Security bulletin TN1474-ST-PSIRT: Information on software-based microarchitectural timing side-channel attacks on MCUs with TrustZone for Armv8-M

Overview

An article entitled *Software-based Microarchitectural Timing Side-channels Attacks on TrustZone-M MCUs* was disclosed on May 11 - 12, 2023 at the *Black Hat Asia* conference. It identifies a potential vulnerability of an application running on an Arm® Cortex®-M33 processor with TrustZone® for Armv8-M. The vulnerability only concerns applications implementing ***secret-dependent* control flow** or ***secret-dependent* memory access**.

STMicroelectronics does not promote or claim protection against this type of side-channel attack. That is, against a side-channel attack targeting applications that implement ***secret-dependent* control flow** or ***secret-dependent* memory access**. Nevertheless, users concerned by this type of side-channel attack can find additional information in the article https://developer.arm.com/documentation/ka005578/latest by Arm and in this document.

Description

The confidentiality of a secret managed by an application could be compromised when the following conditions are all met:

- The integrated circuit (an STMicroelectronics product inclusive) has an architecture that separates Non-secure and Secure zones (such as TrustZone for Armv8-M).
- The Non-secure and Secure zones on the integrated circuit share some of the resources, such as memories.
- The application on the Secure side implements *secret-dependent* control flow or *secret-dependent* memory access.

When these conditions are met, the user must consider the impact and risk of an attack to the Secure zone case by case in their application context.

To include a *secret-dependent* control flow or *secret-dependent* memory access in the Secure zone, the application developer should apply relevant applicative countermeasures against side-channel attacks.

This is a complex attack that requires the knowledge of the code on the Secure side and the rights to execute a malicious code on the Non-secure side.

Credit

Centro ALGORITMI, Universidade do Minho.

Contact information

psirt@st.com

Revision history

Table 1. Document revision history

Date	Version	Changes
05-June-2023	1	Initial version.

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.