DOCUMENT ID: 9AKK108471A0021
REVISION: C
DATE: 2025-05-23

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.

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	<=3.08.03
NEXUS Series	NEX-2x, NEXUS-3-x	2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021	<=3.08.03
MATRIX Series	MAT-x	2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021	<=3.08.03

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-2024-48853	Authenticated Escalation to guest to root	<=3.08.03	3.08.04
2	CVE-2024-48850	Authenticated Absolute Path Traversal	<=3.08.03	3.08.04
3	CVE-2024-9639	Authenticated Remote Code Execution	<=3.08.03	3.08.04

No.	CVE ID	Title	Affected SW version	Fixed in Version
4	CVE-2025-2410	CLASSIFICATION: Admin Authorized Port (iptables) manipulation (open/close/disable ports)	<=3.08.03	3.08.04
5	CVE-2025-2409	CLASSIFICATION: Admin Authorized System File corruption	<=3.08.03	3.08.04
6	CVE-2025-30170	CLASSIFICATION: Admin Authorized Exposure of file path, file size or file existence	<=3.08.03	3.08.04
7	CVE-2025-30171	CLASSIFICATION: Admin Authorized System File Deletion	<=3.08.03	3.08.04
8	CVE-2025-30172	CLASSIFICATION: Admin Authorized Remote Code Execution	<=3.08.03	3.08.04
9	CVE-2025-30173	CLASSIFICATION: Admin Authorized File Upload	<=3.08.03	3.08.04
10	CVE-2025-30169	CLASSIFICATION: Admin Authorized File Upload and Execute PHP	<=3.08.03	3.08.04
11	CVE-2024-13928	Authenticated SQL Injection	<=3.08.03	3.08.04
12	CVE-2024-13929	Authenticated Servlet Command Injection	<=3.08.03	3.08.04
13	CVE-2024-13930	Authenticated Unchecked Loop Condition	<=3.08.03	3.08.04
14	CVE-2024-13931	Authenticated Relative Path Traversal	<=3.08.03	3.08.04
15	CVE-2024-13945	Stored Absolute Path Traversal	<=3.08.03	no plans of corrective measures
16	CVE-2024-13946	Binary Planting / LoadLibrary DLL's not Signed	<=3.08.03	no plans of corrective measures
18	CVE-2024-13947	External System or Configuration Control	<=3.08.03	no plans of corrective measures
19	CVE-2024-13948	Insecure Permissions	<=3.08.03	no plans of corrective measures
20	CVE-2024-48848	LARGECONTENT - device disk overutilization	<=3.08.03	no plans of corrective measures
21	CVE-2024-13949	Log Forging	<=3.08.03	no plans of corrective measures
22	CVE-2024-13950	Log Injection	<=3.08.03	no plans of corrective measures
23	CVE-2024-13951	One way hash with predictable salt	<=3.08.03	no plans of corrective measures

No.	CVE ID	Title	Affected SW version	Fixed in Version
24	CVE-2024-51553	Predictable Filename	<=3.08.03	no plans of corrective measures
25	CVE-2024-13952	Remote Code Execution	<=3.08.03	no plans of corrective measures
26	CVE-2024-13953	Sensitive Information disclosed in log files	<=3.08.03	no plans of corrective measures
27	CVE-2024-13954	Serialization / Deserialization of configuration data	<=3.08.03	no plans of corrective measures
28	CVE-2024-13955	SQL Injection 2nd Order	<=3.08.03	no plans of corrective measures
29	CVE-2024-13956	SSL Verification Bypass	<=3.08.03	no plans of corrective measures
30	CVE-2024-13957	SSRF Server Side Request Forgery	<=3.08.03	no plans of corrective measures
31	CVE-2024-13958	Stored Cross Site Scripting	<=3.08.03	no plans of corrective measures
32	CVE-2024-51552	Weak Password Storage	<=3.08.03	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] 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.

