



author Suzuki K Poulose <suzuki.poulose@arm.com> 2025-04-22 17:16:16 +0100
committer Ingo Molnar <mingo@kernel.org> 2025-04-26 10:17:24 +0200
commit 3318dc299b072a0511d6dfd8367f3304fb6d9827 (patch)
tree 7c9544ee7d852b9c47c9ce19384498f045218067
parent 9d7a0577c9db35c4cc52db90bc415ea248446472 (diff)
download linux-3318dc299b072a0511d6dfd8367f3304fb6d9827.tar.gz

diff options

context:

3 ▼

space:

include ▼

mode:

unified ▼

irqchip/gic-v2m: Prevent use after free of gicv2m_get_fwnode()

With ACPI in place, gicv2m_get_fwnode() is registered with the pci subsystem as pci_msi_get_fwnode_cb(), which may get invoked at runtime during a PCI host bridge probe. But, the call back is wrongly marked as __init, causing it to be freed, while being registered with the PCI subsystem and could trigger:

```
Unable to handle kernel paging request at virtual address ffff8000816c0400
gicv2m_get_fwnode+0x0/0x58 (P)
pci_set_bus_msi_domain+0x74/0x88
pci_register_host_bridge+0x194/0x548
```

This is easily reproducible on a Juno board with ACPI boot.

Retain the function for later use.

Fixes: 0644b3daca28 ("irqchip/gic-v2m: acpi: Introducing GICv2m ACPI support")
Signed-off-by: Suzuki K Poulose <suzuki.poulose@arm.com>
Signed-off-by: Thomas Gleixner <tglx@linutronix.de>
Signed-off-by: Ingo Molnar <mingo@kernel.org>
Reviewed-by: Marc Zyngier <maz@kernel.org>
Cc: stable@vger.kernel.org

Diffstat

```
-rw-r--r-- drivers/irqchip/irq-gic-v2m.c 2
```

1 files changed, 1 insertions, 1 deletions

```
diff --git a/drivers/irqchip/irq-gic-v2m.c b/drivers/irqchip/irq-gic-v2m.c
index c6989486186667..dc98c39d2b2034 100644
```

```
--- a/drivers/irqchip/irq-gic-v2m.c
```

```
+++ b/drivers/irqchip/irq-gic-v2m.c
```

```
@@ -421,7 +421,7 @@ static int __init gicv2m_of_init(struct fwnode_handle *parent_handle,
#ifdef CONFIG_ACPI
static int acpi_num_msi;
```

```
-static __init struct fwnode_handle *gicv2m_get_fwnode(struct device *dev)
+static struct fwnode_handle *gicv2m_get_fwnode(struct device *dev)
{
    struct v2m_data *data;
```

