Security bulletin TN1489-ST-PSIRT: Physical attacks on STM32 and STM32Cube firmware

Overview

This security bulletin relates generally to any physical attack against any version of an STM32 and/or STM32Cube firmware product (collectively referred to as ***STM32 product*** in this document). It does not pertain to any specific known physical attack.

Physical attacks mean attacks made by acquiring physical access, or very close access, to an *STM32 product*. This includes, but may not be limited to:

- attacks made through access to physical interfaces
- perturbation attacks (that is, fault injections to induce an exploitable error)
- side channel attacks (including timing attacks), power analysis (SPA, DPA, and the like), and electromagnetic analysis
- invasive attacks including physical changes and reverse engineering

In addition to requiring physical or close access to an *STM32 product*, *physical attacks* often require specialized tools and techniques.

Description

Regarding *STM32 products* and their resistance to *physical attacks*:

Unless an *STM32 product* is SESIP or PSA certified as having a security assurance level covering ***physical attacker resistance***, it may be vulnerable to *physical attacks*.

For the security assurance level of a certified *STM32 product*:

- Services and features that are protected against *physical attacks* are identified in the certification scope of the product ***security targets***. Note that the protection level (security assurance level) depends on the certification level obtained.
- Resistance level for those services and features is described in the *security targets*.
- Services and features outside the certification scope are not covered.

If a service or a feature of an *STM32 product* is not certified as having *physical attacker resistance*, such *STM32 product* should not be considered resistant to *physical attacks*.

Generally speaking, because *physical attacks* require physical or close access to an *STM32 product*, they are typically limited to only a select number of devices to which attackers have physical access, as opposed to remote attacks. The potential impact of a *physical attack* is therefore typically much more limited than the impact of a remote attack. The overall impact of a *physical attack* also highly depends on the sensitivity of the information associated with the targeted product.

When the application context requires resistance to *physical attacks*, it is advised to select *STM32 products* that are SESIP or PSA certified with *physical attacker resistance*. To meet the application requirements, it may not be sufficient to select a SESIP or PSA certified *STM32 product*. It is also important that the security assurance level stated in that certification provides *physical attacker resistance*.

For certification scope and security assurance level, refer to the product *security targets* and certificates available on the certification body websites:

- https://www.trustcb.com/iot/sesip/sesip-certificates/
- https://www.psacertified.org/certified-products/

Contact information

psirt@st.com

Revision history

Table 1. **Document revision history**

Date	Version	Changes
09-Oct-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.