# Security advisory TN1457-ST-PSIRT: information about certified STM32Cube embedded software based on open source (TF-M and MCUboot)

## Overview

This document describes the impact of the security issues affecting some versions of the TF-M and MCUboot open-source software running on the STM32 certified products. The affected products/embedded software are listed in Table 1.

## Affected products

**Table 1. Affected products**

| Part number | Embedded software |
|---|---|
| - | STM32Cube_FW_U585_Security_certification version 1_0_0 |
| - | STM32Cube_FW_L5 version 1.1.0 |

## How to verify that the product/embedded software is affected

The following silicon products are not affected:

- STM32U585xx devices revision X (Die 482)
- STM32L5 series revision B (Die 472)

The following embedded software are affected:

- STM32Cube_FW_U585_Security_certification version 1.0.0
  - TF-M open source version TF-M v1.0-RC2 including MCUboot open source.
- STM32Cube_FW_L5 version 1.1.0
  - TF-M open source version TF-M v1.0-RC2 including MCUboot open source.

## Vulnerability description

No STMicroelectronics silicon products are affected. However, some vulnerabilities have been published on the **TF-M** and **MCUboot** open-source software versions used in the STM32Cube embedded software (identified in Table 1).

These vulnerabilities do not affect the hardware part of the SESIP/PSA certificates. However, depending on the final application, they can apply to the STM32Cube embedded software packages based on the use of such open-source software (identified in Table 1).

## Impact

The user must study the actual impact according to the final application. It is therefore the responsibility of the user to check if this issue is applicable in the application context, to decide whether the product can be used or not, and how it can be securely managed.

Moreover, STM32Cube embedded software packages (identified in Table 1) were evaluated in the scope of the following certificates:

- SESIP: SESIP-2100003-01 (STM32Cube_FW_U585_Security_certification v1_0_0)
- PSA: 0716053549921 – 10100 (STM32Cube_FW_U585_Security_certification v1_0_0)
- PSA: 0716053549631 – 10010 (STM32Cube_FW_L5 V1.1.0)

The above certificates have been or will be withdrawn.

### Remediation

It is the responsibility of the user to check if the fixes or mitigations proposed in the up-to-date version of the open-source software are relevant in the application context, decide whether the software can be used or not. In case the decision has been made to use it, it is the responsibility of the user to download it from the official repository of the open-source software.

- For TF-M open source version: *tf-m-user-guide.trustedfirmware.org*
- For MCUboot open source version: *www.mucboot.com*

### Contact information

psirt@st.com

## Revision history

Table 2. **Document revision history**

| Date | Revision | Changes |
|---|---|---|
| 20-Mar-2023 | 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.

Security advisories (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.