Impact of Azure RTOS FileX STM32 RAM driver buffer overflow issue on STM32 embedded software (TALOS-2024-2096)

Overview

This security advisory pertains to the impact of Azure RTOS FileX STM32 RAM driver buffer overflow issue on STM32 embedded software, identified as TALOS-2024-2096 by Cisco Talos team.

Affected products

Product[1]	Version	Type	Note
STM32CubeU5	v1.7.0 and earlier *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	-
STM32CubeC0	v1.4.0 and earlier *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	-
STM32CubeH5	v1.5.0 and earlier *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	-
STM32CubeWBA	v1.6.0 and earlier *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	-
STM32CubeN6	v1.1.0 and earlier *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	-
STM32CubeU0	v1.2.0 and earlier *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	-
STM32CubeU3	v1.1.0 and earlier *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	-
STM32CubeMP13	v1.2.0 and earlier *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-AZRTOS-F4	v1.1.0 and earlier *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-AZRTOS-F7	v1.1.0 and earlier *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-AZRTOS-G0	v1.1.0 and earlier *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	-

Product[1]	Version	Type	Note
X-CUBE-AZRTOS-G4	v2.0.0 and earlier *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-AZRTOS-H7	v3.3.0 and earlier *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-AZRT-H7RS	v1.0.0 and earlier *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-AZRTOS-L4	v2.0.0 and earlier *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-AZRTOS-L5	v2.0.0 and earlier *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-AZRTOS-WB	v2.0.0 and earlier *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-AZRTOS-WL	v2.0.0 and earlier *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 the problem is fixed in a version of the STM32Cube firmware package or the STM32 X-CUBE firmware package, check if “SA0038” is mentioned in the release note of the HAL software component as stated in the following table:

Software component relative path	File to read	Version fixing the vulnerabilities
./Middlewares/ST/filex/common/driver	readme.txt	Contains note that SA0038 issue is fixed

Description

Improper restriction of operations within the bounds of a memory buffer inside the Azure RTOS FileX STM32 RAM driver can lead to the corruption of the internal memory of the STM32 device.

Impact

Buffer overflow issue in the Azure RTOS FileX STM32 RAM driver can lead to an attacker-controlled code execution.

Remediation

Refer to Affected products to identify fixed products.

Credit

Kelly Patterson at Cisco Talos

Contact information

psirt@st.com

Revision history

Table 1. **Document revision history**

Date	Version	Changes
27-Mar-2025	1	Initial version.

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.