



author Chen Zhongjin <chenzhongjin@huawei.com> 2022-10-27 20:13:53 +0800
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2022-11-10 18:14:24 +0100
commit [bfd5e62f9a7ee214661cb6f143a3b40ccc63317f](#) (patch)
tree [00fe8a45efba330cb6565441474c7913a6f4ea63](#)
parent [fc3e2fa0a5fb432927fed3f2cdfda22c41340c16](#) (diff)
download [linux-bfd5e62f9a7ee214661cb6f143a3b40ccc63317f.tar.gz](#)

diff options

context: ▼
space: ▼
mode: ▼

i2c: piix4: Fix adapter not be removed in piix4_remove()

[Upstream commit 569bea74c94d37785682b11bab76f557520477cd]

In piix4_probe(), the piix4 adapter will be registered in:

```
piix4_probe()
    piix4_add_adapters_sb800() / piix4_add_adapter()
    i2c_add_adapter()
```

Based on the probed device type, piix4_add_adapters_sb800() or single piix4_add_adapter() will be called.

For the former case, piix4_adapter_count is set as the number of adapters, while for another case it is not set and kept default *zero*.

When piix4 is removed, piix4_remove() removes the adapters added in piix4_probe(), basing on the piix4_adapter_count value. Because the count is zero for the single adapter case, the adapter won't be removed and makes the sources allocated for adapter leaked, such as the i2c client and device.

These sources can still be accessed by i2c or bus and cause problems. An easily reproduced case is that if a new adapter is registered, i2c will get the leaked adapter and try to call smbus_algorithm, which was already freed:

Triggered by: `rmmod i2c_piix4 && modprobe max31730`

```
BUG: unable to handle page fault for address: ffffffff8053d860
#PF: supervisor read access in kernel mode
#PF: error_code(0x0000) - not-present page
Oops: 0000 [#1] PREEMPT SMP KASAN
CPU: 0 PID: 3752 Comm: modprobe Tainted: G
Hardware name: QEMU Standard PC (i440FX + PIIX, 1996)
RIP: 0010:i2c_default_probe (drivers/i2c/i2c-core-base.c:2259) i2c_core
RSP: 0018:ffff888107477710 EFLAGS: 00000246
```

...

<TASK>

```
i2c_detect (drivers/i2c/i2c-core-base.c:2302) i2c_core
__process_new_driver (drivers/i2c/i2c-core-base.c:1336) i2c_core
bus_for_each_dev (drivers/base/bus.c:301)
i2c_for_each_dev (drivers/i2c/i2c-core-base.c:1823) i2c_core
i2c_register_driver (drivers/i2c/i2c-core-base.c:1861) i2c_core
```

```
do_one_initcall (init/main.c:1296)
do_init_module (kernel/module/main.c:2455)
...
</TASK>
---[ end trace 0000000000000000 ]---
```

Fix this problem by correctly set piix4_adapter_count as 1 for the single adapter so it can be normally removed.

Fixes: 528d53a1592b ("i2c: piix4: Fix probing of reserved ports on AMD Family 16h Model 30h")
Signed-off-by: Chen Zhongjin <chenzhongjin@huawei.com>
Reviewed-by: Jean Delvare <jdelvare@suse.de>
Signed-off-by: Wolfram Sang <wsa@kernel.org>
Signed-off-by: Sasha Levin <sasha@kernel.org>

Diffstat

-rw-r--r--	drivers/i2c/busses/i2c-piix4.c	1
------------	--------------------------------	---

1 files changed, 1 insertions, 0 deletions

```
diff --git a/drivers/i2c/busses/i2c-piix4.c b/drivers/i2c/busses/i2c-piix4.c
index 8c1b31ed0c429a..aa1d3657ab4e69 100644
--- a/drivers/i2c/busses/i2c-piix4.c
+++ b/drivers/i2c/busses/i2c-piix4.c
@@ -961,6 +961,7 @@ static int piix4_probe(struct pci_dev *dev, const struct pci_device_id *id)
                                "", &piix4_main_adapters[0]);
        if (retval < 0)
            return retval;
+       piix4_adapter_count = 1;
    }

    /* Check for auxiliary SMBus on some AMD chipsets */
```