Security advisory TN1528-ST-PSIRT: Impact of Mbed TLS security advisories released between 2022-07 and 2024-01 on STM32 embedded software

Overview

This security advisory pertains to the impact of Mbed TLS security advisories released between 2022-07 and 2024-01 on STM32 embedded software.

Affected products

Product[1]	Version	Type	Note
STM32CubeH7	v1.11.1 and earlier *Note: Because the issue might not be fixed in subsequent release[2], refer to the release notes of the **affected product** to check if the issue has been fixed.*	embedded software	Affected by the 4 advisories listed in Section Description.
STM32CubeF4	v1.28.0 and earlier *Note: Because the issue might not be fixed in subsequent release[2], refer to the release notes of the **affected product** to check if the issue has been fixed.*	embedded software	Affected by the 4 advisories listed in Section Description.
STM32CubeF7	v1.17.1 and earlier *Note: Because the issue might not be fixed in subsequent release[2], refer to the release notes of the **affected product** to check if the issue has been fixed.*	embedded software	Affected by the 4 advisories listed in Section Description.
STM32CubeH5	v1.1.1 and earlier *Note: Because the issue might not be fixed in subsequent release[2], refer to the release notes of the **affected product** to check if the issue has been fixed.*	embedded software	Affected by the 4 advisories listed in Section Description.
STM32CubeF2	v1.9.4 and earlier *Note: Because the issue might not be fixed in subsequent release[2], refer to the release notes of the **affected product** to check if the issue has been fixed.*	embedded software	Affected by the 4 advisories listed in Section Description.
STM32CubeU5	v1.4.0 and earlier *Note: Because the issue might not be fixed in subsequent release[2], refer to the release notes of the **affected product** to check if the issue has been fixed.*	embedded software	Affected by the 4 advisories listed in Section Description.
STM32CubeWBA	v1.2.0 and earlier *Note: Because the issue might not be fixed in subsequent release[2], refer to the release notes of the **affected product** to check if the issue has been fixed.*	embedded software	Affected by the 4 advisories listed in Section Description.

Product[1]	Version	Type	Note
STM32CubeL5	v1.4.0 and earlier *Note: Because the issue might not be fixed in subsequent release[2], refer to the release notes of the **affected product** to check if the issue has been fixed.*	embedded software	Affected by the 4 advisories listed in Section Description.
STM32CubeWL	v1.3.0 and earlier *Note: Because the issue might not be fixed in subsequent release[2], refer to the release notes of the **affected product** to check if the issue has been fixed.*	embedded software	Affected by the 4 advisories listed in Section Description.
X-Cube-SBSFU	v2.6.2 and earlier *Note: Because the issue might not be fixed in subsequent release[2], refer to the release notes of the **affected product** to check if the issue has been fixed.*	embedded software	Affected by the 4 advisories listed in Section Description.

1. *Some other STM32Cube Expansion packages (X-CUBE or I-CUBE) could depend on the **affected products** and are not mentioned in this document. Check if the X-CUBE or I-CUBE packages you are using contain the **affected products**. And if this is the case, refer to X-CUBE or I-CUBE packages release notes 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, via STM32CubeMX)*

To know if an STM32 Cube firmware package or an STM32 X-Cube firmware package is impacted, you can check the version of the middleware mbedTLS or the version of the middleware mbed-crypto supported:

Software component	File to read	Version fixing the vulnerabilities
Middlewares/Third_Party/mbedTLS	ST_readme.txt	mbedTLS 2.28.7 and later
Middlewares/Third_Party/mbed-crypto	ST_readme.txt	mbedTLS 2.28.7 and later

Description

The vulnerability description can be found at the following links:

- mbedtls-security-advisory-2022-07 (CVE-2022-35409): https://mbed-tls.readthedocs.io/en/latest/security-advisories/mbedtls-security-advisory-2022-07/(*)
- mbedtls-security-advisory-2024-01-2 (CVE-2024-23775): https://mbed-tls.readthedocs.io/en/latest/security-advisories/mbedtls-security-advisory-2024-01-2/(*)
- mbedtls-security-advisory-2024-01-1 (CVE-2024-23170): https://mbed-tls.readthedocs.io/en/latest/security-advisories/mbedtls-security-advisory-2024-01-1/(*)
- mbedtls-security-advisory-2023-10-1 (CVE-2023-43615):https://mbed-tls.readthedocs.io/en/latest/security-advisories/mbedtls-security-advisory-2023-10-1/(*)

Impact

Refer to the links given in Section Description.

Remediation

Refer to Section Affected products to identify the fixed products.

Credit

Refer to the links given in Section Description.

Contact information

psirt@st.com.

(*) *The URL belongs to a third party. It might be moved, modified, and/or inactivated by them at any time. STMicroelectronics is not responsible for the content of the referenced website.*

Revision history

Table 1. **Document revision history**

Date	Version	Changes
06-Jun-2024	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.