Gmail **zy j <jiazhouyang09@gmail.com>**

[PATCH] scsi: bfa: add error handling for pci_iomap

6 messages

Zhouyang Jia <jiazhouyang09@gmail.com> Mon, Jun 11, 2018 at 4:26 AM
Cc: Zhouyang Jia <jiazhouyang09@gmail.com>, Anil Gurumurthy <anil.gurumurthy@qlogic.com>, Sudarsana Kalluru <sudarsana.kalluru@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 pci_iomap fails, the lack of error-handling code may
cause unexpected results.

This patch adds error-handling code after calling pci_iomap.

Signed-off-by: Zhouyang Jia <jiazhouyang09@gmail.com>

```
---
 drivers/scsi/bfa/bfad.c | 5 +++++
 1 file changed, 5 insertions(+)

diff --git a/drivers/scsi/bfa/bfad.c b/drivers/scsi/bfa/bfad.c
index bd7e6a6f..74e39d7 100644
--- a/drivers/scsi/bfa/bfad.c
+++ b/drivers/scsi/bfa/bfad.c
@@ -760,6 +760,11 @@ bfad_pci_init(struct pci_dev *pdev, struct bfad_s *bfad)
                goto out_release_region;
        }

+       if (bfad->pci_bar2_kva == NULL) {
+               printk(KERN_ERR "Fail to map bar2\n");
+               goto out_release_region;
+       }
+
        bfad->hal_pcidev.pci_slot = PCI_SLOT(pdev->devfn);
        bfad->hal_pcidev.pci_func = PCI_FUNC(pdev->devfn);
        bfad->hal_pcidev.pci_bar_kva = bfad->pci_bar0_kva;
--
2.7.4
```

Johannes Thumshirn <jthumshirn@suse.de> Tue, Jun 12, 2018 at 3:18 AM
To: Zhouyang Jia <jiazhouyang09@gmail.com>
Cc: Anil Gurumurthy <anil.gurumurthy@qlogic.com>, Sudarsana Kalluru <sudarsana.kalluru@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

On Mon, Jun 11, 2018 at 04:26:21PM +0800, Zhouyang Jia wrote:

```
> When pci_iomap fails, the lack of error-handling code may
> cause unexpected results.
>
> This patch adds error-handling code after calling pci_iomap.
>
> Signed-off-by: Zhouyang Jia <jiazhouyang09@gmail.com>
> ---
>  drivers/scsi/bfa/bfad.c | 5 +++++
>  1 file changed, 5 insertions(+)
>
> diff --git a/drivers/scsi/bfa/bfad.c b/drivers/scsi/bfa/bfad.c
> index bd7e6a6f..74e39d7 100644
> --- a/drivers/scsi/bfa/bfad.c
> +++ b/drivers/scsi/bfa/bfad.c
> @@ -760,6 +760,11 @@ bfad_pci_init(struct pci_dev *pdev, struct bfad_s *bfad)
>               goto out_release_region;
>       }
>
> +     if (bfad->pci_bar2_kva == NULL) {
> +             printk(KERN_ERR "Fail to map bar2\n");
> +             goto out_release_region;
> +     }
> +
```

If we hit this, we'll "leak" bfad->pci_bar0_kva.

You'll need to do something like:

```
+       if (bfad->pci_bar2_kva == NULL) {
+                 printk(KERN_ERR "Fail to map bar2\n");
+         goto out_unmap_bar0;
+       }
```

and:

```
+ out_unmap_bar0:
+         pci_iounmap(pdev, bfad->pci_bar0_kva);
  out_release_region:
          pci_release_regions(pdev);
```

--
Johannes Thumshirn Storage
jthumshirn@suse.de +49 911 74053 689
SUSE LINUX GmbH, Maxfeldstr. 5, 90409 Nürnberg
GF: Felix Imendörffer, Jane Smithard, Graham Norton
HRB 21284 (AG Nürnberg)
Key fingerprint = EC38 9CAB C2C4 F25D 8600 D0D0 0393 969D 2D76 0850

Zhouyang Jia <jiazhouyang09@gmail.com> Thu, Jun 14, 2018 at 12:34 AM
To: Johannes Thumshirn <jthumshirn@suse.de>
Cc: Anil Gurumurthy <anil.gurumurthy@qlogic.com>, Sudarsana Kalluru <sudarsana.kalluru@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

Hi,

I'll fix this in v2. Thanks for your kind reply.

