Document ID	Revision	Date	Document category	
AAGS-MA-SA-2026-003	**1**	**2026-11-10**	**Security Advisory**	
Confidentiality level			Status	Page (of)
Public			**Approved**	**1 (3)**

TLP:CLEAR
No Restriction on Distribution

INFORMATION

ASSA ABLOY Global Solutions Marine has become aware of a vulnerability in the IPv4 TCP implementation of the Linux kernel.

A race condition when handling incoming TCP connections can lead to a use-after-free in the kernel. The vulnerability can be triggered over the network and has been rated Critical. It affects Linux kernel versions from 4.4 up to the fixed versions listed below.

The vulnerability affects the following products:

- TilliT – all versions.
- MACS Door Key Bridge – all versions.
- MACS Door Key Hub – all versions.

TilliT and MACS run on Linux, and are therefore affected when deployed on a Linux environment with a vulnerable kernel. The vulnerability is in the Linux kernel and not in TilliT or MACS itself, and is resolved by updating the kernel of the underlying Linux environment.

CVE-2026-98432 (CVSS v3.1 base score 9.8, Critical): https://nvd.nist.gov/vuln/detail/CVE-2026-98432

Affected customers are recommended to update the Linux kernel on all systems running TilliT or MACS:

- Apply the latest kernel security updates from your Linux distribution, and restart the system so that the updated kernel is loaded.
- Verify that the running kernel includes the fix. The vulnerability is fixed in the following upstream Linux kernel versions and later: 5.10.272, 5.15.223, 6.1.190, 6.6.159, 6.12.113, 6.18.56, 7.2.10 and 7.3. Linux distributions often include the fix in kernels with other version numbers, so please refer to your distribution's security advisory for CVE-2026-98432.

If you need assistance, please contact our support using the contact information below.

Rest assured safety and security remain at the core of what we do. Accordingly, we consistently monitor, assess, and optimize our protocols to better ensure the safety and security of our users and technology.

We continuously update our Security Resources Centers with the latest information related to security concerning our products and services and you can find more information about any Security

Public

Advisories:
https://www.assaabloyglobalsolutions.com/en/other-solutions/marine/marine-security-center

CONTACT INFORMATION

If you have any questions about this advisory, please contact our support on

- Europe: +47 32 99 40 26
- USA: +1 954 923 2209

You can also contact us via our new online support tool by registering at:
https://my.assaabloyglobalsolutions.com/assaabloy

REFERENCES

Marine Business Area adheres to a responsible disclosure policy as published on
https://www.assaabloyglobalsolutions.com/en/solutions/solutions-for-marine/marine-security-center/

Public

Document ID	Revision	Date	Document category	
AAGS-MA-SA-2026-003	**1**	**2026-11-10**	**Security Advisory**	
Confidentiality level			Status	Page (of)
Public			**Approved**	**3 (3)**

REVISION HISTORY

Revision	Date	Description
1	2026-11-10	Initial Publication

TERMS OF USE

THIS DOCUMENT IS PROVIDED "AS IS". IT DOES NOT IMPLY ANY KIND OF GUARANTEE, WARRANTY, OR UNDERTAKING, NOR DOES IT EXPAND THE SCOPE OF ANY GUARANTEE, WARRANTY OR UNDERTAKING MADE IN ANY AGREEMENT TO WHICH AN ASSA ABLOY GROUP COMPANY IS A PARTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. ANY USE OF THE INFORMATION CONTAINED HEREIN OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK. ASSA ABLOY GLOBAL SOLUTIONS RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.
A STANDALONE COPY OR PARAPHRASE OF THE TEXT OF THIS DOCUMENT THAT OMITS THE DISTRIBUTION URL IS AN UNCONTROLLED COPY. UNCONTROLLED COPIES MAY LACK IMPORTANT INFORMATION OR CONTAIN FACTUAL ERRORS. THE INFORMATION IN THIS DOCUMENT IS INTENDED SOLY FOR END USERS' LAWFUL USE OF ASSA ABLOY GLOBAL SOLUTIONS PRODUCTS.