DOCUMENT ID: 2CRT000006
REVISION: B
DATE: 2025-05-19

CYBER SECURITY ADVISORY

ANC – ABB Network Card
Multiple vulnerabilities in ANC

CVE ID: CVE-2024-47784, CVE-2024-9876, CVE-2024-9877

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from ABB, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

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

ANC Product	Software version
ANC	<= 1.1.4
ANC-L	
ANC-mini	<= 1.1.4

Vulnerability IDs

CVE-2024-47784, CVE-2024-9876, CVE-2024-9877

Summary

An update is available that resolves internally discovered vulnerabilities in the product versions listed above.

Depending upon the vulnerability, an attacker with the access to the local network who successfully exploited this vulnerability could escalate the privilege to device admin and take control of the product.

Recommended immediate actions

All web HMI related problems (CVE-2024-47784, CVE-2024-9876, CVE-2024-9877) are corrected in the product software version 1.1.5.

ABB recommends that customers apply the update at earliest convenience. The process to identify the installed product version and process to install updates is described in the user manual.

Vulnerability severity and details

Vulnerabilities exists in the ANC – ABB Network Card included in the product software versions listed above. An attacker could exploit the vulnerabilities CVE-2024-47784, CVE-2024-9876, CVE-2024-9877 by sending specially crafted HTTP packets to escalate the privilege to device admin, resulting in product takeover.

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-2024-47784 Unverified Password Change

An unverified password change in ANC software version <= 1.1.4 allows an authenticated attacker to bypass the old Password check in the password change form via a web HMI. Requiring the old password is a common security practice that adds an extra layer of protection against unauthorized changes. Without the need of old password attacker with even a temporary access to user's session could easily change the password and lock out the legitimate user.

This problem is resolved in software version 1.1.5.

CVSS

CVSS v3.1 Base Score:	2.6 (Low)
CVSS v3.1 Temporal Score:	2.5 (Low)
CVSS v3.1 Vector:	CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N/RL:O/RC:C
CVSS v4.0 Score	2.1 (Low)
CVSS v4.0 Vector:	CVSS:4.0/AV:A/AC:H/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/R:U

CWE

CWE-620: Unverified Password Change

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-47784

[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/.

CVE-2024-9876 Application is vulnerable to Privilege escalation

A non-administrative user could gain access to an admin page where they could perform all actions which should be restricted only to an admin user. The vulnerability was due to improper validation in the web HMI server.

This problem is resolved in software version 1.1.5, apply the update at earliest convenience.

CVSS

CVSS v3.1 Base Score:	7.3 (High)
CVSS v3.1 Temporal Score:	7.0 (High)
CVSS v3.1 Vector:	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/RL:O/RC:C
CVSS v4.0 Score	8.5 (High)
CVSS v4.0 Vector:	CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/-SA:N/U:Amber

CWE
CWE-471: Modification of Assumed-Immutable Data (MAID)

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-9876

CVE-2024-9877 Sensitive information submitted using GET method

The use of GET request method with sensitive query strings vulnerability allows an attacker to view plaintext password, if the attacker is able to read the GET requests to those services.

This problem is resolved in software version 1.1.5, apply the update at earliest convenience.

CVSS

CVSS v3.1 Base Score:	4.3 (Medium)
CVSS v3.1 Temporal Score:	4.1 (Medium)
CVSS v3.1 Vector:	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/RL:O/RC:C
CVSS v4.0 Score	5.3 (Medium)
CVSS v4.0 Vector:	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/-SA:N/U:Amber

CWE
CWE-598: Use of GET Request Method With Sensitive Query Strings

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-9877

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.

Frequently asked questions

What causes the vulnerability?

Different vulnerabilities addressed in this advisory have different causes. Please refer to section “Vulnerability severity and details” for more information.

Can vulnerabilities affect connected UPS?

These vulnerabilities cannot affect or disrupt functionality of connected UPS in any way.

What is ANC?

ANC is ABB Network Card for UPS. It provides full, secure connectivity for remote monitoring and management of your uninterruptible power supply. User can monitor UPS with the ABB Network Card via web browser or via network management software which supports SNMP or MODBUS protocol over TCP/IP or RS485.

What is web server?

It is a web server hosted by ANC. ANC being a telemetry device, purpose of web server is to look and search for information regarding the UPS system status, the module status, and so on.

What might an attacker use the vulnerability to do?

Refer to section “Vulnerability severity and details”.

How could an attacker exploit the vulnerability?

Different vulnerabilities addressed in this advisory have different attack vectors. Prerequisite for successful exploitation of either of the vulnerabilities mentioned in this advisory would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section “Mitigating Factors” in addition to section “General security recommendations”.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability. Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

What does the update do?

The update removes vulnerabilities CVE-2024-47784, CVE-2024-9876 and CVE-2024-9877 by modifying the way that the ANC authenticates users, maintains session and updates password.

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 issued.

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.

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	2025-04-30
B	(p) 4	Added NVD link to all vulnerabilities	2025-05-19