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[1]	Version		Type	Note
X-CUBE-CRYPTOLIB	From 4.0.0 to 4.5.0	*Note:* *Because the issue might not be fixed in subsequent version, refer to the release notes[2] of the affected product to check if the issue has been fixed.*	Embedded software	-
X-CUBE-PQC	From 1.0.0 to 1.1.0	*Note:* *Because the issue might not be fixed in subsequent version, refer to the release notes[2] of the affected product to check if the issue has been fixed.*	Embedded software	-

1. *Some other STM32Cube expansion packages or function packages (X-CUBE, I-CUBE, STSW, FPs) could depend on the affected products and are not mentioned in this document. Check if STM32Cube expansion packages or function packages you use contain the affected products. If so, refer to the package release note to check if the issue has been fixed.*

2. *Release notes are available in each downloaded package (on www.st.com product pages, on STMicroelectronics Github product pages, and via STM32CubeMX).*

To know if an STM32Cube firmware package or an STM32 X-Cube firmware package is impacted, check the version of the released libraries inside the cryptographic middleware as described in the following table:

Software component relative path	File to check	Released library version with vulnerabilities
./Middlewares/ST/STM32_Cryptographic/	Release_Notes.html	4.0.0.Build1

No STMicroelectronics STM32 hardware products are affected. However, the issue published regarding the Keccak XKCP SHA-3 open-source software can apply to the above-listed **affected products** 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 above-listed **affected products** are 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.

TN1491 - Rev 3 - November 2025
For further information, contact your local STMicroelectronics sales office.

www.st.com

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 might be moved, modified, and/or inactivated by them at any time. 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.
14-Nov-2025	3	Updated Section Affected products.

IMPORTANT NOTICE – READ CAREFULLY