No checking if ep_descriptor->wMaxPacketSize is greater than zero #81

Closed **TheSilentDawn** opened this issue on Oct 14, 2020 · 2 comments

Assignees	
Labels	enhancement internal bug tracker mw usb
Projects	stm32cube-mcu-fw-dashb...
Milestone	v1.10.0

TheSilentDawn commented on Oct 14, 2020

Describe the set-up

- Software:
  - STM32Cube MCU & MPU Packages
- Version:
  - STM32Cube_FW_H7_V1.8.0
- Verification Hardware Platform:
  - STM32H7B3

Describe the bug

- Function:
  - static void USBH_ParseEPDesc(USBH_EpDescTypeDef *ep_descriptor, uint8_t *buf)
- Location:
  - STM32CubeH7/Middlewares/ST/STM32_USB_Host_Library/Core/Src/usbh_ctlreq.c
    Line 470 in 79196b0

    ```
    470      ep_descriptor->wMaxPacketSize   = LE16(buf + 4);
    ```
- Type:
  - Denial-of-Service.
- Result:
  - The system will hang when try to communicate with the endpoint.
- Description:
  - The function USBH_ParseEPDesc parses the endpoint descriptor of a USB device.
  - It doesn't check if the variable ep_descriptor->wMaxPacketSize is greater than zero as shown in

    STM32CubeH7/Middlewares/ST/STM32_USB_Host_Library/Core/Src/usbh_ctlreq.c
    Line 470 in 79196b0

    ```
    470      ep_descriptor->wMaxPacketSize   = LE16(buf + 4);
    ```

    . If zero, the MSC handler will not able to communicate with the outside world as shown from line 180 to line 200 in https://github.com/STMicroelectronics/STM32CubeH7/blob/79196b09acfb720589f58e93ccf956401b18a191/Middlewares/ST/STM32_USB_Host_Library/Class/MSC/Src/usbh_msc.c

How To Reproduce

1. Running MSC_Standalone application on the STM32H7B3I platform

2. Plug a USB disk

3. Use the attached Bug7.txt to replace the USB device packet.
   Bug7.txt

Additional context

- To patch it, the program should check if ep_descriptor->wMaxPacketSize is greater than zero.

ALABSTM added this to **To do** in **stm32cube-mcu-fw-dashboard** on Oct 15, 2020

ALABSTM self-assigned this on Nov 2, 2020

ALABSTM added the mw label on Nov 2, 2020

ALABSTM moved this from **To do** to **Assigned** in **stm32cube-mcu-fw-dashboard** on Dec 2, 2020

ALABSTM added the usb label on Jan 18, 2021

ALABSTM moved this from **Assigned** to **In progress** in **stm32cube-mcu-fw-dashboard** on Jan 18, 2021

ALABSTM added **enhancement** **internal bug tracker** labels on Jan 18, 2021

ALABSTM commented on Jan 18, 2021 Contributor

ST Internal Reference: 99173

ALABSTM added this to the **v1.10.0** milestone on Feb 22, 2021

ALABSTM moved this from **In progress** to **To release** in **stm32cube-mcu-fw-dashboard** on Feb 22, 2021

TheSilentDawn mentioned this issue on May 31, 2021

No validity chekcing on the variable dev_desc->bMaxPacketSize #75

Closed

ALABSTM commented on Mar 14 Contributor

Hi **@TheSilentDawn**,

Hope you're fine. Just to inform you the fix has been published in the frame of **v1.10.0** release.

With regards,

ALABSTM closed this as completed on Mar 14

stm32cube-mcu-fw-dashboard automation moved this from **To release** to **Done** on Mar 14

Assignees

ALABSTM

Labels

enhancement internal bug tracker mw usb

Projects

stm32cube-mcu-fw-dashboard

Done

Milestone

v1.10.0

Development

No branches or pull requests

2 participants