Best,
Zhouyang
[Quoted text hidden]

Zhouyang Jia <jiazhouyang09@gmail.com> Thu, Jun 14, 2018 at 7:57 AM
Cc: Zhouyang Jia <jiazhouyang09@gmail.com>, Anil Gurumurthy <anil.gurumurthy@qlogic.com>, Sudarsana Kalluru <sudarsana.kalluru@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 pci_iomap fails, the lack of error-handling code may
cause unexpected results.

This patch adds error-handling code after calling pci_iomap.

Signed-off-by: Zhouyang Jia <jiazhouyang09@gmail.com>

```
---
v1->v2:
- Unmap bfad->pci_bar0_kva.
---
 drivers/scsi/bfa/bfad.c | 7 +++++++
 1 file changed, 7 insertions(+)

diff --git a/drivers/scsi/bfa/bfad.c b/drivers/scsi/bfa/bfad.c
index bd7e6a6f..693e180 100644
--- a/drivers/scsi/bfa/bfad.c
+++ b/drivers/scsi/bfa/bfad.c
@@ -760,6 +760,11 @@ bfad_pci_init(struct pci_dev *pdev, struct bfad_s *bfad)
                goto out_release_region;
        }

+       if (bfad->pci_bar2_kva == NULL) {
+               printk(KERN_ERR "Fail to map bar2\n");
+               goto out_unmap_bar0;
+       }
+
        bfad->hal_pcidev.pci_slot = PCI_SLOT(pdev->devfn);
        bfad->hal_pcidev.pci_func = PCI_FUNC(pdev->devfn);
        bfad->hal_pcidev.pci_bar_kva = bfad->pci_bar0_kva;
@@ -797,6 +802,8 @@ bfad_pci_init(struct pci_dev *pdev, struct bfad_s *bfad)

        return 0;

+out_unmap_bar0:
+       pci_iounmap(pdev, bfad->pci_bar0_kva);
 out_release_region:
        pci_release_regions(pdev);
 out_disable_device:
--
2.7.4
```

Andy Shevchenko <andy.shevchenko@gmail.com> Thu, Jun 14, 2018 at 8:00 AM
To: Zhouyang Jia <jiazhouyang09@gmail.com>
Cc: Anil Gurumurthy <anil.gurumurthy@qlogic.com>, Sudarsana Kalluru <sudarsana.kalluru@qlogic.com>, "James E.J. Bottomley" <jejb@linux.vnet.ibm.com>, "Martin K. Petersen" <martin.petersen@oracle.com>, linux-scsi <linux-scsi@vger.kernel.org>, Linux Kernel Mailing List <linux-kernel@vger.kernel.org>

On Thu, Jun 14, 2018 at 2:57 PM, Zhouyang Jia <jiazhouyang09@gmail.com> wrote:

```
> When pci_iomap fails, the lack of error-handling code may
```

> cause unexpected results.

What results?
How had you tested it?

> This patch adds error-handling code after calling pci_iomap.

> +   if (bfad->pci_bar2_kva == NULL) {

> +   printk(KERN_ERR "Fail to map bar2\n");

pr_err() ?

> +   goto out_unmap_bar0;
> +   }

--
With Best Regards,
Andy Shevchenko

Zhouyang Jia <jiazhouyang09@gmail.com> Thu, Jun 14, 2018 at 9:22 AM
To: Andy Shevchenko <andy.shevchenko@gmail.com>
Cc: Anil Gurumurthy <anil.gurumurthy@qlogic.com>, Sudarsana Kalluru <sudarsana.kalluru@qlogic.com>, "James E.J. Bottomley" <jejb@linux.vnet.ibm.com>, "Martin K. Petersen" <martin.petersen@oracle.com>, linux-scsi <linux-scsi@vger.kernel.org>, Linux Kernel Mailing List <linux-kernel@vger.kernel.org>

2018-06-14 20:00 GMT+08:00 Andy Shevchenko <andy.shevchenko@gmail.com>:
> On Thu, Jun 14, 2018 at 2:57 PM, Zhouyang Jia <jiazhouyang09@gmail.com> wrote:
> > When pci_iomap fails, the lack of error-handling code may
> > cause unexpected results.
>
> What results?
> How had you tested it?

I reported this bug since more than 85% callsites of pci_iomap
are well handled in kernel. I guess there would be unexpected
results if missing error handling. I'm sorry I don't know what results.

> > This patch adds error-handling code after calling pci_iomap.
>
> > +   if (bfad->pci_bar2_kva == NULL) {
>
> > +   printk(KERN_ERR "Fail to map bar2\n");
>
> pr_err() ?

printk is used on the line before the fix, and I inherit the style.
I can change it to pr_err if necessary.

> > +   goto out_unmap_bar0;
> > +   }
>
> --
> With Best Regards,
> Andy Shevchenko

Best,
Zhouyang