# Applicability of security vulnerability TCG VRT0011 on STSAFE-TPM products

## Overview

This security advisory pertains to the security vulnerability TCG VRT0011, TPM 2.0 RSA OAEP timing side-channel vulnerability.

## Affected products

| Product root part number | Version | Remediation | Note |
|---|---|---|---|
| ST33TPHF2ESPI<br>ST33TPHF2EI2C<br>ST33TPHF20SPI<br>ST33TPHF20I2C<br>ST33GTPMASPI<br>ST33GTPMAI2C<br>ST33GTPMISPI<br>ST33GTPMII2C | All versions | System workaround | - |
| ST33TPHF2XSPI | All versions | TPM firmware update or system workaround | Fix included in TPM firmware version 1.771 |
| ST33TPHF2XI2C | All versions | TPM firmware update or system workaround | Fix included in TPM firmware version 2.771 |

## Non-affected products

| Product root part number | Version |
|---|---|
| ST33KTPM2XSPI<br>ST33KTPM2XI2C<br>ST33KTPM2X | All versions |
| ST33KTPM2I<br>STSAFE-V100-TPM (aka ST33KTPM2A) | All versions |

The product root part numbers are defined in the above tables. For product ordering codes and firmware versions, refer to the STSAFE-TPM product page (https://www.st.com/en/secure-mcus/authentication.html) and the product databrief description.

## Description

A timing side-channel vulnerability has been found in the RSA OAEP decryption, enabling an attacker to decrypt sensitive blobs (import blobs, credential blobs, and session salts) encrypted to RSA decrypt keys, including the RSA endorsement key (EK) which can reveal imported keys or falsify TPM 2.0 attestation keys. The vulnerability is rooted in the implementation of OAEP padding checks, which can be exploited using repeated requests and timing analysis (Manger's attack).

## Impact

An adversary can use this vulnerability to:

- Decrypt RSA-wrapped credentials from a TPM attestation CA for a falsified attestation key (with the private key known to the adversary rather than protected by the TPM,) and falsify TPM attestations services.
- Decrypt RSA-wrapped import blobs, gaining direct access to sensitive portions (such as private keys) of imported objects.
- Decrypt RSA-wrapped session salts, enabling man-in-the-middle attacks against callers establishing salted sessions.

## Remediation

For the products ST33TPHF2XPI and ST33TPHF2XI2C, STMicroelectronics provides firmware binaries that include a security fix that removes the time side channel leakage. After a firmware update, it is strongly recommended to revoke all the attestation keys whose credential was activated using the RSA EK (command TPM2_ActivateCredential) and regenerate new attestation certificates and/or re-provision keys that were imported using the RSA decrypt keys.

If the firmware update is not deployed, as an alternative, ST recommends a system workaround implementing security countermeasures at system level:

- Using ECC decrypt keys instead of RSA decrypt keys, including the ECC endorsement key.
- For the Credential activate protocol, the verifier should limit the time between the sending of the activate credential blob and the evidence that the blob was decrypted by the origin TPM. The time required to perform the average number of decryption trials for a RSA 2048-bit key is around 2 hours. Setting a time out far below that timing makes less practical for an adversary to complete the attack.

## Contact information

psirt@st.com

The third-party security advisories can be found under the following reference numbers:

- TCGVRT0011, which references the following other third-party security advisories:
  - CVE-2026-6727
  - Vince VU#431093

*Note: STMicroelectronics is not responsible for the content nor the maintenance of the third-party security advisories.*

## Revision history

| Date | Version | Changes |
|---|---|---|
| 10-Aug-2026 | 1 | Initial release |

**IMPORTANT NOTICE – READ CAREFULLY**

STMicroelectronics NV and its subsidiaries ("ST") place a high value on product security, and strive 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, advanced attacks that have not been tested, new or unidentified forms of attack, or any form of attack when using an ST product outside of its specification or intended use, or in conjunction with other components or software that are used by the purchasers 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, the purchasers are responsible for determining whether the level of security protection in an ST product meets their needs, both in relation to the ST product alone and when incorporated into the purchasers' 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.

In the event of any conflict between the provisions of this document and the provisions of any contractual arrangement in force between the purchasers and ST, the provisions of such contractual arrangement shall prevail.

The 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.

The 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 the 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.

If the purchasers identify an ST product that meets their functional and performance requirements, but that is not designated for the purchasers' market segment, the purchasers shall contact ST for more information.

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.