# SFI security enhancement for STM32H523/533 microcontrollers, STM32U5 series, and STM32L5 series

## Overview

This security advisory pertains to the SFI security enhancement for STM32H523/533 microcontrollers, STM32U5 series, and STM32L5 series.

The STM32 SFI solution is implemented through an SFI RSSe binary file, which must be integrated inside the customer secure programming tool. Refer to *Introduction to secure firmware install (SFI) for STM32 MCUs* (AN4992).

The SFI RSSe binaries were distributed through the STM32CubeProgrammer until the 2.17 version. The SFI RSSe binaries are currently distributed through the X-CUBE-RSSe expansion package.

## Affected products

| Product | Version | Type | Note |
|---|---|---|---|
| STM32CubeProgrammer (STM32CubeProg) | From version 2.4.0 up to version 2.17 | Tools | The tool itself is not affected, but some of the SFI RSSe binaries delivered as part of the tool are. |
| X-CUBE-RSSe | Versions 1.1.0 and 1.0.0 | STM32 Cube expansion package | - |

**For STM32CubeProgrammer**:

The user can get the STM32CubeProgrammer version from the listed path relative to the STM32CubeProgrammer installation directory:

- Under Windows®:
  - Path: ./STM32CubeProgrammer/bin/
  - Command: STM32_Programmer_CLI.exe --version
- Under Linux®:
  - Path: ./STM32CubeProgrammer/bin/
  - Command: ./STM32_Programmer_CLI --version
- Under MacOS®:
  - Path: ./STM32CubeProgrammer/bin/
  - Command: ./STM32_Programmer_CLI --version

The user can get the SFI RSSe binary version by editing the RSSe binary file. The version “x.y.z” is located in bytes [24:26]:

- Byte 24: z digit
- Byte 25: y digit
- Byte 26: x digit

The impacted versions of the SFI RSSe binary file used in the secure programming tool are the following:

| STM32 product | SFI RSSe binary file location | Affected version |
|---|---|---|
| STM32H523/533 | ./STM32CubeProgrammer/bin/RSSe/H5/ enc_signed_RSSe_SFI_STM32H5_512K_v1.0.0.0.bin | v1.0.0 |
| STM32U575/585 | ./STM32CubeProgrammer/bin/RSSe/U5/enc_signed_RSSe_sfi_U5_2M.bin | v4.0.0 and previous versions |
| STM32U59x/5Ax | ./STM32CubeProgrammer/bin/RSSe/U5/enc_signed_RSSe_sfi_U5_4M.bin | v4.0.0 and previous versions |
| STM32U5Fx/5Gx | ./STM32CubeProgrammer/bin/RSSe/U5/enc_signed_RSSe_sfi_U5_4M_Tiger.bin | v4.0.0 and previous versions |
| STM32U535/545 | ./STM32CubeProgrammer/bin/RSSe/U5/enc_signed_RSSe_sfi_U5_512k.bin | v4.0.0 and previous versions |
| STM32L552/562 | ./STM32CubeProgrammer/bin/RSSe/L5/enc_signed_RSSe_sfi.bin | v5.0.0 and previous versions |

**For X-CUBE-RSSe**:
The impacted versions of the SFI RSSe binary file used in the secure programming tool are the following:

| STM32 product | SFI RSSe binary file location | Affected version |
|---|---|---|
| STM32H523/533 | RSSe_SFI_H523_H533_v2.0.0.bin<br>RSSe_SFI_H523_H533_v2.1.0.bin | v2.0.0 and<br>v2.1.0 |
| STM32U575/585 | RSSe_SFI_U575_U585_v5.0.0.bin | v5.0.0 |
| STM32U59x/5Ax | RSSe_SFI_U59x_U5Ax_v5.0.0.bin | v5.0.0 |
| STM32U5Fx/5Gx | RSSe_SFI_U5Fx_U5Gx_v5.0.0.bin | v5.0.0 |
| STM32U535/545 | RSSe_SFI_U535_U545_v5.0.0.bin | v5.0.0 |
| STM32L552/562 | RSSe_SFI_L552_L562_v6.0.0.bin | v6.0.0 |

## Description

The SFI process can be compromised under specific conditions.

## Impact

Confidentiality of the firmware that is protected by SFI cannot be fully guaranteed. For STM32U5 and STM32L5 microcontrollers, only the SFI process to program the external flash memory is impacted.

## Remediation

The user must use the SFI RSSe binary files delivered within the X-CUBE-RSSe v1.2.0 or higher:

| STM32 product | SFI RSSe binary file location | Version fixing the problem |
|---|---|---|
| STM32H523/533 | **RSSe binary**: RSSe_SFI_H523_H533_v3.0.0.bin | v3.0.0 |
| | **Personalization data files**: Perso_Data_ H523_ H533_4780101B_SFI._v3.0.0.bin | v3.0.0 |
| STM32U575/585 | **RSSe binary**: RSSe_SFI_U575_U585_v6.0.0.bin | v6.0.0 |
| | **Personalization data files**:<br>• Perso_Data_U575_U585_4820200B_SFI._v6.0.0.bin | v6.0.0 |

| STM32 product | SFI RSSe binary file location | Version fixing the problem |
|---|---|---|
| STM32U575/585 | • Perso_Data_U575_U585_4820200B_SFIA_v6.0.0.bin | v6.0.0 |
| STM32U59x/5Ax | **RSSe binary**: RSSe_SFI_U59x_U5Ax_v6.0.0.bin | v6.0.0 |
| | **Personalization data files**:<br>• Perso_Data_ U59x_U5Ax_4810200F_SFI._v6.0.0.bin<br>• Perso_Data_ U59x_U5Ax_4810200F_SFIA_v6.0.0.bin | <br>v6.0.0<br>v6.0.0 |
| STM32U5Fx/5Gx | **RSSe binary**: RSSe_SFI_U5Fx_U5Gx_v6.0.0.bin | v6.0.0 |
| | **Personalization data files**:<br>• Perso_Data_ U5Fx_U5Gx _47601016_SFI._v6.0.0.bin<br>• Perso_Data_ U5Fx_U5Gx _47601016_SFIA_v6.0.0.bin | <br>v6.0.0<br>v6.0.0 |
| STM32U535/545 | **RSSe binary**: RSSe_SFI_U535_U545_v6.0.0.bin | v6.0.0 |
| | **Personalization data files**:<br>• Perso_Data_ U535_U545_45501015_SFI._v6.0.0.bin<br>• Perso_Data_ U535_U545_45501015_SFIA_v6.0.0.bin | <br>v6.0.0<br>v6.0.0 |
| STM32L552/562 | **RSSe binary**: RSSe_SFI_L552_L562_v7.0.0.bin | v7.0.0 |
| | **Personalization data file**: Perso_Data_L555_L562_47201003_SFI._v7.0.0.bin | v7.0.0 |

During the SFI firmware image creation process, the user must use an SFI RSSe binary with associated personalization data file version, as described in the table above.

For firmware image secure programming in production, the user must use a programmer tool supporting an SFI RSSe binary version, as described in the table above.

A new STM32HSM-V2 must be programmed with a personalization data file version, as described in the table above.

## Contact information

psirt@st.com

## Revision history

Table 1. **Document revision history**

| Date | Version | Changes |
|---|---|---|
| 05-Jan-2026 | 1 | Initial release. |
| 23-Mar-2026 | 2 | Changed document scope to public. |

**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.