Security advisory TN1514-ST-PSIRT: STM32Cube software ETH hardware abstraction layer (HAL) tail pointer management issue

Overview

This security advisory pertains to the STM32Cube software ETH hardware abstraction layer (HAL) tail pointer management issue and potential security impacts.

Affected products

Product[1]	Version	Type	Note
STM32CubeH7	v1.11.1 and earlier	embedded software	-
STM32CubeF4	v1.27.1 and earlier	embedded software	-
STM32CubeF7	v1.17.1 and earlier 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	-
STM32CubeH5	v1.1.1 and earlier 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	v1.8.5 and earlier 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	v1.9.4 and earlier 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	-
STM32CubeMP13	v1.0.0 and earlier 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 STM32Cube Expansion packages (X-CUBE or I-CUBE) could depend on the affected product and are not mentioned in this document. Check if the X-CUBE or I-CUBE packages you are using contain the affected product. And if this is the case, refer to X-CUBE or I-CUBE package release notes to check if the issue has been fixed.*
2. *Release note are available in each downloaded package (on ST.com product pages, on STMicroelectronics Github product pages, via STM32CubeMX).*

Regarding the standalone components offered through GitHub which might be used with the affected products, the following fixes are now available: STMicroelectronics/stm32h7xx_hal_driver at release/v1.11.2 (github.com).

The user will need to reconfigure the affected package with the fixed component.

Description

Tail pointer management issue for the ETH hardware abstraction layer (HAL) for products listed above can lead to a race condition. This race condition can induce a potential vulnerability.

Impact

An attacker with a network access (to a STM32 hardware product that embeds STM32Cube software products listed in Affected products section) can spray packets and cause either a denial of service (by inducing a fault in the Rx DMA channel), or cause packet data to be written to arbitrary addresses.

Remediation

For the products not fixed (or not yet fixed) as described in the Affected products section, the final application developer shall properly manage the tail pointer in accordance with STM32 hardware products reference manual recommendations.

Credit

Matt Keeter, Oxide Computer Company

Contact information

psirt@st.com

Revision history

Table 1. **Document revision history**

Date	Version	Changes
25-Mar-2024	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.