STMicroelectronics / **STM32CubeH7** Public

New issue

Jump to bottom

No checking on both IN and OUT pipe constructed #80

Closed **TheSilentDawn** opened this issue on Oct 14, 2020 · 5 comments

Assignees	
Labels	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 USBH_StatusTypeDef USBH_MSC_InterfaceInit(USBH_HandleTypeDef *phost)
- Location:
  - 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
- Type:
  - Denial-of-Service.
- Result:
  - The system will hang when try to communicate with the endpoint.
- Description:
  - The function USBH_MSC_InterfaceInit() inits the status of MSC handler. It initializes the IN endpoint and OUT endpoint 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.
  - However, when the variable bEndpointAddress of endpoint descriptor are both masked as IN or OUT without checking as shown in

    STM32CubeH7/Middlewares/ST/STM32_USB_Host_Library/Core/Src/usbh_ctlreq.c
    Line 468 in 79196b0

    ```
    468      ep_descriptor->bEndpointAddress = *(uint8_t *)(buf + 2);
    ```

    , the MSC handler will also only initialize the IN or OUT part 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 Bug6.txt to replace the USB device packet.
   Bug6.txt

Additional context

- To patch it, the program should check both IN and OUT pipe is constructed.

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 commented on Nov 24, 2020 Contributor

Hi **@TheSilentDawn**,

Thank you for this other report. To be sure I understood your point, please allow me these questions:

- We are dealing with the case of a **simultaneously** IN and OUT endpoint? This is what I understood from the expression *"the variable bEndpointAddress of endpoint descriptor are both masked as IN or OUT"*.
- We are requesting from the software to check both? This is what I understood from the expression *"the program should check **both** IN and OUT pipe is constructed"*

Thank you in advance for your clarifications.

With regards,

TheSilentDawn commented on Nov 25, 2020 • edited ▾ Author

Hi @ALABSTM,
Yes, the firmware should open an IN pipe and an OUT pipe to communicate with a device normally. However, as the report described, the driver codes do not check this. It will open two IN pipes or two OUT pipes unexpectedly which will block the communication in the subsequent execution of the firmware. If anything not clear, please let me know. Thanks for your help.^_^

ALABSTM commented on Dec 2, 2020 • edited ▾ Contributor

Hi @TheSilentDawn,

Thank you for the clarification. Hence, the case you are describing is an interface exposing 2x IN endpoints **or** 2x OUT endpoints **instead of** 1x IN endpoint and 1x OUT endpoint (which is the normal case for a **MSC**).

I will forward your report to our development teams. I will get back to you as soon as they provide me with their feedback.

With regards,

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 the **internal bug tracker** label 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

internal bug tracker mw usb

Projects

stm32cube-mcu-fw-dashboard

Done

Milestone

v1.10.0

Development

No branches or pull requests

2 participants