DOCUMENT ID: 9AKK108471A4462
REVISION: F
DATE: 2025-09-04

CYBER SECURITY ADVISORY

ELSB/BLBA
ASPECT advisory several CVEs.

CVE ID: Several CVEs see table

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 one is determined to be a design or coding issue 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.

Assessed products

Platform	Model number	ABB Product ID	Affected firmware Version
ASPECT®-Enterprise	ASP-ENT-x	2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021	<3.08.04-s01
NEXUS Series	NEX-2x, NEXUS-3-x	2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021	<3.08.04-s01
MATRIX Series	MAT-x	2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021	<3.08.04-s01

Note: All the Platforms listed above are defined as ASPECT in the subsequent document.

Vulnerability IDs

No.	CVE ID	Title	Affected SW version	Fixed in Version
1	CVE-2025-53187	Authentication bypass due to a SW configuration issue	<3.08.04-s01	>=3.08.04-s01
2	CVE-2025-7677	DOS attack possible	All versions	no plans of corrective measures
3	CVE-2025-7679	Session ID Basic Auth Bypass	All versions	no plans of corrective measures

Summary

General statement

ABB became aware of vulnerabilities in ASPECT versions listed above. The earliest report dates to June 2023. ABB has fixed most of the vulnerabilities reported. At the moment there are no plans of corrective measures for remaining vulnerabilities in the affected products.

ASPECT is an on-premise Building Management System (BMS) that provides an additional option to be remotely accessible. In order to support customers' demand for cloud connectivity, ABB has decided to replace ASPECT and will introduce customers to a new solution based on the latest Industry level cyber security standards. The new solution will bring HW and SW capabilities that reflect state-of-the-art technology and is delivered including a maintenance plan that offers customers the best planning security.

Customers who have concerns about continuing the operation of ASPECT may contact ABB sales service to become advised about further support options.

Statement on newly reported vulnerabilities

ASPECT devices are not intended to be internet-facing. A product advisory issued in June 2023 informed customers regarding this fact.

An attacker who successfully exploits these vulnerabilities could potentially gain unauthorized access and potentially compromise the system's - and log-file-confidentiality, integrity and availability.

ABB requires, as noted in previous security advisories and user documentation, that ASPECT should not be exposed to the Internet or any other unsecured network.

Note: To exploit ASPECT, an attacker would need a misconfigured system.

ABB strongly advises customers and system integrators to follow the instructions documented in: FBXi, CBXi and ASPECT® SOLUTIONS, which can be downloaded from the ABB library.

Recommended immediate actions

Please immediately do the following actions on any released SW version of ASPECT:

- Stop and disconnect any ASPECT products that are exposed directly to the Internet, either via a direct ISP connection or via NAT port forwarding
- Ensure that physical controls are in place, so no unauthorized personnel can access your devices, components, peripheral equipment, and networks
- Ensure log-files, downloaded from the equipment is protected against unauthorized access
- Ensure that all ASPECT products are upgraded to the latest firmware version. Please find the latest version of ASPECT firmware on the respective product homepage
- When remote access is required, only use secure methods. If a Virtual Private Network (VPN) is used, ensure that the chosen VPN is secure i.e. updated to the most current version available and configured for secure access

Vulnerability severity and details

ABB has become aware of vulnerabilities.

An attacker who successfully exploited this vulnerability might be able to:

- Can tamper with data and compromise integrity

Customers who operate instances of ASPECT and exposing its ports through the Internet e.g. to support remote access, are requested to disconnect and isolate the devices immediately.

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

The following CVSS v3.1 and CVSS v4.0 scores of below listed CVE's, rate the severity of the respective vulnerability based on an ASPECT system which is installed and configured in accordance with ABB specifications.

Note: In accordance with ABB specifications, ASPECT should never be exposed to the Internet.

No.	CVE ID	Title	
1	CVE-2025-53187	Authentication bypass due to a SW configuration issue <3.08.04-s01	
	Source	Researcher	
	Status	Fixed	
	Description	Due to an issue in configuration, code that was intended for debugging purposes, was included in the market release of the ASPECT FW allowing to bypass authentication in particular context. An attacker was able to change the system time, access files and make function calls (RCE) without prior authentication. This issue affects all versions of ASPECT <3.08.04-s01	
	CWE	CWE-288: Authentication Bypass Using an Alternate Path or Channel	
	CVSS v3.1	Base Score:	9.8
		Temporal Score:	9.8
		Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
	CVSS v4.0	Score	9.3
		Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-53187	
2	CVE-2025-7677	DOS attack possible	
	Source	Researcher	
	Status	no plans of corrective measures	

[1] 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.

