New issue

Jump to bottom

Buffer Overflow due to the variable if_descriptor->bLength #83

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 • 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_ParseInterfaceDesc(USBH_InterfaceDescTypeDef *if_descriptor, uint8_t *buf)
- Location:
  - STM32CubeH7/Middlewares/ST/STM32_USB_Host_Library/Core/Src/usbh_ctlreq.c
    Line 444 in 79196b0

```
444     if_descriptor->bLength            = *(uint8_t *)(buf + 0);
```

- Type:
  - Buffer Overflow
- Result:
  - The system could be configured incorrectly with wrong parameters.
- Description:
  - The function USBH_ParseInterfaceDesc() parse interface descriptor. It's called by the function USBH_ParseCfgDesc() as shown in

    STM32CubeH7/Middlewares/ST/STM32_USB_Host_Library/Core/Src/usbh_ctlreq.c
    Line 413 in 79196b0

```
413     USBH_ParseInterfaceDesc(pif, (uint8_t *)(void *)pdesc);
```

    .
  - It doesn't check the validity of the variable if_descriptor->bLength compared with the total length of the input buffer which may cause a buffer overflow by the following called function USBH_GetNextDesc() as shown in

    STM32CubeH7/Middlewares/ST/STM32_USB_Host_Library/Core/Src/usbh_ctlreq.c
    Line 419 in 79196b0

```
419     pdesc = USBH_GetNextDesc((uint8_t *)(void *)pdesc, &ptr);
```

    .

How To Reproduce

1. Running MSC_Standalone application on the STM32H7B3I platform
2. Plug a USB disk
3. Use the attached Bug9.txt to replace the USB device packet. Bug9.txt

Additional context

- To patch it, the program should check if reach the end of the input buffer when plus if_descriptor->bLength.

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

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