Re: [PATCH] hw/net/e1000e: advance desc_offset in case of null descripto

From: Jason Wang
Subject: Re: [PATCH] hw/net/e1000e: advance desc_offset in case of null descriptor
Date: Thu, 12 Nov 2020 13:51:32 +0800
User-agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Thunderbird/68.10.0

On 2020/11/11 下午9:06, P J P wrote:

> ```
> From: Prasad J Pandit <pjp@fedoraproject.org>
>
> While receiving packets via e1000e_write_packet_to_guest() routine,
> 'desc_offset' is advanced only when RX descriptor is processed. And
> RX descriptor is not processed if it has NULL buffer address.
> This may lead to an infinite loop condition. Increament 'desc_offset'
> to process next descriptor in the ring to avoid infinite loop.
>
> Reported-by: Cheol-woo Myung <330cjfdn@gmail.com>
> Signed-off-by: Prasad J Pandit <pjp@fedoraproject.org>
> ---
>   hw/net/e1000e_core.c | 8 ++++----
>   1 file changed, 4 insertions(+), 4 deletions(-)
>
> diff --git a/hw/net/e1000e_core.c b/hw/net/e1000e_core.c
> index bcfd46696f..3b096db3a4 100644
> --- a/hw/net/e1000e_core.c
> +++ b/hw/net/e1000e_core.c
> @@ -1596,13 +1596,13 @@ e1000e_write_packet_to_guest(E1000ECore *core, struct
> NetRxPkt *pkt,
>                              (const char *) &fcs_pad, e1000x_fcs_len(core->mac));
>                   }
>               }
> -            desc_offset += desc_size;
> -            if (desc_offset >= total_size) {
> -                is_last = true;
> -            }
>           } else { /* as per intel docs; skip descriptors with null buf addr */
>               trace_e1000e_rx_null_descriptor();
>           }
> +        desc_offset += desc_size;
> +        if (desc_offset >= total_size) {
> +            is_last = true;
> +        }
> e1000e_write_rx_descr(core, desc, is_last ? core->rx_pkt : NULL,
>                               rss_info, do_ps ? ps_hdr_len : 0,
> &bastate.written);
> ```

Applied.

Thanks

reply via email to
Jason Wang

[Prev in Thread] **Current Thread** [Next in Thread]

- **[PATCH] hw/net/e1000e: advance desc_offset in case of null descriptor**, *P J P*, 2020/11/11
  - **Re: [PATCH] hw/net/e1000e: advance desc_offset in case of null descriptor**, *Jason Wang* <=

- Prev by Date: **Re: [PATCH-for-5.2 v2] hw/i386/acpi-build: Fix maybe-uninitialized error when ACPI hotplug off**
- Next by Date: **Re: [PATCH] net: do not exit on "netdev_add help" monitor command**
- Previous by thread: **[PATCH] hw/net/e1000e: advance desc_offset in case of null descriptor**
- Next by thread: **[PATCH 0/2] char: Deprecate backend aliases**
- Index(es):
  - **Date**
  - **Thread**