



author Zeng Heng <zengheng4@huawei.com> 2022-11-10 16:20:56 +0800
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2022-11-25 17:40:23 +0100
commit a988dcd3dd9e691c5ccc3324b209688f3b5453e9 (patch)
tree 7d16243a5c6ce636ffa90bfea58035d4cebaleac
parent dd0b9dac4ca995eeef48fefcc5bd9ac705745edf (diff)
download linux-a988dcd3dd9e691c5ccc3324b209688f3b5453e9.tar.gz

diff options

context:

3 ▼

space:

include ▼

mode:

unified ▼

pinctrl: devicetree: fix null pointer dereferencing in pinctrl_dt_to_map

[Upstream commit 91d5c5060ee24fe8da88cd585bb43b843d2f0dce]

Here is the BUG report by KASAN about null pointer dereference:

BUG: KASAN: null-ptr-deref in strcmp+0x2e/0x50
Read of size 1 at addr 0000000000000000 by task python3/2640
Call Trace:
strcmp
__of_find_property
of_find_property
pinctrl_dt_to_map

kasprintf() would return NULL pointer when kmalloc() fail to allocate.
So directly return ENOMEM, if kasprintf() return NULL pointer.

Fixes: 57291ce295c0 ("pinctrl: core device tree mapping table parsing support")
Signed-off-by: Zeng Heng <zengheng4@huawei.com>
Link: <https://lore.kernel.org/r/20221110082056.2014898-1-zengheng4@huawei.com>
Signed-off-by: Linus Walleij <linus.walleij@linaro.org>
Signed-off-by: Sasha Levin <sashal@kernel.org>

Diffstat

```
-rw-r--r-- drivers/pinctrl/devicetree.c 2
```

1 files changed, 2 insertions, 0 deletions

diff --git a/drivers/pinctrl/devicetree.c b/drivers/pinctrl/devicetree.c
index 177ee1136e3497..6f5acfcba57ce5 100644

--- a/drivers/pinctrl/devicetree.c

+++ b/drivers/pinctrl/devicetree.c

```
@@ -235,6 +235,8 @@ int pinctrl_dt_to_map(struct pinctrl *p, struct pinctrl_dev *pctldev)
     for (state = 0; ; state++) {
         /* Retrieve the pinctrl-* property */
         propname = kasprintf(GFP_KERNEL, "pinctrl-%d", state);
+
+         if (!propname)
+             return -ENOMEM;
         prop = of_find_property(np, propname, &size);
         kfree(propname);
         if (!prop) {
```