Impact of Azure RTOS NetXDuo HTTP server issues on STM32 embedded software (TALOS-2024-2097, TALOS-2024-2102, and TALOS-2024-2103)

Overview

This security advisory pertains to the impact of Azure RTOS NetXDuo HTTP server issues on STM32 embedded software, identified as TALOS-2024-2097, TALOS-2024-2102, and TALOS-2024-2103 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	-
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	-
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	-

SA0040 - Rev 1 - March 2025
For further information, contact your local STMicroelectronics sales office.

www.st.com

Product[1]	Version		Type	Note
X-CUBE-AZRTOS-G4	v2.0.0 and earlier		Embedded software	-
	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.*		
X-CUBE-AZRTOS-H7	v3.3.0 and earlier		Embedded software	-
	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.*		
X-CUBE-AZRT-H7RS	v1.0.0 and earlier		Embedded software	-
	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.*		
X-CUBE-AZRTOS-L4	v2.0.0 and earlier		Embedded software	-
	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.*		
X-CUBE-AZRTOS-L5	v2.0.0 and earlier		Embedded software	-
	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.*		
X-CUBE-AZRTOS-WB	v2.0.0 and earlier		Embedded software	-
	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.*		
X-CUBE-AZRTOS-WL	v2.0.0 and earlier		Embedded software	-
	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.*		

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 STM32 Cube firmware package, an STM32 X-Cube firmware package, or a function package is impacted, check the version of the NetXDuo software component supported:

Software component relative path	File to read	Version with vulnerabilities
./Middlewares/ST/netxDuo	st_readme.txt	6.4.0 and earlier

Description

The following table makes the link between these ST issues and their description:

ST issue	Link to the issue description
TALOS-2024-2097	Eclipse ThreadX NetX Duo HTTP server denial of service vulnerability (TALOS-2024-2098)[1]
TALOS-2024-2102	Eclipse ThreadX NetX Duo HTTP server chunked PUT request integer underflow vulnerability (TALOS-2024-2104)[1]
TALOS-2024-2103	Eclipse ThreadX NetX Duo HTTP server single PUT request integer underflow vulnerability (TALOS-2024-2105)[1]

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.*

Note: *The Cisco Talos team assigned the issue number in the left table column to ST, and the issue number in the right table column to Eclipse Foundation.*

Impact

Follow the links given in Description section.

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