# coreboot - Bug #154

## mainboard: via: epia-m700: NULL pointer dereference (if SeaBIOS is payload)

01/19/2018 12:03 PM - Martin Kepplinger

| | | | |
|---|---|---|---|
| **Status:** | New | **Start date:** | 01/19/2018 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | | **% Done:** | 0% |
| **Category:** | board support | **Estimated time:** | 1.00 hour |
| **Target version:** | | | |

**Description**

If you have a look at the following part of mainboard/via/epia-m700/wakeup.c
some bells must ring.

```
#if PAYLOAD_IS_SEABIOS == 1
    /* WAKE_MEM_INFO inited in get_set_top_available_mem in tables.c. */
    src =
        (unsigned char *)((*(u32 *) WAKE_MEM_INFO) - 64 * 1024 - 0x100000);
    dest = 0;

    /*
     * If recovered 0-e0000, then when resume, before WinXP turn on the
     * desktop screen, there is gray background which last 1sec.
     */
    for (i = 0; i < 0xa0000; i++)
            dest[i] = src[i];
```