DOCUMENT ID: 9AKK108472A7840
REVISION: A
DATE: 2026-06-03

CYBER SECURITY ADVISORY

Vulnerabilities in T-MAC Plus

CVE ID: CVE-2025-14771, CVE-2025-14772, CVE-2025-14773, CVE-2025-14774

Purpose

ABB has a rigorous internal cyber security continuous improvement process which involves regular testing with industry leading tools and periodic assessments to identify potential product issues. Occasionally an issue is determined to be a design or coding flaw with implications that may impact product cyber security.

When a potential product vulnerability is identified or reported, ABB immediately initiates our vulnerability handling process. This entails validating if the issue is in fact a product issue, identifying root causes, determining what related products may be impacted, developing a remediation, and notifying end users and governmental organizations.

The resulting Cyber Security Advisory intends to notify customers of the vulnerability and provide details on which products are impacted, how to mitigate the vulnerability or explain workarounds that minimize the potential risk as much as possible. The release of a Cyber Security Advisory should not be misconstrued as an affirmation or indication of an active threat or ongoing campaign targeting the products mentioned here. If ABB is aware of any specific threats, it will be clearly mentioned in the communication.

The publication of this Cyber Security Advisory is an example of ABB's commitment to the user community in support of this critical topic. Responsible disclosure is an important element in the chain of trust we work to maintain with our many customers. The release of an Advisory provides timely information which is essential to help ensure our customers are fully informed.

Affected products

Product name: **T-MAC Plus**

Product version: **4.0-24**.

Vulnerability IDs

CVE-2025-14771, CVE-2025-14772, CVE-2025-14773, CVE-2025-14774

Summary

ABB is aware of the vulnerabilities in the product version listed above. An update is available that resolves the reported vulnerabilities in the product versions listed above.

An attacker who successfully exploited any of these vulnerabilities could potentially compromise the system in different ways.

Recommended immediate actions

ABB has investigated these vulnerabilities to provide adequate protection to customers. The problem is corrected in the following product versions:

T-MAC Plus version 4.0-25

ABB recommends that customers apply the update at earliest convenience.

Vulnerability severity and details

A vulnerability exists in T-MAC Plus web application and in the interface with card readers included in the product version listed above.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS)[1] for both v3.1[2] and v4.0[3].

The indicated Common Weakness Enumerations (CWE) have been selected from the MITRE CWE list[4].

CVE-2025-14771 File Disclosure in ABB T-MAC Plus web application and in ABB T-MAC plus Server - Default IIS Web Site

File Disclosure in ABB T-MAC Plus web application allows authenticated users to exfiltrate files containing sensitive information via crafted HTTP GET request.

CVSS

CVSS v3.1 Base Score: 9.9
CVSS v3.1 Temporal Score: 9.9
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CVSS v4.0 Score 7.3
CVSS v4.0 Vector: CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:L/VA:H/SC:H/SI:L/SA:H

CWE

CWE-552: Files or Directories Accessible to External Parties

NVD Link: https://nvd.nist.gov/vuln/detail/CVE-2025-14771

CVE-2025-14772 Broken Access Control in ABB T-MAC Plus web application

Broken access controls in ABB T-MAC Plus web application allow unprivileged users to perform administrative operations

CVSS

CVSS v3.1 Base Score: 8.8
CVSS v3.1 Temporal Score: 8.8
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

---

[1] Common Vulnerability Scoring System (CVSS), Forum of Incident Response and Security Teams, Inc., https://www.first.org/cvss/.

[2] For the CVSS v3.1 scoring only the CVSS Base Score and the Temporal Score (if information is available) are considered in this advisory. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

[3] For the CVSS v4.0 scoring only the CVSS Base Metrics and the CVSS Supplemental Metrics (if information is available) are considered in this advisory. The CVSS Environmental and Threat Metrics, which can affect the vulnerability severity, are not provided in this advisory since they reflect the potential impact of a vulnerability within the end-user organizations' computing environment and over time depending on the vulnerability exploit maturity. Therefore, end-user organizations are recommended to analyze their situation and specify the Environmental and Threat Metrics.

[4] Common Weakness Enumeration (CWE), The MITRE Corporation, https://cwe.mitre.org/.

CVSS v4.0 Score	7.3
CVSS v4.0 Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:L/VI:H/VA:H/SC:L/SI:H/SA:H

CWE
CWE-639: Authorization Bypass Through User-Controlled Key

NVD Link: https://nvd.nist.gov/vuln/detail/CVE-2025-14772

CVE-2025-14773 Stored Cross-Site Scripting in ABB T-MAC Plus web application

Stored Cross-Site Scripting (XSS) in ABB T-MAC Plus web application allows authenticated users to execute arbitrary HTML or JavaScript code on victims browser.

