author	Nilesh Javali <njavali@marvell.com>	2023-03-12 21:37:10 -0700
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2023-04-05 11:23:37 +0200
commit	231cfa78ec5badd84a1a2b09465bfad1a926aba1 (patch)	
tree	4fdfd151a63b7f2c6ca0efc40ea00d67ae42dbda	
parent	f73a88df19b7997829fd05ae9bbc62f86541d789 (diff)	
download	linux-231cfa78ec5badd84a1a2b09465bfad1a926aba1.tar.gz	

scsi: qla2xxx: Perform lockless command completion in abort path

```
commit 0367076b0817d5c75dfb83001ce7ce5c64d803a9 upstream.

While adding and removing the controller, the following call trace was
observed:

WARNING: CPU: 3 PID: 623596 at kernel/dma/mapping.c:532 dma_free_attrs+0x33/0x50
CPU: 3 PID: 623596 Comm: sh Kdump: loaded Not tainted 5.14.0-96.el9.x86_64 #1
RIP: 0010:dma_free_attrs+0x33/0x50

Call Trace:
   qla2x00_async_sns_sp_done+0x107/0x1b0 [qla2xxx]
   qla2x00_abort_srb+0x8e/0x250 [qla2xxx]
   ? ql_dbg+0x70/0x100 [qla2xxx]
   __qla2x00_abort_all_cmds+0x108/0x190 [qla2xxx]
   qla2x00_abort_all_cmds+0x24/0x70 [qla2xxx]
   qla2x00_abort_isp_cleanup+0x305/0x3e0 [qla2xxx]
   qla2x00_remove_one+0x364/0x400 [qla2xxx]
   pci_device_remove+0x36/0xa0
   __device_release_driver+0x17a/0x230
   device_release_driver+0x24/0x30
   pci_stop_bus_device+0x68/0x90
   pci_stop_and_remove_bus_device_locked+0x16/0x30
   remove_store+0x75/0x90
   kernfs_fop_write_iter+0x11c/0x1b0
   new_sync_write+0x11f/0x1b0
   vfs_write+0x1eb/0x280
   ksys_write+0x5f/0xe0
   do_syscall_64+0x5c/0x80
   ? do_user_addr_fault+0x1d8/0x680
   ? do_syscall_64+0x69/0x80
   ? exc_page_fault+0x62/0x140
   ? asm_exc_page_fault+0x8/0x30
   entry_SYSCALL_64_after_hwframe+0x44/0xae

The command was completed in the abort path during driver unload with a
lock held, causing the warning in abort path. Hence complete the command
without any lock held.

Reported-by: Lin Li <lilin@redhat.com>
Tested-by: Lin Li <lilin@redhat.com>
Cc: stable@vger.kernel.org
```

Signed-off-by: Nilesh Javali <njavali@marvell.com>
Link: https://lore.kernel.org/r/20230313043711.13500-2-njavali@marvell.com
Reviewed-by: Himanshu Madhani <himanshu.madhani@oracle.com>
Reviewed-by: John Meneghini <jmeneghi@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_os.c 11

1 files changed, 11 insertions, 0 deletions

```
diff --git a/drivers/scsi/qla2xxx/qla_os.c b/drivers/scsi/qla2xxx/qla_os.c
index e1132970f18922..38b8ff87ec0a73 100644
--- a/drivers/scsi/qla2xxx/qla_os.c
+++ b/drivers/scsi/qla2xxx/qla_os.c
@@ -1762,6 +1762,17 @@ __qla2x00_abort_all_cmds(struct qla_qpair *qp, int res)
        for (cnt = 1; cnt < req->num_outstanding_cmds; cnt++) {
                sp = req->outstanding_cmds[cnt];
                if (sp) {
+                       /*
+                        * perform lockless completion during driver unload
+                        */
+                       if (qla2x00_chip_is_down(vha)) {
+                               req->outstanding_cmds[cnt] = NULL;
+                               spin_unlock_irqrestore(qp->qp_lock_ptr, flags);
+                               sp->done(sp, res);
+                               spin_lock_irqsave(qp->qp_lock_ptr, flags);
+                               continue;
+                       }
+
                        switch (sp->cmd_type) {
                        case TYPE_SRB:
                                qla2x00_abort_srb(qp, sp, res, &flags);
```