TN1460

Technical note

STSAFE-TPM: assessment of vulnerability VU#782720

Introduction

This document is a confirmation that the vulnerabilites linked to VU#782770 do not reprensent any security vulnerability for all STMicroelectronics STSAFE-TPM products. The exhaustive list of products is provided in Table 2.

Table 1. **Vulnerabilities identification**

Organization	Vulnerability ID
CERT coordination center (CERT/CC)	VU#782720 TCG TPM2.0 implementations vulnerable to memory corruption
TCG	TCG ID: TCGVRT0007
Mitre	CVE ID: CVE-2023-1017
	CVE ID: CVE-2023-1018
ST PSIRT	Reference: 221130-01-MDG

Table 2. **Products covered by the assessment**

Type	Root part number
Secure microcontrollers	ST33TPHF2XSPI, ST33TPHF2XI2C ST33TPHF2ESPI, ST33TPHF2EI2C ST33TPHF20SPI, ST33TPHF20I2C
	ST33GTPMISPI, ST33GTPMII2C, ST33GTPMASPI, ST33GTPMAI2C
	ST33KTPM2XSPI, ST33KTPM2XI2C

1 Vulnerability assessment of STSAFE-TPM products on VU#782720

The STSAFE-TPM products defined in Table 2 are not affected by vulnerability VU#782720 and it is confirmed that:

- No secret asset can be revealed
- STSAFE-TPM expected behavior and memory integrity cannot be modified.

The assessment has been conducted by reviewing the code and by testing the STSAFE-TPM products.

For both potential vulnerabilities, all STSAFE-TPM perform the following actions:

- check all the command parameters length
- detect incorrect lengths
- interrupt command execution before memory access (read or write)
- report specific error codes.

Regarding potential OOB write vulnerability

- STSAFE-TPM products reject any command that is wrongly formatted by performing one of the following behaviors:
  - Error code TPM_RC_SIZE and remain fully functional
  - Error code TPM_RC_Failure and enter failure mode

Note: *In both cases, the internal memory is not corrupted. The product behaves as expected after error code or failure mode exit.*

The following table shows the product behavior for potential OOB write vulnerability:

Table 3. **STSAFE-TPM behavior on OOB write error**

Product	Firmware version	OOB write error code	State after error code
ST33TPHF2Exxx	71.x	RC_Failure	Failure mode
ST33TPHF2Exxx	73.00/04/08/20	RC_Failure	Failure mode
ST33TPHF2Exxx	73.64/65	RC_Size	Functional
ST33TPHF20xxx	74.00/04/08/09/20	RC_Failure	Failure mode
ST33TPHF20xxx	74.16/64/65	RC_Size	Functional
ST33TPHF2Xxxx	1.x & 2.x	RC_Size	Functional
ST33GTPMI/Axxx	3.x & 6.x	RC_Size	Functional
ST33KTPM2Xxxx	9.x	RC_Size	Functional

Regarding potential OOB read vulnerability

- STSAFE-TPM products reject any command that is wrongly formatted by performing the following behavior:
  - Error code TPM_RC_INSUFFICIENT and remain fully functional.

There is no risk of memory leak.

2 Conclusion

The assessment performed on STSAFE-TPM products via code review and product testing confirm that VU#782720 does not represent any security vulnerability for the products listed in Table 2.

Revision history

Table 4. **Document revision history**

Date	Revision	Changes
28-Feb-2023	1	Initial release.
08-Mar-2023	2	Updated Table 1. Vulnerabilities identification: Mitre row.

Contents

List of tables

IMPORTANT NOTICE – READ CAREFULLY

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 acknowledgment.

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. 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.