


PRODUCT / PROCESS CHANGE INFORMATION

1. PCI basic data

1.1 Company		STMicroelectronics International N.V
1.2 PCI No.	MDG/24/13550	
1.3 Title of PCI	STM32MP151x STM32MP153x STM32MP157x - Security Advisory - Improper isolation of protected secure resources.	
1.4 Product Category	STM32MP151x, STM32MP153x, STM32MP157x	
1.5 Issue date	2024-01-29	

2. PCI Team

2.1 Contact supplier	
2.1.1 Name	NEMETH KRISZTINA
2.1.2 Phone	+49 89460062210
2.1.3 Email	krisztina.nemeth@st.com
2.2 Change responsibility	
2.2.1 Product Manager	Ricardo Antonio DE SA EARP
2.1.2 Marketing Manager	Veronique BARLATIER
2.1.3 Quality Manager	Pascal NARCHE

3. Change

3.1 Category	3.2 Type of change	3.3 Manufacturing Location
General Product & Design	Modification of datasheet : Errata/error fix	ST Crolles 300 (France)

4. Description of change

	Old	New
4.1 Description	Current STM32MP151x STM32MP153x STM32MP157x (Die 500 -revision B, Z) product has Improper isolation of protected secure resource	STM32MP151x STM32MP153x STM32MP157x (Die 500 - Revision B,Z) products vulnerability for secure and non-secure embedded software can be worked around by following the remediation as described in the ST Technical Note TN1500 "Security advisory TN1500-ST-PSIRT: Improper isolation of protected secure resource"
4.2 Anticipated Impact on form,fit, function, quality, reliability or processability?	No impact	

5. Reason / motivation for change

5.1 Motivation	<p>Please find attached ST Technical Note TN1500 "Security advisory TN1500-ST-PSIRT: Improper isolation of protected secure resource" this information is communicated to STM32MP15 customers and remains under embargo until further notice.</p> <p>IMPORTANT - This information is published under embargo until further notice by ST. During this period this information and the attached document (13550 DM01027493_1_0.pdf) is not public and cannot be forwarded.</p> <p>At the end of this embargo period, TN1500 will be released on the ST PSIRT page https://www.st.com/content/st_com/en/security/report-vulnerabilities.html</p>
5.2 Customer Benefit	SERVICE IMPROVEMENT

6. Marking of parts / traceability of change

6.1 Description	No change of Finished Good. Traceability is not applicable.
------------------------	--

7. Timing / schedule

7.1 Date of qualification results	2023-12-07
7.2 Intended start of delivery	2023-12-07

7.3 Qualification sample available?	Upon Request
-------------------------------------	--------------

8. Qualification / Validation			
-------------------------------	--	--	--

8.1 Description	13550 As no product change no qualification document is expected to be released.pdf		
8.2 Qualification report and qualification results	Available (see attachment)	Issue Date	2024-01-29

9. Attachments (additional documentations)			
--	--	--	--

13550 Public product.pdf
13550 As no product change no qualification document is expected to be released.pdf
13550 DM01027493_1_0 - UNDER EMBARGO - CANNOT BE MADE PUBLIC - .pdf

10. Affected parts		
--------------------	--	--

10. 1 Current		10.2 New (if applicable)
10.1.1 Customer Part No	10.1.2 Supplier Part No	10.1.2 Supplier Part No
	STM32MP151FAB1	
	STM32MP157FAA1	

IMPORTANT NOTICE – PLEASE READ CAREFULLY

Subject to any contractual arrangement in force with you or to any industry standard implemented by us, STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. 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 acknowledgement.

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 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.

ST and the ST logo are trademarks of ST. 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.

© 2022 STMicroelectronics – All rights reserved



Public Products List

Public Products are off the shelf products. They are not dedicated to specific customers, they are available through ST Sales team, or Distributors, and visible on ST.com

PCI Title : STM32MP151x STM32MP153x STM32MP157x - Security Advisory - Improper isolation of protected secure resources.

PCI Reference : MDG/24/13550

Subject : Public Products List

Dear Customer,

Please find below the Standard Public Products List impacted by the change.

STM32MP151DAD1	STM32MP153DAD1	STM32MP157DAD1
STM32MP157CAB3T	STM32MP153DAB1	STM32MP153FAA1
STM32MP157AAB3T	STM32MP157DAB1	STM32MP153AAA3
STM32MP157AAA3	STM32MP153CAB3T	STM32MP151FAA1
STM32MP151CAB3T	STM32MP151AAA3	STM32MP151CAD3
STM32MP157FAC1	STM32MP151CAB3	STM32MP153CAB3
STM32MP151DAA1	STM32MP153AAB3T	STM32MP151DAB1
STM32MP151AAB3T	STM32MP157CAA3	STM32MP157CAB3
STM32MP153CAC3T	STM32MP157AAD3	STM32MP153AAD3
STM32MP151AAA3T	STM32MP151AAB3	STM32MP153DAA1
STM32MP151AAD3T	STM32MP151CAD3T	STM32MP151CAA3
STM32MP157CAC3T	STM32MP157DAA1	STM32MP151CAA3T
STM32MP151FAB1	STM32MP153CAD3	STM32MP157CAD3
STM32MP151FAC1	STM32MP157CAC3	STM32MP151FAD1
STM32MP153CAC3	STM32MP157AAC3T	STM32MP157FAA1
STM32MP157FAA1T	STM32MP153AAC3T	STM32MP151DAC1
STM32MP157CAD3T	STM32MP151AAC3	STM32MP153CAD3T
STM32MP153AAA3T	STM32MP157AAC3	STM32MP153AAC3
STM32MP157FAD1	STM32MP153CAA3T	STM32MP157AAD3T
STM32MP153FAD1	STM32MP157CAA3T	STM32MP153CAA3
STM32MP157AAA3T	STM32MP153AAD3T	STM32MP151CAC3T
STM32MP151AAD3	STM32MP153DAC1	STM32MP157DAC1
STM32MP157AAB3	STM32MP153FAB1	STM32MP153AAB3
STM32MP153FAC1	STM32MP151CAC3	STM32MP157FAB1
STM32MP151AAC3T		

IMPORTANT NOTICE – PLEASE READ CAREFULLY

Subject to any contractual arrangement in force with you or to any industry standard implemented by us, STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. 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 acknowledgement.

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 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.

ST and the ST logo are trademarks of ST. 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.

As no change affecting the product itself no qualification document is planned to be released.

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.

**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.

© 2023 STMicroelectronics – All rights reserved