

[PATCH 2 of 4] x86-64: Calgary IOMMU: deobfuscate calgary_init

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2006-09/msg09028.html>

- *From:* Muli Ben-Yehuda <muli@xxxxxxxxxx>
 - *Date:* Sat, 30 Sep 2006 11:43:30 +0300
-

1 files changed, 7 insertions(+), 5 deletions(-)
arch/x86_64/kernel/pci-calgary.c | 12 ++++++-----

```
# HG changeset patch
# User Muli Ben-Yehuda <muli@xxxxxxxxxx>
# Date 1159604311 -10800
# Node ID e0562474cf16b13d8c3c815fce3159ba7cd0f540
# Parent 28658cf477bc8c6adc5a5335363a4d1428f58273
x86-64: Calgary IOMMU: deobfuscate calgary_init
```

From: Jon Mason <jdmason@xxxxxxxx>

calgary_init's for loop does not correspond to the actual device being checked, which makes its upperbound check for array overflow useless. Changing this to a do-while loop is the correct way of doing this. There should be no possibility of spinning forever in this loop, as pci_get_device states that it will go through all iterations, then return NULL (thus breaking the loop).

Signed-off-by: Jon Mason <jdmason@xxxxxxxx>
Signed-off-by: Muli Ben-Yehuda <muli@xxxxxxxxxx>

```
diff -r 28658cf477bc -r e0562474cf16 arch/x86_64/kernel/pci-calgary.c
--- a/arch/x86_64/kernel/pci-calgary.c Sat Sep 30 11:16:12 2006 +0300
+++ b/arch/x86_64/kernel/pci-calgary.c Sat Sep 30 11:18:31 2006 +0300
@@ -817,6 +817,8 @@ static int __init calgary_init_one(struc
void __iomem *bbar;
int ret;
```

```
+ BUG_ON(dev->bus->number >= MAX_PHB_BUS_NUM);
+
address = locate_register_space(dev);
/* map entire 1MB of Calgary config space */
bbar = ioremap_nocache(address, 1024 * 1024);
@@ -843,10 +845,10 @@ done:
```

```
static int __init calgary_init(void)
```

```
{
- int i, ret = -ENODEV;
+ int ret = -ENODEV;
struct pci_dev *dev = NULL;

- for (i = 0; i < MAX_PHB_BUS_NUM; i++) {
+ do {
dev = pci_get_device(PCI_VENDOR_ID_IBM,
PCI_DEVICE_ID_IBM_CALGARY,
dev);
@@ -862,12 +864,12 @@ static int __init calgary_init(void)
ret = calgary_init_one(dev);
if (ret)
goto error;
- }
+ } while (1);

return ret;

error:
- for (i--; i >= 0; i--) {
+ do {
dev = pci_find_device_reverse(PCI_VENDOR_ID_IBM,
PCI_DEVICE_ID_IBM_CALGARY,
dev);
@@ -883,7 +885,7 @@ error:
calgary_disable_translation(dev);
calgary_free_bus(dev);
pci_dev_put(dev); /* Undo calgary_init_one()'s pci_dev_get() */
- }
+ } while (1);

return ret;
}
-
```

To unsubscribe from this list: send the line "unsubscribe linux-kernel" in the body of a message to majordomo@xxxxxxxxxxxxxxxxxxx
More majordomo info at <http://vger.kernel.org/majordomo-info.html>
Please read the FAQ at <http://www.tux.org/lkml/>