STM32Cube *USB Device* library potential issues

Overview

This security advisory pertains to potential issues of the *USB Device* library of STM32Cube.

One potential vulnerability affects the *USB Device* library *Core* software component. Another affects the *MSC* class driver. A third potential vulnerability applies when a customer uses the *MTP* class driver with an STM32 USB HS instance.

Affected products

Product(1)	Version	Type	Note
STM32CubeF0	1.11.6 and earlier *Note: Because the issue might not be fixed in subsequent release, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	Affected by the *Core* software component vulnerability and the *MSC* class driver vulnerability, listed in Description.
STM32CubeF1	1.8.7 and earlier *Note: Because the issue might not be fixed in subsequent release, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	Affected by the *Core* software component vulnerability and the *MSC* class driver vulnerability, listed in Description.
STM32CubeF2	1.9.6 and earlier *Note: Because the issue might not be fixed in subsequent release, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	Affected by the three vulnerabilities listed in Description.
STM32CubeF3	1.11.6 and earlier *Note: Because the issue might not be fixed in subsequent release, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	Affected by the *Core* software component vulnerability and the *MSC* class driver vulnerability, listed in Description.
STM32CubeF4	1.28.3 and earlier *Note: Because the issue might not be fixed in subsequent release, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	Affected by the three vulnerabilities listed in Description.
STM32CubeF7	1.17.4 and earlier *Note: Because the issue might not be fixed in subsequent release, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	Affected by the three vulnerabilities listed in Description.
STM32CubeG0	1.6.3 and earlier *Note: Because the issue might not be fixed in subsequent release, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	Affected by the *Core* software component vulnerability and the *MSC* class driver vulnerability, listed in Description.
STM32CubeG4	1.6.2 and earlier *Note: Because the issue might not be fixed in subsequent release, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	Affected by the *Core* software component vulnerability and the *MSC* class driver vulnerability, listed in Description.
STM32CubeH7	1.13.0 and earlier *Note: Because the issue might not be fixed in subsequent release, refer to the release notes(2) of the **affected product** to check if the issue has been fixed.*	Embedded software	Affected by the three vulnerabilities listed in Description.

Product[1]	Version	Type	Note
STM32CubeH7RS	1.3.0 and earlier *Note: Because the issue might not be fixed in subsequent release, refer to the release notes[2] of the **affected product** to check if the issue has been fixed.*	Embedded software	Affected by the three vulnerabilities listed in Description.
STM32CubeL0	1.12.4 and earlier *Note: Because the issue might not be fixed in subsequent release, refer to the release notes[2] of the **affected product** to check if the issue has been fixed.*	Embedded software	Affected by the *Core* software component vulnerability and the *MSC* class driver vulnerability, listed in Description.
STM32CubeL1	1.10.6 and earlier *Note: Because the issue might not be fixed in subsequent release, refer to the release notes[2] of the **affected product** to check if the issue has been fixed.*	Embedded software	Affected by the *Core* software component vulnerability and the *MSC* class driver vulnerability, listed in Description.
STM32CubeL4	1.18.2 and earlier *Note: Because the issue might not be fixed in subsequent release, refer to the release notes[2] of the **affected product** to check if the issue has been fixed.*	Embedded software	Affected by the *Core* software component vulnerability and the *MSC* class driver vulnerability, listed in Description.
STM32CubeL5	1.6.0 and earlier *Note: Because the issue might not be fixed in subsequent release, refer to the release notes[2] of the **affected product** to check if the issue has been fixed.*	Embedded software	Affected by the *Core* software component vulnerability and the *MSC* class driver vulnerability, listed in Description.
STM32CubeMP13	1.2.0 and earlier *Note: Because the issue might not be fixed in subsequent release, refer to the release notes[2] of the **affected product** to check if the issue has been fixed.*	Embedded software	Affected by the three vulnerabilities listed in Description.
STM32CubeWB	1.24.0 and earlier *Note: Because the issue might not be fixed in subsequent release, refer to the release notes[2] of the **affected product** to check if the issue has been fixed.*	Embedded software	Affected by the *Core* software component vulnerability and the *MSC* class driver vulnerability, listed in Description.

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 the 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 an STM32Cube firmware or an STM32 X-CUBE firmware package is impacted, check the supported version of the *USB Device* library:

File to read	Version with vulnerabilities	Version fixing the vulnerabilities
Release_Notes.html	2.11.5 and earlier	2.11.6 and later

A standalone *USB Device* library fixing the issues is available at: https://github.com/STMicroelectronics/stm32-mw-usb-device/releases/tag/v2.11.6.

Description

A weakness in the *USB Device* library *Core* software component `get_ep` status handling and in the *USB Device* library *MSC* class driver `SCSI CMD` handling can lead to a buffer overflow or to reading more data than expected.

A weakness in the *USB Device* library *MTP* class driver can cause a remote USB host to send an MTP transaction with a packet size larger than 255 bytes.

These weaknesses can lead to memory corruption.

Impact

Buffer overflow or reading more data than expected could compromise confidentiality of the memory in the device and even cause crashes or arbitrary code execution.

Remediation

Refer to Affected products to identify fixed products. For products that are not fixed, reconfigure the affected package with the fixed *USB Device* library delivered via GitHub.

Credit

- Maxime Rossi Bellom and Ramtine Tofighi Shirazi, SecMate, for issues in the *USB Device* library *Core* software component and *MSC* class driver
- Barrack (Byungyoung Yi) for the issue in the *USB Device* library *MTP* class driver

The individuals above contacted ST separately.

Contact information

psirt@st.com

Revision history

Date	Version	Changes
23-Apr-2026	1	Initial release.

IMPORTANT NOTICE – READ CAREFULLY

STMicroelectronics NV and its subsidiaries ("ST") place a high value on product security, and strive 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, advanced attacks that have not been tested, new or unidentified forms of attack, or any form of attack when using an ST product outside of its specification or intended use, or in conjunction with other components or software that are used by the purchasers 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, the purchasers are responsible for determining whether the level of security protection in an ST product meets their needs, both in relation to the ST product alone and when incorporated into the purchasers' 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.

In the event of any conflict between the provisions of this document and the provisions of any contractual arrangement in force between the purchasers and ST, the provisions of such contractual arrangement shall prevail.

The purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST's terms and conditions of sale in place at the time of order acknowledgment.

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

If the purchasers identify an ST product that meets their functional and performance requirements, but that is not designated for the purchasers' market segment, the purchasers shall contact ST for more information.

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.