Impact of the FreeRTOS kernel third-party security advisories released between 2021-04 and 2024-10 on STM32 embedded software

Overview

This security advisory pertains to the impact of the FreeRTOS kernel third-party security advisories released between 2021-04 and 2024-10 in version 10.6.1 and earlier on STM32 embedded software.

Affected products

Product[1]	Version		Type	Note
STM32CubeH7RS	V1.0.0	*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.*	Embedded software	Impacted by CVE-2024-2811
STM32CubeMP2	V1.1.1	*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.*	Embedded software	Impacted by CVE-2024-2811
STM32CubeWB0	V1.0.0	*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.*	Embedded software	Impacted by CVE-2024-2811
X-CUBE-FREERTOS	V1.2.0 and earlier	*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.*	Embedded software	Impacted by CVE-2024-2811
STM32CubeF4	V1.28.1 and earlier	*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.*	Embedded software	Impacted by all the CVEs listed in Section Description
STM32CubeF7	V1.17.2 and earlier	*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.*	Embedded software	Impacted by all the CVEs listed in Section Description
STM32CubeG4	V1.6.0 and earlier	*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.*	Embedded software	Impacted by all the CVEs listed in Section Description
STM32CubeL0	V1.20.1 and earlier	*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.*	Embedded software	Impacted by all the CVEs listed in Section Description
STM32CubeL4	V1.18.1 and earlier	*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.*	Embedded software	Impacted by all the CVEs listed in Section Description
STM32CubeL5	V1.5.1 and earlier			

SA0036 - Rev 1 - March 2025
For further information, contact your local STMicroelectronics sales office.

www.st.com

Product[1]	Version		Type	Note
	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.*	Embedded software	Impacted by all the CVEs listed in Section Description
STM32CubeF0	V1.11.5 and earlier		Embedded software	Impacted by all the CVEs listed in Section Description
	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.*		
STM32CubeF1	V1.8.6 and earlier		Embedded software	Impacted by all the CVEs listed in Section Description
	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.*		
STM32CubeF2	V1.9.5 and earlier		Embedded software	Impacted by all the CVEs listed in Section Description
	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.*		
STM32CubeF3	V1.11.5 and earlier		Embedded software	Impacted by all the CVEs listed in Section Description
	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.*		
STM32CubeH7	V1.12.2 and earlier		Embedded software	Impacted by all the CVEs listed in Section Description
	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.*		
STM32CubeMP13	V1.1.0 and earlier		Embedded software	Impacted by CVE-2024-2811
	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.*		
STM32CubeMP1	V1.6.0 and earlier		Embedded software	Impacted by all the CVEs listed in Section Description
	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.*		
STM32CubeWB	V1.20.0 and earlier		Embedded software	Impacted by all the CVEs listed in Section Description
	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.*		
STM32CubeWL	V1.3.0 and earlier		Embedded software	Impacted by all the CVEs listed in Section Description
	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.*		

1. *Some other STM32Cube expansion packages or function packages (X-CUBE, I-CUBE, STSW, FPs) can depend on the **affected products** and are not mentioned in this document. Check if the 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 FreeRTOS software component supported:

Software component relative path	File to read	FreeRTOS version with CVEs	List of CVEs	FreeRTOS version fixing the vulnerabilities
./Middlewares/Third_Party/FreeRTOS	st_readme.txt	Earlier than 10.4.3	CVE-2021-31572 CVE-2021-31571 CVE-2021-32020	10.4.3 and later
./Middlewares/Third_Party/FreeRTOS	st_readme.txt	Earlier than 10.5.0	CVE-2021-43997	10.5.0 and later
./Middlewares/Third_Party/FreeRTOS	st_readme.txt	Earlier than 10.6.2	CVE-2024-28115	10.6.2 and later

Regarding the standalone components offered through GitHub that might be used with the **affected products**, the corresponding fixes are available at https://github.com/STMicroelectronics/stm32-mw-freertos/releases/tag/v10.6.2_20241011.

The user needs to reconfigure the affected package with the fixed component.

Description

The third-party security advisories can be found at following links:

- CVE-2021-31572[1]
- CVE-2021-31571[1]
- CVE-2021-32020[1]
- CVE-2024-28115[1]
- CVE-2021-43997[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.*

Impact

Follow the links given in Section Description.

Remediation

Refer to Section Affected products to identify the fixed products.

Contact information

psirt@st.com

Revision history

Table 1. Document revision history

Date	Version	Changes
28-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.