STMicroelectronics / **STM32CubeH7** Public

Code · **Issues** 40 · Pull requests 4 · Actions · Projects · Security · ...

New issue

Jump to bottom

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

Closed **TheSilentDawn** opened this issue on Oct 14, 2020 · 12 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_ParseDevDesc(USBH_DevDescTypeDef *dev_desc, uint8_t *buf, uint16_t length)
- Location:
  - STM32CubeH7/Middlewares/ST/STM32_USB_Host_Library/Core/Src/usbh_ctlreq.c
    Line 355 in 79196b0

    ```
    355      dev_desc->bMaxPacketSize      = *(uint8_t *)(buf +  7);
    ```
- Type:
  - Denial-of-Service.
- Result:
  - A malformed USB device packet may cause the system to hang when it tries to communicate with the outside world.
- Description:
  - The function USBH_ParseDevDesc() parses the device descriptor by input data from a USB device.
  - The valid max packet size of the device descriptor should be 8, 16, 32, and 64 as USB specification required. However, the function USBH_ParseDevDesc() doesn't check the value of dev_desc->bMaxPacketSize as shown in

    STM32CubeH7/Middlewares/ST/STM32_USB_Host_Library/Core/Src/usbh_ctlreq.c
    Line 355 in 79196b0

    ```
    355      dev_desc->bMaxPacketSize      = *(uint8_t *)(buf +  7);
    ```

    . The variable dev_desc->bMaxPacketSize will be used as the size to construct the control pipe between host and device as shown in

    STM32CubeH7/Middlewares/ST/STM32_USB_Host_Library/Core/Src/usbh_core.c
    Line 828 in 79196b0

    ```
    828      phost->Control.pipe_size = phost->device.DevDesc.bMaxPacketSize;
    ```

    . If bMaxPacketSize is zero, the firmware will get the error status USBH_FAIL in the function USBH_HandleControl() called by the function USBH_CtlReq() when trying to communicate with the outside world by IN and OUT pipe in the future and the host will try to re-enumerate. This process will loop again and again.

How To Reproduce

1. Running MSC_Standalone application on the STM32H7B3I platform
2. Plug a USB disk
3. Use the attached Bug1.txt to replace the USB device packet. Bug1.txt

Additional context

- To patch it, the program should check if dev_desc->bMaxPacketSize is equal to 8, 16, 32 or 64. At least, it should be greater than zero.

TheSilentDawn changed the title ~~No validity chekcing on dev_desc->bMaxPacketSize~~ **No validity chekcing on the variable dev_desc->bMaxPacketSize** on Oct 14, 2020

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

ALABSTM added the mw label on Nov 2, 2020

ALABSTM self-assigned this on Nov 2, 2020

ALABSTM commented on Nov 24, 2020 Contributor

Hi **@TheSilentDawn**,

Thank you for your interest in our products and software solutions. Thank you also for this report and for all the other ones. They will be transmitted to our development teams for analysis.

However, may I first ask you whether these cases you are reporting (or at least some of them) are real error cases you faced while using our library or simulated test cases you designed based on a code review? Thank you in advance for your answer.

With regards,

ALABSTM added the **enhancement** label on Nov 24, 2020

TheSilentDawn commented on Nov 25, 2020 • edited Author

Hi, **@ALABSTM**,
All the vulnerabilities reported are discovered by the research work of our team. We are building an automatic method to find the bugs. And all the testcases are checked manually before reporting to make sure it could be leveraged by the attackers. Also, these vulnerabilities could be patched as described in the **Addition context** part. Could you please share an email? When our paper is ready for submission, I will let you know and share the draft with you asap. Thanks for your help.^_^

👍 1

ALABSTM commented on Dec 2, 2020 Contributor

Hi **@TheSilentDawn**,

Thank you for your contribution. All the reports you sent will be forwarded to our development teams. I will get back to you as soon as they provide me with their feedback.

Thank you again for your contribution and thank you in advance for your patience.

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 commented on Jan 18, 2021 Contributor

Hi **@TheSilentDawn**,

I hope you are doing well. Our technical committee discussed the several points you reported. Actions will be taken to make the necessary updates. I will keep you informed.

Any news or progress from your side? Thank you for your answer and thank you once more for your contribution.

With regards,

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 commented on May 31, 2021 • edited Author

@ALABSTM @CCASTM @Tombana @RKOUSTM
Hello Sir/Madam,

I'm a Ph.D. student from the University of Chinese Academy of Sciences and the University of Georgia. We are working on a fuzzing tool for automatic bug discovery. In the past year, I have reported several bugs that influence the MCU product line of STMicroelectronics. Some other STMicroelectronics engineers and your team have confirmed with us and the reported bugs have been patched. Currently, we are working on a research paper that systematically describes our new method. I wonder if your team can help apply for CVE IDs for these bugs so that we can refer to these CVE IDs and state our responsible disclosure with confidence.

Thanks for your help. If you want, we can also send you a draft of our paper before submission so that you can check whether the wording is appropriate. Below is a list of relevant bugs we reported.

[STM PLC]
https://community.st.com/s/question/0D53W00000BKF70SAH/stmplc-bug1
https://community.st.com/s/question/0D53W00000BKF7PSAX/stmplc-bug2
https://community.st.com/s/question/0D53W00000BKF7QSAX/stmplc-bug3
https://community.st.com/s/question/0D53W00000BKF8rSAH/stmplc-bug4
https://community.st.com/s/question/0D53W00000BKF8sSAH/stmplc-bug5
https://community.st.com/s/question/0D53W00000BKF9uSAH/stmplc-bug6
https://community.st.com/s/question/0D53W00000BKGAMSA5/stmplc-bug7
https://community.st.com/s/question/0D53W00000BKGANSA5/stmplc-bug8
https://community.st.com/s/question/0D53W00000BKGJWSA5/stmplc-bug9
[STM32 SDK USB Driver]
#75
#76
#77
#78
#79
#80
#81
#82
#83
#84

We look forwards to your reply.

Sincerely,
Wenqiang Li
Email: wenqiang-li@outlook.com, liwenqiang@iie.ac.cn

👍 2

ALABSTM commented on Jun 22, 2021 Contributor

Hello **@TheSilentDawn**,

You request will be reported to our development team to see whether it is possible to address it. However, as the PLC-related list of posts on the ST Community has not been confirmed yet, I can only formulate the request for the USB-related list you reported on this repository. I will keep you informed should there be any news.

Please try to contact the ST Community administrators to ask for a feedback about the PLC-related list of potential vulnerabilities.

With regards,

TheSilentDawn commented on Jun 22, 2021 • edited Author

Hi **@ALABSTM** ,
Thanks for your help and advice.

TheSilentDawn commented on Oct 20, 2021 • edited Author

Hi **@ALABSTM**
How about the CVE requesting process? Our research paper needs CVE ID support.
And we find more bugs in the STM32 MCU package. Should we report it here or email them to you?

CHAMSTM commented on Nov 15, 2021

> Hi **@ALABSTM** How about the CVE requesting process? Our research paper needs CVE ID support. And we find more bugs in the STM32 MCU package. Should we report it here or email them to you?

Hello,
Our Security Support team is trying to create CVE IDs and will share them asap.

Kind Regards,

CHAMSTM commented on Nov 15, 2021

Issue fixed in USB Host 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