SFI security enhancement for STM32H5, STM32U5, STM32L5, and STM32WL5

Overview

This security advisory pertains to the SFI security enhancement for STM32H5, STM32U5, STM32L5, and STM32WL5 microcontrollers.

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

Affected products

Product	Version	Type	Note
STM32CubeProgrammer (STM32CubeProg)	V2.17, V2.16, V2.15, V2.14	Tools	The tool itself is not affected, but some of the SFI RSSe binaries delivered as part of the tool are.

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:

Table 1. SFI RSSe binary file versions used in the secure programming tool

STM32 product	SFI RSSe binary file location	Affected version
STM32H562/563/573	./STM32CubeProgrammer/bin/RSSe/H5/enc_signed_RSSe_SFI_STM32H5_v2.0.1.0.bin	v2.0.1
STM32H562/563/573	./STM32CubeProgrammer/bin/RSSe/H5/enc_signed_RSSe_SFI_STM32H5_v2.0.0.0.bin	v2.0.0
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
STM32U59x/5Ax	./STM32CubeProgrammer/bin/RSSe/U5/enc_signed_RSSe_sfi_U5_4M.bin	v4.0.0
STM32U5Fx/5Gx	./STM32CubeProgrammer/bin/RSSe/U5/enc_signed_RSSe_sfi_U5_4M_Tiger.bin	v4.0.0
STM32U535/545	./STM32CubeProgrammer/bin/RSSe/U5/enc_signed_RSSe_sfi_U5_512k.bin	v4.0.0
STM32L552/562	./STM32CubeProgrammer/bin/RSSe/L5/enc_signed_RSSe_sfi.bin	v5.0.0
STM32WL5x	./STM32CubeProgrammer/bin/RSSe/WL/enc_signed_RSSe_sfi.bin	v5.0.0

Description

When using the affected versions of the SFI RSSe binary, an attacker can corrupt the SFI image, leading to an erroneous application execution after the SFI procedure.

Impact

The execution of the application might be erroneous, leading to a denial of service.

Remediation

The user must use the SFI RSSe binary files delivered within the X-CUBE-RSSe v1.0.0 or higher:

Table 2. SFI RSSe binary files delivered within the X-CUBE-RSSe v1.0.0 or higher

STM32 product	SFI RSSe binary file location	Version fixing the problem
STM32H562/563/573	RSSe binary: RSSe_SFI_H56x_H573_v3.0.0.bin Personalization data file: Perso_Data_ H56x_H573_48402011_SFI._v3.0.0.bin	v3.0.0 v3.0.0
STM32H523/533	RSSe binary: RSSe_SFI_H523_H533_v2.0.0.bin Personalization data files: Perso_Data_ H523_ H533_4780101B_SFI._v2.0.0.bin	V2.0.0 V2.0.0
STM32U575/585	RSSe binary: RSSe_SFI_U575_U585_v5.0.0.bin Personalization data files: • Perso_Data_U575_U585_4820200B_SFI._v5.0.0.bin • Perso_Data_U575_U585_4820200B_SFIA_v5.0.0.bin	V5.0.0 V5.0.0 V5.0.0
STM32U59x/5Ax	RSSe binary: RSSe_SFI_U59x_U5Ax_v5.0.0.bin Personalization data files: • Perso_Data_ U59x_U5Ax_4810200F_SFI._v5.0.0.bin • Perso_Data_ U59x_U5Ax_4810200F_SFIA_v5.0.0.bin	V5.0.0 V5.0.0 V5.0.0
STM32U5Fx/5Gx	RSSe binary: RSSe_SFI_U5Fx_U5Gx_v5.0.0.bin Personalization data files: • Perso_Data_ U5Fx_U5Gx _47601016_SFI._v5.0.0.bin • Perso_Data_ U5Fx_U5Gx _47601016_SFIA_v5.0.0.bin	V5.0.0 V5.0.0 V5.0.0
STM32U535/545	RSSe binary: RSSe_SFI_U535_U545_v5.0.0.bin Personalization data files: • Perso_Data_ U535_U545_45501015_SFI._v5.0.0.bin • Perso_Data_ U535_U545_45501015_SFIA_v5.0.0.bin	V5.0.0 V5.0.0 V5.0.0
STM32L552/562	RSSe binary: RSSe_SFI_L552_L562_v6.0.0.bin Personalization data file: Perso_Data_L555_L562_47201003_SFI._v6.0.0.bin	V6.0.0 V6.0.0
STM32WL5x	RSSe binary: RSSe_SFI_WL5x_v6.0.0.bin Personalization data file: Perso_Data_WL5x_49701005_SFI._v6.0.0.bin	V6.0.0 V6.0.0

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 HSM must be programmed with a personalization data file version as described in the table above.

Contact information

psirt@st.com

Revision history

Table 3. **Document revision history**

Date	Version	Changes
16-Oct-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.