Security advisory TN1500-ST-PSIRT: Improper isolation of protected secure resources

Overview

This security advisory pertains to the vulnerability of improperly isolating protected secure resources. It suggests measures to mitigate its impact.

Affected products

Product	Version[1]	Type	Note
STM32MP151A, STM32MP151C, STM32MP151D, STM32MP151F	B, Z	silicon product	-
STM32MP153A, STM32MP153C, STM32MP153D, STM32MP153F			
STM32MP157A, STM32MP157C, STM32MP157D, STM32MP157F			

1. *The version character is displayed in the device revision field of the package marking. Upon reading, the REV_ID[15:0] bitfield of the DBGMCU_IDC register returns 0x2000 for the device revision B and 0x2001 for the device revision Z.*

Description

Certain bus controllers (Cortex®-A7, SDMMC3, MDMA) can perform nonsecure write accesses to SRAM1/2/3/4, BKPSRAM, and RETRAM secure memories and to AHB5 secure peripherals. In addition, ETH can perform nonsecure read and write accesses to SRAM1/2/3/4 and RETRAM secure memories.

Impact

A user application using TrustZone® may potentially be impacted by the vulnerability. The secure boot chain is not impacted. A nonsecure application can write to some secure executable memories.

The overall impact depends on the user application context.

Users must assess the impact case by case, depending on their application requirements and architecture.

The PSA certificate 0716053550392–10316 has been withdrawn.

Remediation

For nonsecure embedded software, restrict the programming of nonsecure bus controller peripherals to the Linux® kernel (privileged mode).

For secure embedded software (software executed in the TrustZone®), apply one of the following measures:

- Do not use SRAM1/2/3/4, BKPSRAM, or RETRAM for storing secure executable code or sensitive data.
- Manage static abort exception and bus controller interrupt to detect illegal accesses. Apply the relevant action depending on the application context.

For the secure embedded software, optionally apply one or more of the following measures:

- Encrypt SRAM1/2/3/4, BKPSRAM, or RETRAM content if applicable.
- Check the integrity of SRAM1/2/3/4, BKPSRAM, or RETRAM content if applicable.
- Check the configuration integrity of the CRYP1, HASH1, RNG1, and AHB5 secure peripherals.
- Program all MDMA channels in secure mode.

Contact information

psirt@st.com

Revision history

Table 1. Document revision history

Date	Version	Changes
23-Nov-2023	1	Initial version.
02-Feb-2024	2	Initial public 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.