# SA0053

Security advisory

# Arbitrary code execution with privilege on STM32H73xxx and STM32H7Bxxx microcontrollers

## Overview

This security advisory pertains to an arbitrary code execution with privilege on STM32H73xxx and STM32H7Bxxx microcontrollers that feature the OTFDEC encryption service.

## Affected products

| Product | Version | Type | Note |
|---|---|---|---|
| STM32H73xx | Revisions A and Z | Silicon product | - |
| STM32H7Bxxx | Revisions X and Z | Silicon products | - |

## Description

A vulnerability exists in the root secure services (RSS) code for the resetAndEncrypt service described in the application note AN5281. This vulnerability can be exploited to perform arbitrary code execution with the same privileges as the RSS code.

## Impact

Arbitrary code execution with the same privileges as the RSS code.

## Remediation

The customer should configure the product in RDP level 2. In this configuration, the vulnerability cannot be exploited without a successful preliminary attack on the user application.

## Credit

Vulnerability found by GaryOderNichts.

## Contact information

psirt@st.com

## Revision history

Table 1. Document revision history

| Date | Version | Changes |
|---|---|---|
| 26-Sep-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.