Security advisory TN1491-ST-PSIRT: Keccak XKCP SHA-3 reference implementation issue impact on STM32 products

Overview

This security advisory pertains to the Keccak XKCP SHA-3 open-source software reference implementation attack described in CVE-2022-37454, and its impact on STM32 products.

Affected products

Product	Version	Type	Note
X-CUBE-CRYPTOLIB	version 4.0.0, 4.0.1, and 4.1.0	embedded software	-

No STMicroelectronics STM32 hardware products are affected. However, the issue published regarding the Keccak XKCP SHA-3 open-source software can apply to the X-CUBE-CRYPTOLIB listed above if the following functions are made directly accessible by the application:

- SHA-3
- SHAKE
- EdDSA (only using the Edwards448 curve) signature generation and verification.

In particular, the X-CUBE-CRYPTOLIB is impacted if the user can fully control the input and/or the output sizes of the Keccak sponge function, by specifying sizes greater than or equal to 2^{32} – 200 bytes.

Description

Refer to *Incorrect integer comparisons and buffer overflows*(1) and *CVE-2022-37454*(1).

Impact

The Keccak sponge function interface accepts partial inputs to be absorbed and partial outputs to be squeezed. A buffer can overflow when at least one partial data of size higher than or equal to 2^{32} – 200 bytes is queued to the Keccak sponge function. To exploit the bug, it is not necessary to have this number of bytes, but it is just sufficient to provide that length to the Keccak function. Because of the bug, the function tries to read that quantity of bytes from the memory, most probably ending in a crash. In view of this, the user must consider the actual impact according to the final application.

Remediation

The issue can be avoided by limiting the size of the partial input data (or partial output digest) below 2^{32} – 200 bytes. Multiple calls to the system queue can be chained at a higher level to retain the original functionality. Alternatively, one can process the entire input (or produce the entire output) at once, avoiding use of the Keccak sponge function with partial inputs/outputs.

Credit

Refer to CVE-2022-37454(1).

Contact information

psirt@st.com

(1) *The URL belongs to a third party. It may be moved, modified, and/or inactivated by them at anytime. STMicroelectronics is not responsible for the content of the referenced website.*

Revision history

Table 1. **Document revision history**

Date	Version	Changes
11-Oct-2023	1	Initial version.
11-Dec-2023	2	Removed Section *How to verify that the product is affected* and content moved to Section Affected products. Updated Section Affected products and Section Impact.

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.