263.786826] ffff88011a4e3bf0 ffffffff8105379d ffff88011a4e3c40 ffff8801dfba1000
[3263.786858] <0> 000000000002a348 0000000000000008 0000404000000000 000005a800000e81
[3263.786905] <0> 0000000000000e81 ffff8800d61ae250 ffff88011a4e3ca8 000000000000017f
[3263.786967] Call Trace:
[3263.786993] [<ffffffff8105379d>] ? default_wake_function+0xd/0x10
[3263.787022] [<ffffffff8147015c>] tcp_sendpage+0x5c/0x80

```
[ 3263.787051]  [<ffffffff81423876>] kernel_sendpage+0x16/0x30
[ 3263.787091]  [<ffffffffa035de27>] con_work+0x347/0x1d60 [ceph]
[ 3263.787121]  [<ffffffff815252b9>] ? thread_return+0x48/0x37f
[ 3263.787155]  [<ffffffffa035dae0>] ? con_work+0x0/0x1d60 [ceph]
[ 3263.787186]  [<ffffffff810731a5>] run_workqueue+0x95/0x170
[ 3263.787213]  [<ffffffff81073324>] worker_thread+0xa4/0x120
[ 3263.787241]  [<ffffffff810784b0>] ? autoremove_wake_function+0x0/0x40
[ 3263.787270]  [<ffffffff81073280>] ? worker_thread+0x0/0x120
[ 3263.787297]  [<ffffffff810780c6>] kthread+0xa6/0xb0
[ 3263.787324]  [<ffffffff810130aa>] child_rip+0xa/0x20
[ 3263.787349]  [<ffffffff81078020>] ? kthread+0x0/0xb0
[ 3263.787375]  [<ffffffff810130a0>] ? child_rip+0x0/0x20
[ 3263.787399] Code: 83 08 02 00 00 e9 85 fe ff ff 0f 1f 40 00 8b 7c 16 14 03 7c 32 10 39 7d 98 c7 45 8c 01 00 00 00 0f 85 96 fe ff ff e9 52 fd ff ff <66> 41 83 39 00 0f 88 e4 00 00 00 4c 89 c8 f0 ff 40 08 8b 81 d8
[ 3263.787559] RIP  [<ffffffff8146f4d5>] do_tcp_sendpages+0x425/0x520
[ 3263.787587]  RSP <ffff88011a4e3be0>
[ 3263.787608] CR2: 000000000002a348
[ 3263.788150] ---[ end trace 89a9ffe49d7f9748 ]---
[ 3309.951906] ceph: mds0 caps stale
[ 3323.660043] ceph:  tid 1539 timed out on osd6, will reset osd
```

History

#1 - 04/28/2010 11:23 AM - Sage Weil

- Target version set to v2.6.34

#2 - 05/03/2010 11:13 AM - Sage Weil

this is probably a problem with the backport.. it went away when we switch to 2.6.34-rc3 on issdm

#3 - 05/07/2010 09:39 AM - Sage Weil

- Status changed from New to Resolved

may have also been related to #109.

closing this one, since we haven't seen it in a while.