

New issue

Jump to bottom

No validity checking on the variable `cfg_desc->wTotalLength` #76

Closed TheSilentDawn opened this issue on Oct 14, 2020 · 3 comments

Assignees

Labels enhancement internal bug tracker mw usb

Projects stm32cube-mcu-fw-dashb...

Milestone v1.10.0

TheSilentDawn commented on Oct 14, 2020 · edited

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_ParseCfgDesc(USBH_CfgDescTypeDef *cfg_desc, uint8_t *buf, uint16_t length)
- Location:
 - STM32CubeH7/Middlewares/ST/STM32_USB_Host_Library/Core/usbh_ctreq.c
Line 395 in 79196b0

395 cfg_desc->wTotalLength = LE16(buf + 2);
- Type:
 - Buffer Overflow
- Result:
 - The system could be configured incorrectly with wrong parameters.
- Description:
 - The function USBH_ParseCfgDesc() parses the configuration descriptor, interface descriptor, and endpoint descriptor by input data from a USB device.
 - However, it doesn't check the validity of the variable `cfg_desc->wTotalLength` compared with the total length of the input buffer as shown in

STM32CubeH7/Middlewares/ST/STM32_USB_Host_Library/Core/usbh_ctreq.c
Line 395 in 79196b0

395 cfg_desc->wTotalLength = LE16(buf + 2);

. This will cause the following program including calling to the function USBH_GetNextDesc(), USBH_ParseInterfaceDesc() and USBH_ParseEPDesc() configure the system incorrectly.

How To Reproduce


- Running MSC_Standalone application on the STM32H7B3I platform
- Plug a USB disk
- Use the attached Bug2.txt to replace the USB device packet. [Bug2.txt](#)

Additional context

- To patch it, the program should check if reach the end of the input buffer when plus `cfg_desc->wTotalLength`.

- 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 enhancement label on Dec 15, 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

CHAMSTM commented on Jul 26, 2021

Already fixed in USBH V3.4.0


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

3 participants

