Security advisory TN1529-ST-PSIRT: STM32CubeProgrammer for STM32H563/573 RSSe SFI security enhancement

Overview

This security advisory pertains to the STM32CubeProgrammer for STM32H563/573 RSSe SFI security enhancement.

Affected products

Product	Version	Type	Note
STM32CubeProg	V2.14, V2.15, V2.16	Tools	Affected component from STM32CubeProgrammer installation directory: • STM32H563/573 RSSe SFI: `./STM32CubeProgrammer/bin/RSSe/H5/enc_signed_RSSe_SFI_STM32H5_v2.0.0.0.bin` • Personalization data file: `./STM32CubeProgramme/bin/PersoPackages/STM32H5_48402011_SFI._01000000_00000000.enc.bin`

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 STM32H563/573 SFI RSSe codep version from the RSSe file name: ./STM32CubeProgrammer/bin/RSSe/H5/enc_signed_RSSe_SFI_STM32H5_v<`version: 4 digits dot separated`>.bin.

The user can get the personalization data file version from the personalization data file name: ./CubeProgrammer/bin/PersoPackages/STM32H5_48402011_SFI._01000000_<`version: 2 digits`>000000.enc.bin.

Description

When using the affected versions of the STM32H563/573 RSSe SFI delivered through the STM32CubeProgrammer tool, an attacker with physical access to the STM32H563/573 may be able to extract data protected by SFI. The issue is fixed within the new RSSe version described in the remediation section.

Impact

The data protected by the SFI might be extracted when the firmware loading strategy is not closely monitored or managed by the user.

Remediation

During SFI firmware image creation process, the user must use an STM32CubeProgrammer that supports a personalization data file version 1.0 or higher (`STM32H5_48402011_SFI._01000000_10000000.enc.bin`) in order to program the HSM.

For firmware image secure programming in production, the user must use a programmer tool supporting STM32H563/573 RSSe version 2.0.1.0 or higher (`enc_signed_RSSe_SFI_STM32H5_v2.0.1.0.bin`).

An HSM programmed with a personalization data file version 1.0 or higher only supports STM32H573/563 RSSe version 2.0.1.0 or higher (`enc_signed_RSSe_SFI_STM32H5_v2.0.1.0.bin`).

The user can also contact her/his STMicroelectronics representative to obtain the latest version of the STM32H563/573 RSSe SFI file and the latest version of the STM32H563/573 SFI dedicated personalization data file.

Contact information

psirt@st.com

Revision history

Table 1. **Document revision history**

Date	Version	Changes
18-Jul-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.