1	CVE-2024-48853	Authenticated Escalation to guest to root	
	Source	Researcher	
	Status	Fixed	
	Description	An escalation of privilege vulnerability in ASPECT could provide an attacker root access to a server when logged in as a "non" root ASPECT user. This issue affects ASPECT <= 3.08.03	
	CWE	CWE-286: Incorrect User Management	
	CVSS v3.1	Base Score:	9.0
		Temporal Score:	9.0
		Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
	CVSS v4.0	Score	9.5
		Vector:	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/S:N/AU:N/R:U/V:C/U:Clear
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-48853	
2	CVE-2024-48850	Authenticated Absolute Path Traversal	
	Source	Researcher	
	Status	Fixed	
	Description	Absolute File Traversal vulnerabilities in ASPECT allows access and modification of unintended resources. This issue affects ASPECT<= 3.08.03	
	CWE	CWE-36: Absolute Path Traversal	
	CVSS v3.1	Base Score:	7.2
		Temporal Score:	7.2
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
	CVSS v4.0	Score	7.5
		Vector:	CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/S:N/AU:N/R:U/V:C/U:Clear
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-48850	
3	CVE-2024-9639	Authenticated Remote Code Execution	
	Source	Researcher	
	Status	Fixed	
	Description	Remote Code Execution vulnerabilities are present in ASPECT if session administrator credentials become compromised. This issue affects ASPECT<= 3.08.03	
	CWE	CWE-94: Improper Control of Generation of Code ('Code Injection')	
	CVSS v3.1	Base Score:	8.0
		Temporal Score:	8.0
		Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H
	CVSS v4.0	Score	7.5
		Vector:	CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/S:N/AU:N/R:U/V:C/U:Clear
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-9639	
4	CVE-2025-2410	Admin Authorized Port (iptables) manipulation (open/close/disable ports)	
	Source	ABB	
	Status	Fixed	

	Description	Port manipulation vulnerabilities in ASPECT provide attackers with the ability to control TCP/IP port access if session administrator credentials become compromised. This issue affects ASPECT <= 3.08.03.	
	CWE	CWE-99: Improper Control of Resource Identifiers ('Resource Injection')	
	CVSS v3.1	Base Score:	9.1
		Temporal Score:	9.1
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
	CVSS v4.0	Score	8.9
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/S:N/AU:N/R:U/V:C/U:Clear
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-2410	
5	CVE-2025-2409	Admin Authorized System File corruption	
	Source	ABB	
	Status	Fixed	
	Description	File corruption vulnerabilities in ASPECT provide attackers access to overwrite system files if session administrator credentials become compromised. This issue affects ASPECT <= 3.08.03.	
	CWE	CWE-73: External Control of File Name or Path	
	CVSS v3.1	Base Score:	9.1
		Temporal Score:	9.1
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
	CVSS v4.0	Score	8.9
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/S:N/AU:N/R:U/V:C/U:Clear
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-2409	
6	CVE-2025-30170	Admin Authorized Exposure of file path, file size or file existence	
	Source	ABB	
	Status	Fixed	
	Description	Exposure of file path, file size or file existence vulnerabilities in ASPECT provide attackers access to file system information if session administrator credentials become compromised. This issue affects ASPECT <= 3.08.03	
	CWE	CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere	
	CVSS v3.1	Base Score:	5.5
		Temporal Score:	5.5
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:N
	CVSS v4.0	Score	5.9
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N/S:N/AU:N/R:U/V:C/U:Clear
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-30170	
7	CVE-2025-30171	Admin Authorized System File Deletion	
	Source	ABB	
	Status	Fixed	

	Description	System File Deletion vulnerabilities in ASPECT provide attackers access to delete system files if session administrator credentials become compromised. This issue affects ASPECT <= 3.08.03	
	CWE	CWE-863: Incorrect Authorization	
	CVSS v3.1	Base Score:	9.0
		Temporal Score:	9.0
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:H/A:H
	CVSS v4.0	Score	7.3
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:L/VI:H/VA:H/SC:L/SI:H/SA:H/S:N/AU:N/R:U/V:C/U:Clear
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-30171	
8	CVE-2025-30172	Admin Authorized Remote Code Execution	
	Source	ABB	
	Status	Fixed	
	Description	Remote Code Execution vulnerabilities are present in ASPECT if session administrator credentials become compromised. This issue affects ASPECT<= 3.08.03	
	CWE	CWE-94: Improper Control of Generation of Code ('Code Injection')	
	CVSS v3.1	Base Score:	8.0
		Temporal Score:	8.0
		Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H
	CVSS v4.0	Score	8.9
		Vector:	CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/S:N/AU:N/R:U/V:C/U:Clear
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-30172	
9	CVE-2025-30173	Admin Authorized File Upload	
	Source	ABB	
	Status	Fixed	
	Description	File upload vulnerabilities are present in ASPECT if session administrator credentials become compromised. This issue affects ASPECT <= 3.08.03	
	CWE	CWE-434: Unrestricted Upload of File with Dangerous Type	
	CVSS v3.1	Base Score:	6.7
		Temporal Score:	6.7
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:H
	CVSS v4.0	Score	6.0
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N/S:N/AU:N/R:U/V:C/U:Clear
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-30173	
10	CVE-2025-30169	Admin Authorized File Upload and Execute PHP	
	Source	ABB	
	Status	Fixed	
	Description	File upload and execute vulnerabilities in ASPECT allow PHP script injection if session administrator credentials become compromised. This issue affects ASPECT <= 3.08.03	
	CWE	CWE-434: Unrestricted Upload of File with Dangerous Type	

