



author Quinn Tran <qutran@marvell.com> 2023-03-12 21:37:11 -0700  
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2023-03-30 12:49:13 +0200  
commit [6d57b77d7369ed73836c82b25f785b34923eef84](#) (patch)  
tree [37bae13a135a2ee6320f50aec2a73c86a8c05403](#)  
parent [682938af0a5fd7c3f3e7453ea10c89c7c59b33d9](#) (diff)  
download [linux-6d57b77d7369ed73836c82b25f785b34923eef84.tar.gz](#)

**diff options**

context:

3 ▼

space:

include ▼

mode:

unified ▼

**scsi: qla2xxx: Synchronize the IOCB count to be in order**

commit d3affdeb400f3adc925bd996f3839481f5291839 upstream.

A system hang was observed with the following call trace:

```
BUG: kernel NULL pointer dereference, address: 0000000000000000
PGD 0 P4D 0
Ops: 0000 [#1] PREEMPT SMP NOPTI
CPU: 15 PID: 86747 Comm: nvme Kdump: loaded Not tainted 6.2.0+ #1
Hardware name: Dell Inc. PowerEdge R6515/04F3CJ, BIOS 2.7.3 03/31/2022
RIP: 0010:__wake_up_common+0x55/0x190
Code: 41 f6 01 04 0f 85 b2 00 00 00 48 8b 43 08 4c 8d
      40 e8 48 8d 43 08 48 89 04 24 48 89 c6\
      49 8d 40 18 48 39 c6 0f 84 e9 00 00 00 <49> 8b 40 18 89 6c 24 14 31
      ed 4c 8d 60 e8 41 8b 18 f6 c3 04 75 5d
RSP: 0018:ffffb05a82afbba0 EFLAGS: 00010082
RAX: 0000000000000000 RBX: ffff8f9b83a00018 RCX: 0000000000000000
RDX: 0000000000000001 RSI: ffff8f9b83a00020 RDI: ffff8f9b83a00018
RBP: 0000000000000001 R08: ffffffffefefefef R09: ffff8f9b83a00018
R10: 70735f7472617473 R11: 5f30307832616c71 R12: 0000000000000001
R13: 0000000000000003 R14: 0000000000000000 R15: 0000000000000000
FS:  00007f815cf4c740(0000) GS:ffff8f9e00000000(0000)
      knlGS:0000000000000000
CS:  0010 DS: 0000 ES: 0000 CR0: 0000000080050033
CR2: 0000000000000000 CR3: 0000000010633a000 CR4: 0000000000350ee0
Call Trace:
<TASK>
__wake_up_common_lock+0x83/0xd0
qla_nvme_ls_req+0x21b/0x2b0 [qla2xxx]
__nvme_fc_send_ls_req+0x1b5/0x350 [nvme_fc]
nvme_fc_xmt_disconnect_assoc+0xca/0x110 [nvme_fc]
nvme_fc_delete_association+0x1bf/0x220 [nvme_fc]
? nvme_remove_namespaces+0x9f/0x140 [nvme_core]
nvme_do_delete_ctrl+0x5b/0xa0 [nvme_core]
nvme_sysfs_delete+0x5f/0x70 [nvme_core]
kernfs_fop_write_iter+0x12b/0x1c0
vfs_write+0x2a3/0x3b0
ksys_write+0x5f/0xe0
do_syscall_64+0x5c/0x90
? syscall_exit_work+0x103/0x130
? syscall_exit_to_user_mode+0x12/0x30
? do_syscall_64+0x69/0x90
```

```
? exit_to_user_mode_loop+0xd0/0x130
? exit_to_user_mode_prepare+0xec/0x100
? syscall_exit_to_user_mode+0x12/0x30
? do_syscall_64+0x69/0x90
? syscall_exit_to_user_mode+0x12/0x30
? do_syscall_64+0x69/0x90
entry_SYSCALL_64_after_hwframe+0x72/0xdc
RIP: 0033:0x7f815cd3eb97
```

The IOCB counts are out of order and that would block any commands from going out and subsequently hang the system. Synchronize the IOCB count to be in correct order.

Fixes: 5f63a163ed2f ("scsi: qla2xxx: Fix exchange oversubscription for management commands")

Cc: stable@vger.kernel.org

Signed-off-by: Quinn Tran <qutran@marvell.com>

Signed-off-by: Niles Javali <njavali@marvell.com>

Link: <https://lore.kernel.org/r/20230313043711.13500-3-njavali@marvell.com>

Reviewed-by: Himanshu Madhani <himanshu.madhani@oracle.com>

Reviewed-by: John Meneghini <jmeneghi@redhat.com>

Tested-by: Lin Li <lilin@redhat.com>

Signed-off-by: Martin K. Petersen <martin.petersen@oracle.com>

Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>

## Diffstat

```
-rw-r--r-- drivers/scsi/qla2xxx/qla_isr.c 3
```

1 files changed, 2 insertions, 1 deletions

**diff --git a/drivers/scsi/qla2xxx/qla\_isr.c b/drivers/scsi/qla2xxx/qla\_isr.c**

**index cbbd7014da939b..86928a762a7a62 100644**

**--- a/drivers/scsi/qla2xxx/qla\_isr.c**

**+++ b/drivers/scsi/qla2xxx/qla\_isr.c**

```
@@ -1900,6 +1900,8 @@ qla2x00_get_sp_from_handle(scsi_qla_host_t *vha, const char *func,
    }
```

```
    req->outstanding_cmds[index] = NULL;
```

```
+
+    qla_put_fw_resources(sp->qpair, &sp->iores);
    return sp;
}
```

```
@@ -3112,7 +3114,6 @@ qla25xx_process_bidir_status_iocb(scsi_qla_host_t *vha, void *pkt,
    }
    bsg_reply->reply_payload_rcv_len = 0;
```

```
-    qla_put_fw_resources(sp->qpair, &sp->iores);
done:
    /* Return the vendor specific reply to API */
    bsg_reply->reply_data.vendor_reply.vendor_rsp[0] = rval;
```