



author Kang Chen <void0red@gmail.com> 2023-02-27 17:30:37 +0800
committer Greg Kroah-Hartman <gregkh@linuxfoundation.org> 2023-03-17 08:30:37 +0100
commit [ad11b872bc9b5d27e56183c6b01f9218c85395d2](#) (patch)
tree [f32a98dd0140d580152e25d5c391adc43b7930a8](#)
parent [192027fe6a1cc4f88306de36d64b8e26b57efdab](#) (diff)
download [linux-ad11b872bc9b5d27e56183c6b01f9218c85395d2.tar.gz](#)

diff options

context:

3 ▼

space:

include ▼

mode:

unified ▼

nfc: fdp: add null check of devm_kmalloc_array in fdp_nci_i2c_read_device_properties

[Upstream commit 11f180a5d62a51b484e9648f9b310e1bd50b1a57]

devm_kmalloc_array may fails, *fw_vsc_cfg might be null and cause out-of-bounds write in device_property_read_u8_array later.

Fixes: [a06347c04c13](#) ("NFC: Add Intel Fields Peak NFC solution driver")

Signed-off-by: Kang Chen <void0red@gmail.com>

Reviewed-by: Krzysztof Kozłowski <krzysztof.kozłowski@linaro.org>

Reviewed-by: Simon Horman <simon.horman@corigine.com>

Link: <https://lore.kernel.org/r/20230227093037.907654-1-void0red@gmail.com>

Signed-off-by: Paolo Abeni <pabeni@redhat.com>

Signed-off-by: Sasha Levin <sashal@kernel.org>

Diffstat

```
-rw-r--r-- drivers/nfc/fdp/i2c.c 4
```

1 files changed, 4 insertions, 0 deletions

diff --git a/drivers/nfc/fdp/i2c.c b/drivers/nfc/fdp/i2c.c

index 4020c11a9415b8..3c543981ea180e 100644

--- a/drivers/nfc/fdp/i2c.c

+++ b/drivers/nfc/fdp/i2c.c

```
@@ -263,6 +263,9 @@ static void fdp_nci_i2c_read_device_properties(struct device *dev,  
                                len * sizeof(**fw_vsc_cfg),  
                                GFP_KERNEL);
```

```
+                if (!*fw_vsc_cfg)  
+                    goto alloc_err;  
+
```

```
        r = device_property_read_u8_array(dev, FDP_DP_FW_VSC_CFG_NAME,  
                                *fw_vsc_cfg, len);
```

```
@@ -276,6 +279,7 @@ vsc_read_err:  
        *fw_vsc_cfg = NULL;  
    }
```

+alloc_err:

```
    dev_dbg(dev, "Clock type: %d, clock frequency: %d, VSC: %s",  
            *clock_type, *clock_freq, *fw_vsc_cfg != NULL ? "yes" : "no");
```

```
}
```