	CVSS v3.1	Base Score:	6.7
		Temporal Score:	6.7
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:H
	CVSS v4.0	Score	6.0
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N/S:N/AU:N/R:U/V:C/U:Clear
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-30169	
11	CVE-2024-13928	Authenticated SQL Injection	
	Source	Researcher	
	Status	Fixed	
	Description	SQL injection vulnerabilities in ASPECT allow unintended access and manipulation of database repositories if session administrator credentials become compromised. This issue affects ASPECT <= 3.08.03	
	CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	
	CVSS v3.1	Base Score:	7.2
		Temporal Score:	7.2
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
	CVSS v4.0	Score	6.0
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/S:N/AU:N/R:U/V:C/U:Clear
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-13928	
12	CVE-2024-13929	Authenticated Servlet Command Injection	
	Source	Researcher	
	Status	Fixed	
	Description	Servlet injection vulnerabilities in ASPECT allow remote code execution if session administrator credentials become compromised. This issue affects ASPECT <= 3.08.03	
	CWE	CWE-94: Improper Control of Generation of Code ('Code Injection')	
	CVSS v3.1	Base Score:	7.2
		Temporal Score:	7.2
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
	CVSS v4.0	Score	7.5
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/S:N/AU:N/R:U/V:C/U:Clear
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-13929	
13	CVE-2024-13930	Authenticated Unchecked Loop Condition	
	Source	Researcher	
	Status	Fixed	
	Description	An Unchecked Loop Condition in ASPECT provides an attacker the ability to maliciously consume system resources if session administrator credentials become compromised. This issue affects ASPECT <= 3.08.03	
	CWE	CWE-606: Unchecked Input for Loop Condition	

	CVSS v3.1	Base Score:	4.9
		Temporal Score:	4.9
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H
	CVSS v4.0	Score	5.9
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/S:N/AU:N/R:U/V:C/U:Clear
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-13930	
14	CVE-2024-13931	Authenticated Relative Path Traversal	
	Source	Researcher	
	Status	Fixed	
	Description	Relative Path Traversal vulnerabilities in ASPECT allow access to file resources if session administrator credentials become compromised. This issue affects ASPECT <= 3.08.03	
	CWE	CWE-23: Relative Path Traversal	
	CVSS v3.1	Base Score:	7.2
		Temporal Score:	7.2
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
	CVSS v4.0	Score	7.5
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/S:N/AU:N/R:U/V:C/U:Clear
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-13931	
15	CVE-2024-13945	Stored Absolute Path Traversal	
	Source	Researcher	
	Status	no plans of corrective measures	
	Description	Stored Absolute Path Traversal vulnerabilities in ASPECT could expose sensitive data if administrator credentials become compromised. This issue effects all versions of ASPECT.	
	CWE	CWE-36: Absolute Path Traversal	
	CVSS v3.1	Base Score:	6.0
		Temporal Score:	6.0
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:L
	CVSS v4.0	Score	8.4
		Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:L/VA:L/SC:H/SI:L/SA:L
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-13945	
16	CVE-2024-13946	Binary Planting / LoadLibrary DLL's not Signed	
	Source	Researcher	
	Status	no plans of corrective measures	
	Description	DLL's are not digitally signed when loaded in ASPECT's configuration toolset exposing the application to binary planting during device commissioning. This issue affects all versions of ASPECT.	
	CWE	CWE-427: Uncontrolled Search Path Element	
	CVSS v3.1	Base Score:	6.8
		Temporal Score:	6.4

		Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:L/E:P/RL:U/RC:C/CR:M/IR:M/AR:L
	CVSS v4.0	Score	7.1
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:H/VI:L/VA:L/SC:H/SI:L/SA:L
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-13946	
18	CVE-2024-13947	External System or Configuration Control	
	Source	Researcher	
	Status	no plans of corrective measures	
	Description	Device commissioning parameters in ASPECT may be modified by an external source if administrative credentials become compromised. This issue affects all versions of ASPECT.	
	CWE	CWE-863: Incorrect Authorization	
	CVSS v3.1	Base Score:	6.0
		Temporal Score:	6.0
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:L
	CVSS v4.0	Score	7.1
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:H/VI:L/VA:L/SC:H/SI:L/SA:L
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-13947	
19	CVE-2024-13948	Insecure Permissions	
	Source	Researcher	
	Status	no plans of corrective measures	
	Description	Windows permissions for ASPECT configuration toolsets are not fully secured allowing exposure of configuration information. This issue affects all versions of ASPECT.	
	CWE	CWE-276: Incorrect Default Permissions	
	CVSS v3.1	Base Score:	7.3
		Temporal Score:	7.3
		Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N
	CVSS v4.0	Score	7.3
		Vector:	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:L/VA:N/SC:H/SI:L/SA:N
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-13948	
20	CVE-2024-48848	LARGECONTENT - device disk overutilization	
	Source	Researcher	
	Status	no plans of corrective measures	
	Description	Large content vulnerabilities are present in ASPECT exposing a device to disk overutilization on a system if administrator credentials become compromised. This issue affects all versions of ASPECT.	
	CWE	CWE-774: Allocation of File Descriptors or Handles Without Limits or Throttling	
	CVSS v3.1	Base Score:	6.5
		Temporal Score:	6.5
		Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

	CVSS v4.0	Score	7.0
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-48848	
21	CVE-2024-13949	Log Forging	
	Source	Researcher	
	Status	no plans of corrective measures	
	Description	Log forging vulnerabilities in ASPECT provide attacker access to manipulate log messages with false information if administrator credentials become compromised. This issue affects all versions of ASPECT.	
	CWE	CWE-117: Improper Output Neutralization for Logs	
	CVSS v3.1	Base Score:	6.8
		Temporal Score:	6.8
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N
	CVSS v4.0	Score	6.9
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:N/VI:H/VA:N/SC:N/SI:H/SA:N
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-13949	
22	CVE-2024-13950	Log Injection	
	Source	Researcher	
	Status	no plans of corrective measures	
	Description	Log injection vulnerabilities in ASPECT provide attacker access to inject malicious browser scripts if administrator credentials become compromised. This issue affects all versions of ASPECT.	
	CWE	CWE-79: Improper Neutralization of Input During Web Page Generation	
	CVSS v3.1	Base Score:	6.8
		Temporal Score:	6.8
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N
	CVSS v4.0	Score	6.9
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:N/VI:H/VA:N/SC:N/SI:H/SA:N
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-13950	
23	CVE-2024-13951	One way hash with predictable salt	
	Source	Researcher	
	Status	no plans of corrective measures	
	Description	One way hash with predictable salt vulnerabilities in ASPECT may expose sensitive information to a potential attacker. This issue affects all versions of ASPECT.	
	CWE	CWE-760: Use of a One-Way Hash with a Predictable Salt	
	CVSS v3.1	Base Score:	7.6
		Temporal Score:	7.6
		Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L
	CVSS v4.0	Score	6.1
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:L/VA:L/SC:N/SI:L/SA:L

