Potential internal data leakage via Ethernet in STM32 embedded software networking RTOS applications based on LwIP

Overview

This security advisory pertains to a potential internal data leakage via Ethernet in STM32 embedded software networking RTOS applications using LwIP stack v2.2.0 and earlier versions.

Affected products

Product[1]	Version		Type	Note
STM32CubeH7RS	V1.1.0 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	-
STM32CubeH7	V1.11.2 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	-
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	-
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	-
STM32CubeF1	V1.8.6 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	-
STM32CubeF2	V1.9.5 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	-

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).*

Description

Due to a race condition in the Ethernet `low_level_output` function of RTOS applications based on the LwIP stack, out-of-bounds reads to uncontrolled memory sections can happen via Ethernet.

Impact

This out-of-bounds read issue can lead to internal data being leaked via Ethernet. These data can be potentially sensitive, depending on the application context.

SA0039 - Rev 1 - April 2025
For further information, contact your local STMicroelectronics sales office.

www.st.com

Remediation

To remediate this problem, the user can change the global variable `TxConfig` defined in `src/ethernetif.c` and used inside the `low_level_output` function to be local, or use the thread-safe netifapi APIs of LwIP instead of the netif ones used inside Netif_Config function.

Credit

Moritz Bley, CISPA

Contact information

psirt@st.com

Revision history

Table 1. Document revision history

Date	Version	Changes
04-Apr-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.