STM32Cube software USB driver buffer overflow issues

Overview

This security advisory pertains to the STM32Cube software USB hardware abstraction layer (HAL) peripheral control driver (PCD) setup and data buffer overflow issues and potential security impacts.

Affected products

Product(1)	Version	Type	Note
STM32CubeC0	V1.3.0 and earlier *Note: Because the issue might not be fixed in subsequent version, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	-
STM32CubeF0	V1.11.5 and earlier *Note: Because the issue might not be fixed in subsequent version, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	-
STM32CubeF1	V1.8.6 and earlier *Note: Because the issue might not be fixed in subsequent version, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	-
STM32CubeF3	V1.11.5 and earlier *Note: Because the issue might not be fixed in subsequent version, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	-
STM32CubeL0	V1.12.2 and earlier *Note: Because the issue might not be fixed in subsequent version, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	-
STM32CubeL1	V1.10.4 and earlier *Note: Because the issue might not be fixed in subsequent version, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	-
STM32CubeL4	V1.18.1 and earlier *Note: Because the issue might not be fixed in subsequent version, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	-
STM32CubeL5	V1.5.1 and earlier *Note: Because the issue might not be fixed in subsequent version, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	-
STM32CubeWB	V1.21.0 and earlier *Note: Because the issue might not be fixed in subsequent version, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	-
STM32CubeG4	V1.6.1 and earlier *Note: Because the issue might not be fixed in subsequent version, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	-
STM32CubeG0	V1.6.2 and earlier *Note: Because the issue might not be fixed in subsequent version, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	-
STM32CubeU5	V1.7.0 and earlier *Note: Because the issue might not be fixed in subsequent version, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	-

Product[1]	Version	Type	Note
STM32CubeH5	V1.4.0 and earlier *Note: Because the issue might not be fixed in subsequent version, refer to the release notes[2] of the **affected product** to check if the issue has been fixed.*	Embedded software	-
STM32CubeU0	V1.2.0 and earlier *Note: Because the issue might not be fixed in subsequent version, refer to the release notes[2] of the **affected product** to check if the issue has been fixed.*	Embedded software	-
STM32CubeU3	V1.0.0 *Note: Because the issue might not be fixed in subsequent version, refer to the release notes[2] of the **affected product** to check if the issue has been fixed.*	Embedded software	-

1. *Some other STM32Cube expansion packages or function packages (X-CUBE, I-CUBE, STSW, FPs) could depend on the **affected products** and are not mentioned in this document. Check if STM32Cube expansion packages or function packages you use contain the **affected products**. If so, refer to the package release note to check if the issue has been fixed.*
2. *Release notes are available in each downloaded package (on www.st.com product pages, on STMicroelectronics Github product pages, and via STM32CubeMX).*

To know if the problem is fixed in a version of the STM32Cube firmware package or the STM32 X-CUBE firmware package, check if “SA0035” is mentioned in the release note of the HAL software component as stated in the following table:

Software component relative path[1]	File to read	Version fixing the vulnerabilities
./Drivers/STM32YYxx_hal_driver/	Release_Notes.html	Contains note “SA0035 fixed”

1. *“YY” corresponds to the STM32 series used*

Description

PCD setup and data buffer overflow in the USB HAL for the ***affected products*** can lead to data corruption.

Impact

PCD setup buffer overflow can lead to a potential unexpected behavior of the application.

PCD data buffer overflow can lead to an attacker-controlled out-of-bound write, allowing the attacker to corrupt memory and execute arbitrary code if the application does not protect SRAMs against code execution.

Remediation

To remediate the PCD setup buffer overflow issue, add checks inside the `PCD_EP_ISR_Handler` function to ensure that the amount of data to read does not exceed the setup buffer size. Only allow read operations with the full transfer size fitting the buffer size.

To remediate the PCD data buffer overflow issue, move the receive buffer incrementation from the USB driver (inside `PCD_EP_ISR_Handler` function) to the application. The application software must manage the buffer correctly to avoid any overflow.

Credit

Felix Buchmann at fuzzware.io

Tobias Scharnowski at fuzzware.io

Simon Wörner at fuzzware.io

Contact information

psirt@st.com

Revision history

Table 1. **Document revision history**

Date	Version	Changes
19-Feb-2025	1	Initial release.

IMPORTANT NOTICE – READ CAREFULLY

The STMicroelectronics group of companies (ST) places a high value on product security, and strives to continuously improve its products. However, no level of security certification and/or built-in security measures can guarantee that ST products are resistant to all forms of attack including, for example, against advanced attacks which have not been tested for, against new or unidentified forms of attack, or against any form of attack when using an ST product outside of its specification or intended use, or in conjunction with other components or software which are used by a customer to create their end product or application. As such, regardless of the incorporated security features and/or any information or support that may be provided by ST, each customer is responsible for determining if the level of security protection in and ST product meets their needs, both in relation to the ST product alone and when incorporated into a customer end product or application.

ST Technical Notes, security bulletins, security advisories, and the like (including suggested mitigations), and security features of ST products (inclusive of any hardware, software, documentation, and the like), together with any enhanced security features added by ST and any technical assistance and/or recommendations provided by ST, are provided on an "AS IS" BASIS. AS SUCH, TO THE EXTENT PERMITTED BY APPLICABLE LAW, ST DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, unless the applicable written and signed contract terms specifically provide otherwise.

ST reserves the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Customer should obtain the latest relevant information on ST products before placing orders.

Customers are solely responsible for the choice, selection, and use of ST products, and ST assumes no liability for application assistance or the design of customers' products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.