[PATCH] scsi: qla4xxx: add error handling for try_module_get

3 messages

Zhouyang Jia <jiazhouyang09@gmail.com> Tue, Jun 12, 2018 at 12:48 AM
Cc: Zhouyang Jia <jiazhouyang09@gmail.com>, QLogic-Storage-Upstream@qlogic.com, "James E.J. Bottomley" <jejb@linux.vnet.ibm.com>, "Martin K. Petersen" <martin.petersen@oracle.com>, linux-scsi@vger.kernel.org, linux-kernel@vger.kernel.org

When try_module_get fails, the lack of error-handling code may
cause unexpected results.

This patch adds error-handling code after calling try_module_get.

Signed-off-by: Zhouyang Jia <jiazhouyang09@gmail.com>
---
drivers/scsi/qla4xxx/ql4_os.c | 9 +++++++--
1 file changed, 7 insertions(+), 2 deletions(-)

```
diff --git a/drivers/scsi/qla4xxx/ql4_os.c b/drivers/scsi/qla4xxx/ql4_os.c
index 0e13349..6b677ab 100644
--- a/drivers/scsi/qla4xxx/ql4_os.c
+++ b/drivers/scsi/qla4xxx/ql4_os.c
@@ -7687,7 +7687,10 @@ static int qla4xxx_sysfs_ddb_logout_sid(struct iscsi_cls_session *cls_sess)
         * to be seamless without actually destroying the
         * session
         **/
-       try_module_get(qla4xxx_iscsi_transport.owner);
+       if (!try_module_get(qla4xxx_iscsi_transport.owner))
+               ql4_printk(KERN_WARNING, ha,
+                          "%s: cannot get module.\n", __func__);
+
        iscsi_destroy_endpoint(ddb_entry->conn->ep);

        spin_lock_irqsave(&ha->hardware_lock, flags);
@@ -8970,7 +8973,9 @@ static void qla4xxx_destroy_fw_ddb_session(struct scsi_qla_host *ha)
                         * to be seamless without actually destroying the
                         * session
                         **/
-                       try_module_get(qla4xxx_iscsi_transport.owner);
+                       if (!try_module_get(qla4xxx_iscsi_transport.owner))
+                               ql4_printk(KERN_WARNING, ha,
+                                          "%s: cannot get module.\n", __func__);
                        iscsi_destroy_endpoint(ddb_entry->conn->ep);
                        qla4xxx_free_ddb(ha, ddb_entry);
                        iscsi_session_teardown(ddb_entry->sess);
--
2.7.4
```

Rangankar, Manish <Manish.Rangankar@cavium.com> Tue, Jun 12, 2018 at 3:52 AM
To: Zhouyang Jia <jiazhouyang09@gmail.com>
Cc: Dept-Eng QLogic Storage Upstream <QLogic-Storage-Upstream@cavium.com>, "James E.J. Bottomley" <jejb@linux.vnet.ibm.com>, "Martin K. Petersen" <martin.petersen@oracle.com>, "linux-scsi@vger.kernel.org" <linux-scsi@vger.kernel.org>, "linux-kernel@vger.kernel.org" <linux-kernel@vger.kernel.org>

[Quoted text hidden]
Thanks,

Acked-by: Manish Rangankar <Manish.Rangankar@cavium.com>

James Bottomley <jejb@linux.vnet.ibm.com> Tue, Jun 12, 2018 at 10:08 AM
To: Zhouyang Jia <jiazhouyang09@gmail.com>
Cc: QLogic-Storage-Upstream@qlogic.com, "Martin K. Petersen" <martin.petersen@oracle.com>, linux-scsi@vger.kernel.org, linux-kernel@vger.kernel.org

> On Tue, 2018-06-12 at 12:48 +0800, Zhouyang Jia wrote:
> > When try_module_get fails, the lack of error-handling code may
> > cause unexpected results.
> >
> > This patch adds error-handling code after calling try_module_get.
> >
> > Signed-off-by: Zhouyang Jia <jiazhouyang09@gmail.com>
> > ---
> > drivers/scsi/qla4xxx/ql4_os.c | 9 +++++++--
> > 1 file changed, 7 insertions(+), 2 deletions(-)
> >
> > diff --git a/drivers/scsi/qla4xxx/ql4_os.c
> > b/drivers/scsi/qla4xxx/ql4_os.c
> > index 0e13349..6b677ab 100644
> > --- a/drivers/scsi/qla4xxx/ql4_os.c
> > +++ b/drivers/scsi/qla4xxx/ql4_os.c
> > @@ -7687,7 +7687,10 @@ static int qla4xxx_sysfs_ddb_logout_sid(struct
> > iscsi_cls_session *cls_sess)
> >   * to be seamless without actually destroying the
> >   * session
> >   **/
> > -   try_module_get(qla4xxx_iscsi_transport.owner);
> > +   if (!try_module_get(qla4xxx_iscsi_transport.owner))
> > +   ql4_printk(KERN_WARNING, ha,
> > +   "%s: cannot get module.\n", __func__);
> > +

This isn't error handling at all. If try_module_get() fails it means
you're about to get the text segment freed from underneath you if the
code can be executed concurrently with the module_exit function. The
comment implies that qla4xxx operates with a zero module use count even
when there are logged in sessions, so module_exit can race with logout
(or indeed any other userspace initiated function). This means that
the entire module reference counting of qla4xxx looks to be racy and
wrong. Can we get a description of what the expected theoretical model
is so we can validate (or invalidate) this theory?

James