	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-13951	
24	CVE-2024-51553	Predictable Filename	
	Source	Researcher	
	Status	no plans of corrective measures	
	Description	Predictable filename vulnerabilities in ASPECT may expose sensitive information to a potential attacker if administrator credentials become compromised. This issue affects all versions of ASPECT.	
	CWE	CWE-73: External Control of File Name or Path	
	CVSS v3.1	Base Score:	6.5
		Temporal Score:	6.5
		Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
	CVSS v4.0	Score	7.0
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:N/VA:N/SC:H/SI:N/SA:N
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-51553	
25	CVE-2024-13952	Remote Code Execution	
	Source	Researcher	
	Status	no plans of corrective measures	
	Description	Remote Code Execution vulnerabilities are present in ASPECT if administrator credentials become compromised . This issue affects all versions of ASPECT.	
	CWE	CWE-94: Improper Control of Generation of Code	
	CVSS v3.1	Base Score:	8.4
		Temporal Score:	8.4
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H
	CVSS v4.0	Score	8.7
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:A/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-13952	
26	CVE-2024-13953	Sensitive Information disclosed in log files	
	Source	Researcher	
	Status	no plans of corrective measures	
	Description	Sensitive device logger information in ASPECT may be exposed if administrator credentials become compromised. This issue affects all versions of ASPECT.	
	CWE	CWE-359: Exposure of Private Information ('Privacy Violation')	
	CVSS v3.1	Base Score:	4,9
		Temporal Score:	4.9
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N
	CVSS v4.0	Score	6.9
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:H/VI:N/VA:N/SC:H/SI:N/SA:N
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-13953	
27	CVE-2024-13954	Serialization / Deserialization of configuration data	
	Source	Researcher	

	Status	no plans of corrective measures	
	Description	Serialized configuration information may be disclosed during device commissioning while using ASPECT's configuration toolset. This issue affects all versions of ASPECT.	
	CWE	CWE-922: Insecure Storage of Sensitive Information	
	CVSS v3.1	Base Score:	6.5
		Temporal Score:	6.5
		Vector	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L
	CVSS v4.0	Score	5.1
		Vector:	CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:L/SI:L/SA:L
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-13954	
28	CVE-2024-13955	SQL Injection 2nd Order	
	Source	Researcher	
	Status	no plans of corrective measures	
	Description	2nd Order SQL injection vulnerabilities in ASPECT allow unintended access and manipulation of database repositories if administrator credentials become compromised. This issue affects all versions of ASPECT.	
	CWE	CWE-89 – SQL Injection	
	CVSS v3.1	Base Score:	8.8
		Temporal Score:	8.8
		Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
	CVSS v4.0	Score	9.4
		Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-13955	
29	CVE-2024-13956	SSL Verification Bypass	
	Source	Researcher	
	Status	no plans of corrective measures	
	Description	SSL Verification Bypass vulnerabilities exist in ASPECT if administrator credentials become compromised. This issue affects all versions of ASPECT.	
	CWE	CWE-295: Improper Certificate Validation	
	CVSS v3.1	Base Score:	6.7
		Temporal Score:	6.7
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:L
	CVSS v4.0	Score	8.8
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:H/VI:H/VA:L/SC:H/SI:H/SA:L
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-13956	
30	CVE-2024-13957	SSRF Server Side Request Forgery	
	Source	Researcher	
	Status	no plans of corrective measures	
	Description	SSRF Server Side Request Forgery vulnerabilities exist in ASPECT if administrator credentials become compromised. This issue affects all versions of ASPECT.	
	CWE	CWE-918 – Server-Side Request Forgery (SSRF)	

	CVSS v3.1	Base Score:	7.6
		Temporal Score:	7.6
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:L/A:N
	CVSS v4.0	Score	7.0
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:H/VI:L/VA:N/SC:H/SI:L/SA:N
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-13957	
31	CVE-2024-13958	Stored Cross Site Scripting	
	Source	Researcher	
	Status	no plans of corrective measures	
	Description	Stored Cross Site Scripting vulnerabilities exist in ASPECT if administrator credentials become compromised. This issue affects all versions of ASPECT.	
	CWE	CWE-79 – Stored XSS	
	CVSS v3.1	Base Score:	4.8
		Temporal Score:	4.8
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
	CVSS v4.0	Score	4.6
		Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:A/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-13958	
32	CVE-2024- 51552	Weak Password Storage	
	Source	Researcher	
	Status	no plans of corrective measures	
	Description	Weak password storage vulnerabilities exist in ASPECT if administrator credentials become compromised. This issue affects all versions of ASPECT.	
	CWE	CWE-257: Storing Passwords in a Recoverable Format	
	CVSS v3.1	Base Score:	6.0
		Temporal Score:	6.0
		Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:L
	CVSS v4.0	Score	7.1
		Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:H/VI:L/VA:L/SC:H/SI:L/SA:L
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-51552	

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	2025-22-05
B	10	CVE-2024-13945, added CVSS4.0 vector	2025-23-05
C	3, 11	Removed CVE-2024-51547 due to duplicate with an earlier advisory	2025-23-05