[2] 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.

	Description	A DoS attack is possible if access to the local network is provided to unauthorized users. Due to a copy issue in a buffer that may lead to a SW crash, the device appears out of order. This issue affects all versions of ASPECT.	
	CWE	CWE-120 Buffer Copy without checking size of input	
	CVSS v3.1	Base Score:	5.9
		Temporal Score:	5.9
		Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
	CVSS v4.0	Score:	8.2
		Vector:	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-7677	
3	CVE-2025-7679	Session ID Basic Auth Bypass	
	Source	Researcher	
	Status	no plans of corrective measures	
	Description	The ASPECT system allows users to bypass authentication. This issue affects all versions of ASPECT	
	CWE	CWE-288: Authentication Bypass Using an Alternate Path or Channel	
	CVSS v3.1	Base Score:	8.1
		Temporal Score:	8.1
		Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
	CVSS v4.0	Score:	9.2
		Vector:	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-7679	

Mitigating factors

The vulnerabilities reported in scope of this document are only exploitable if attackers can access the network segment where ASPECT is installed and exposed directly to the internet. ABB therefore recommends the following guidelines to protect customer networks:

- ASPECT devices should never be exposed directly to the Internet either via a direct ISP connection nor via NAT port forwarding. If remote access to an ASPECT system is a customer requirement, the system shall operate behind a firewall. Users accessing ASPECT remotely shall do this using a VPN Gateway allowing access to the network segment where ASPECT is installed and configured
- Note: it is crucial that the VPN Gateway and Network is set up in accordance with best industry standards and maintained in terms of security patches for all related components
- Authorized users shall change all default credentials during commissioning of an ASPECT system. If credentials have not been changed during commission state, ABB advises to change each changeable credential at the earliest
- Ensure that all ASPECT products are upgraded to the latest firmware version. Please find the latest version of ASPECT firmware on the respective product homepage

Frequently asked questions

What causes the vulnerabilities?

These vulnerabilities have possible root causes in missing hardware supported secure storage and system integrity protection.

What is ASPECT?

ASPECT is intended to collect energy data. Based on the values of the collected energy data, ASPECT may trigger controls to optimize energy consumption in a building.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability might be able to:

- Intercept the connection between two or more ASPECT instances
- Can decrypt usernames and passwords stored in the devices database
- Can tamper with data and compromise integrity

If one of these vulnerabilities has been successfully exploited by an attacker, this could allow the attacker to take control of the system node. Furthermore, it allows the attacker to insert and run arbitrary code.

How could an attacker exploit the vulnerability?

An attacker who successfully exploits this vulnerability may decrypt data transferred to or from the product or stored inside or outside the product.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit one or more of these vulnerabilities. Recommended practices include ensuring process control systems are physically protected, have no direct connections to the Internet nor any other untrusted network, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

Can functional safety be affected by an exploitation of one of these vulnerabilities?

ASPECT is not designed as a functional safety device.

Is a software update available to address the issue?

On the day this advisory has been published, ABB has no firmware update available to fully remedy the issue. Customers are advised to apply the mitigating actions described in this document, to prevent potential attackers from making use of the credentials that may be publicly available.

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

Some issues were publicly disclosed while others were not.

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 and especially for products in scope of the ASPECT product line, we strongly recommend the following (non-exhaustive) list of cyber security practices:

- Ensure that all ASPECT products are upgraded to the latest firmware version. Please find the latest version of ASPECT firmware on the respective product homepage
- 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 ASPECT ports and endpoints to ensure that they are not accessible directly from the Internet
- 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
- Authorized users shall change all default credentials during commissioning of an ASPECT system. If credentials have not been changed during commission state, ABB advises to change each changeable credential at the earliest

More information on recommended practices can be found in the following documents:

HT0038	FBXi, CBXi and ASPECT® SOLUTIONS

Acknowledgement

ABB acknowledges Gjoko Krstikj, Zero Science Lab, for reporting vulnerabilities in responsible disclosure.

References

HT0038	FBXi, CBXi and ASPECT® SOLUTIONS

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	2025-11-08
B	6	Corrected CVE values	2025-12-08
C	4-6	Corrected CVSS vectors and scores accordingly.	2025-12-08
D	4-6	Merging CVEs due to a common root cause The following CVE's have been rejected/removed by ABB: - CVE-2025-53188 - CVE-2025-53189 - CVE-2025-53190 - CVE-2025-53191	2025-21-08
E	4-6	Adopted CWE values and titles to match the CVE a bit better.	2025-27-08
F	4-6	Adopted some values in CVSS4.0 score to match with the corresponding CVSS3.1 score or the same CVE.	2025-04-09