Security advisory TN1492-ST-PSIRT: Bypass of the CKS locking mechanism

Overview

This security advisory pertains to an improper resource locking for key usage of the keys stored in the CKS managed by STM32CubeWB.

Affected products

Product	Version	Type	Note
STM32CubeWB	Version v1.17.1 and earlier	Embedded software	-

How to verify the product is affected

This issue relates to the embedded software listed above.

Description

This issue may allow software running on CPU1 to bypass the locking mechanism of the CKS.

Impact

Some locked keys stored in the CKS may be loaded in the AES engine, and used by the product executing the embedded software to encrypt or decrypt data. However, the keys cannot be obtained or viewed by the user.

Remediation

The issue is fixed in STM32CubeWB starting from the version v1.17.2.

The updates can at least be found at the following location: STM32CubeWB. STMicroelectronics recommends that the users update their software to the most recent version.

Credit

-

Contact information

psirt@st.com

Revision history

Table 1. Document revision history

Date	Version	Changes
11-Oct-2023	1	Initial release.

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.