SA0034

Security advisory

KMS security enhancement for STM32 embedded software

Overview

This security advisory pertains to a KMS (key management services) security enhancement for STM32 embedded software.

Affected products

Product[1]	Version	Type	Note
X-CUBE-SBSFU	From v2.2.0 to v2.6.2 *Note: Because the issue might not be fixed in subsequent release, refer to the release notes[2] of the **affected product** to check if the issue has been fixed.*	STM32Cube expansion package	-
STM32CubeWL	From v1.0.0 to v1.3.0 *Note: Because the issue might not be fixed in subsequent release, refer to the release notes[2] of the **affected product** to check if the issue has been fixed.*	STM32Cube firmware	-

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 are using 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, an STM32Cube expansion package, or a function package is impacted, check the version of the KMS software component supported:

Software component relative path	File to read	Version with the vulnerability
./Middlewares/ST/ STM32_Key_Management_Services	Release_Notes.html	V1.1.9 and earlier

Description

The ECC key pair generation service (`C_GenerateKeyPair()`) does not use any entropy source when the KMS middleware is configured to use the ST Cryptographic library (compilation switch `CA_ST_CRYPTOLIB_SUPP` activated in the application IDE project) and when the key pair generation service is used (compilation switch `KMS_GENERATE_KEYS` activated in the application IDE project).

Impact

The ECC key pair generation service produces always the same key pair.

Remediation

To remediate this problem, generate the entropy data, managed by the `KMS_GenerateKeyPair()`, using a random generator solution (such as the STM32 RNG or TRNG hardware peripheral).

Contact information

psirt@st.com

Revision history

Table 1. Document revision history

Date	Version	Changes
12-Feb-2025	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.