CVSS

CVSS v3.1 Base Score:	8.0
CVSS v3.1 Temporal Score:	8.0
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

CVSS v4.0 Score	7.2
CVSS v4.0 Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:A/VC:L/VI:H/VA:H/SC:L/SI:H/SA:H

CWE
CWE-79: Improper Neutralization of Input During Web Page Generation (Cross-Site Scripting)

NVD Link: https://nvd.nist.gov/vuln/detail/CVE-2025-14773

CVE-2025-14774 Communication analysis between the Card Reader and *TP2CardReaderService* daemon

Insecure network protocol in ABB T-MAC Plus allows unauthenticated attackers to perform a denial-of-service (DoS) of the *Card Reader* service.

CVSS

CVSS v3.1 Base Score:	7.4
CVSS v3.1 Temporal Score:	7.4
CVSS v3.1 Vector:	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

CVSS v4.0 Score	7.2
CVSS v4.0 Vector:	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:H/SA:H

CWE
CWE-863: Incorrect Authorization

NVD Link: https://nvd.nist.gov/vuln/detail/CVE-2025-14774

Mitigating factors

Mitigating factors describe conditions and circumstances that make an attack that exploits the vulnerability difficult or less likely to succeed.

Refer to section “General security recommendations” for further advise on how to keep your system secure.

CVE-2025-14771 Mitigating factor
The misconfigurations on the IIS server, which were reported to security auditing, have been corrected. File Browsing Feature was enabled on that IIS server. That feature along with the default IIS site has been removed.

CVE-2025-14772 Mitigating factor
ABB T-MAC Plus web application supports several classes of users (e.g., *Admin*, *Customer*, *Operator*, etc.) with different roles. An authenticated user with low privileges (e.g., *Customer*) can execute administrative operations. The privileges associated to the different users have been revised and applied correctly.

CVE-2025-14773 Mitigating factor
A DOM-based XSS vulnerability is present. If a malicious actor gains access to the operations network and can create or edit an existing entity, they could insert malicious JavaScript code to be executed in the web forms. New T-MAC Plus version 4.0-25 will correct the vulnerability.

CVE-2025-14774 Mitigating factor
If a malicious actor gains physical access to a serial device, disables it, connects a malicious device with same IP address, and sends a specially crafted message, the service responsible for communicating with the device will be blocked until a manual restart is performed. New T-MAC Plus version 4.0-25 will correct the vulnerability.

Workarounds

Workarounds are specific measures that a user can take to help block an attack, for example, temporarily disabling the vulnerable feature may remove the exposure with well-known impact on functionality. ABB has tested the following workarounds. Although these workarounds will not correct the underlying vulnerability, they can help block known attack vectors. When a workaround reduces functionality, this is identified below as “Impact of workaround”.

Frequently asked questions

What causes the vulnerability?

The vulnerabilities are caused by:

- Wrong configuration in T-MAC Plus IIS Server.
- Wrong configuration of privileges of users.
- Lack of encryption in communication protocol.

What is T-MAC Plus?

T-MAC Plus is a Terminal Management System (TMS) that handles the different operations (receipt and dispatch product, access control, product movement in the tank farm, …) in a terminal. It is applicable to different type of products such as chemical and petroleum terminals, pipeline or refinery tankage, bulk plants or hydrogen terminals.

The following components are affected:

- TMAC Plus Web application
- Communication protocol with Card Readers

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause the affected system node to stop or become inaccessible and allow the attacker to insert and run arbitrary code.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected system node. This would require that the attacker has access to the system network, by connecting to the network directly. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

No, to exploit this vulnerability an attacker would need to have physical access to an affected system node.

Can functional safety be affected by an exploit of this vulnerability?

While these vulnerabilities primarily impact confidentiality, integrity, and availability, they do not directly affect functional safety in the traditional sense.

What does the update do?

The update removes the vulnerability by modifying the way that the T-MAC Plus web application and the communication protocol are configured.

When this security advisory was issued, had this vulnerability been publicly disclosed?

No, ABB received information about this vulnerability through responsible disclosure.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?

No, ABB had not received any information indicating that this vulnerability had been exploited when this security advisory was originally.

General security recommendations

For any installation of software-related ABB products we strongly recommend the following (non-exhaustive) list of cyber security practices:

– Isolate special purpose networks (e.g. for automation systems) and remote devices behind firewalls and separate them from any general-purpose network (e.g. office or home networks).

- Install physical controls so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.
- Never connect programming software or computers containing programing software to any network other than the network for the devices that it is intended for.
- Scan all data imported into your environment before use to detect potential malware infections.
- Minimize network exposure for all applications and endpoints to ensure that they are not accessible from the Internet unless they are designed for such exposure and the intended use requires such.
- Ensure all nodes are always up to date in terms of installed software, operating system, and firmware patches as well as anti-virus and firewall.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

Acknowledgement

ABB acknowledges and thanks Angelo Catalani from the Italian National Cybersecurity Agency (ACN) for responsibly disclosing the vulnerabilities and providing valuable input on product improvements.

Support

For additional instructions and support please contact your local ABB service organization. For contact information, see www.abb.com/contactcenters.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	2026-06-03