From Yang Yingliang <>
Subject [PATCH] serial: 8250: fix null-ptr-deref in serial8250_start_tx()
Date Tue, 21 Jul 2020 14:38:52 +0000

```
I got null-ptr-deref in serial8250_start_tx():

[   78.114630] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000
[   78.123778] Mem abort info:
[   78.126560]   ESR = 0x86000007
[   78.129603]   EC = 0x21: IABT (current EL), IL = 32 bits
[   78.134891]   SET = 0, FnV = 0
[   78.137933]   EA = 0, S1PTW = 0
[   78.141064] user pgtable: 64k pages, 48-bit VAs, pgdp=00000027d41a8600
[   78.147562] [0000000000000000] pgd=0000027893f0003, p4d=0000027893f0003, pud=0000027893f0003, pmd=00000027c9a20003, pte=0000000000000000
[   78.160029] Internal error: Oops: 86000007 [#1] SMP
[   78.164886] Modules linked in: sunrpc vfat fat aes_ce_blk crypto_simd cryptd aes_ce_cipher crct10dif_ce ghash_ce sha2_ce sha256_arm64 sha1_ce ses enclosure sg sbsa_gwdt ipmi_ssif spi_dw_mmio sch_fq_codel vhost_net tun vhost vhost_iotlb tap ip_tables ext4 mbcach
[   78.207383] CPU: 11 PID: 23258 Comm: null-ptr Not tainted 5.8.0-rc6+ #48
[   78.214056] Hardware name: Huawei TaiShan 2280 V2/BC82AMDC, BIOS 2280-V2 CS V3.B210.01 03/12/2020
[   78.222888] pstate: 80400089 (Nzcv daIf +PAN -UAO BTYPE=--)
[   78.228435] pc : 0x0
[   78.230618] lr : serial8250_start_tx+0x160/0x260
[   78.235215] sp : ffff800062eefb80
[   78.238517] x29: ffff800062eefb80 x28: 0000000000000fff
[   78.243807] x27: ffff800062eefd80 x26: ffff202fd83b3000
[   78.249098] x25: ffff800062eefd80 x24: ffff202fd83b3000
[   78.254388] x23: ffff002fc5e50be8 x22: 0000000000000002
[   78.259679] x21: 0000000000000001 x20: 0000000000000000
[   78.264969] x19: ffffa688827eecc8 x18: 0000000000000000
[   78.270259] x17: 0000000000000000 x16: 0000000000000000
[   78.275550] x15: ffffa68881bc67a8 x14: 00000000000002e6
[   78.280841] x13: ffffa68881bc67a8 x12: 000000000000c539
[   78.286131] x11: d37a6f4de9bd37a7 x10: ffffa68881cccff0
[   78.291421] x9 : ffffa68881bc6000 x8 : ffffa688819daa88
[   78.296711] x7 : ffffa688822a0f20 x6 : ffffa688819e0000
[   78.302002] x5 : ffff800062eef9d0 x4 : ffffa68881e707a8
[   78.307292] x3 : 0000000000000000 x2 : 0000000000000002
[   78.312582] x1 : 0000000000000001 x0 : ffffa688827eecc8
[   78.317873] Call trace:
[   78.320312]  0x0
[   78.322147]  __uart_start.isra.9+0x64/0x78
[   78.326229]  uart_start+0xb8/0x1c8
[   78.329620]  uart_flush_chars+0x24/0x30
[   78.333442]  n_tty_receive_buf_common+0x7b0/0xc30
[   78.338128]  n_tty_receive_buf+0x44/0x2c8
[   78.342122]  tty_ioctl+0x348/0x11f8
[   78.345599]  ksys_ioctl+0xd8/0xf8
[   78.348903]  __arm64_sys_ioctl+0x2c/0xc8
[   78.352812]  el0_svc_common.constprop.2+0x88/0x1b0
[   78.357583]  do_el0_svc+0x44/0xd0
[   78.360887]  el0_sync_handler+0x14c/0x1d0
[   78.364880]  el0_sync+0x140/0x180
[   78.368185] Code: bad PC value

SERIAL_PORT_DFNS is not defined on each arch, if it's not defined,
serial8250_set_defaults() won't be called in serial8250_isa_init_ports(),
so the p->serial_in pointer won't be initialized, and it leads a null-ptr-deref.
Fix this problem by calling serial8250_set_defaults() after init uart port.

Signed-off-by: Yang Yingliang <yangyingliang@huawei.com>
---
 drivers/tty/serial/8250/8250_core.c | 2 +-
 1 file changed, 1 insertion(+), 1 deletion(-)

diff --git a/drivers/tty/serial/8250/8250_core.c b/drivers/tty/serial/8250/8250_core.c
index fc118f649887..cae61d1ebec5 100644
--- a/drivers/tty/serial/8250/8250_core.c
+++ b/drivers/tty/serial/8250/8250_core.c
@@ -524,6 +524,7 @@ static void __init serial8250_isa_init_ports(void)
                 */
                up->mcr_mask = ~ALPHA_KLUDGE_MCR;
                up->mcr_force = ALPHA_KLUDGE_MCR;
+               serial8250_set_defaults(up);
        }

        /* chain base port ops to support Remote Supervisor Adapter */
@@ -547,7 +548,6 @@ static void __init serial8250_isa_init_ports(void)
                port->membase  = old_serial_port[i].iomem_base;
                port->iotype   = old_serial_port[i].io_type;
                port->regshift = old_serial_port[i].iomem_reg_shift;
-               serial8250_set_defaults(up);

                port->irqflags |= irqflag;
                if (serial8250_isa_config != NULL)
--
2.25.1
```