DOCUMENT ID: 9AKK108469A7497
REVISION: D
DATE: 2024-12-05

CYBER SECURITY ADVISORY

ASPECT system
ASPECT System, multiple vulnerabilities reported

Several CVE’s, see table inside document

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

Platform	Model number	ABB Product ID	Affected firmware Version	FW version improving the product
ASPECT®-Enterprise	ASP-ENT-x	2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021	3.08.02 and earlier	3.08.03 and newer
NEXUS Series	NEX-2x, NEXUS-3-x	2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021	3.08.02 and earlier	3.08.03 and newer
MATRIX Series	MAT-x	2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021	3.08.02 and earlier	3.08.03 and newer

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

Vulnerability IDs

CVE ID	Title	Version fixing the Issue
CVE-2024-6209	Unauthorized Access	3.08.02
CVE-2024-6298	Remote Code Execution	3.08.02
CVE-2024-6515	Clear Text Passwords	3.08.03
CVE-2024-6516	Cross Site Scripting XSS	3.08.03
CVE-2024-6784	SSRF Server Side Request Forgery	3.08.03
CVE-2024-48843	SQL Injection	3.08.03
CVE-2024-48844	Denial of Service, DoS	3.08.03
CVE-2024-48845	Weak Password Rules/Strength	3.08.03
CVE-2024-48846	Cross Side Request Forgery, CSRF	3.08.03

CVE ID	Title	Version fixing the Issue
CVE-2024-48847	MD5 bypass operation	3.08.03
CVE-2024-48839	Remote Code Execution, RCE	3.08.03
CVE-2024-48840	Unauthorized Access	3.08.03
CVE-2024-51541	Local File Inclusion	3.08.03
CVE-2024-51542	Configuration Download	3.08.03
CVE-2024-51543	Information Disclosure	3.08.03
CVE-2024-51544	Service Control	3.08.03
CVE-2024-51545	Username Enumeration	3.08.03
CVE-2024-51546	Credentials Disclosure	3.08.03
CVE-2024-51548	Dangerous File Upload	3.08.03
CVE-2024-51549	Absolute Path Traversal	3.08.03
CVE-2024-51550	Data Validation / Sanitization	3.08.03
CVE-2024-51551	Default Credentials	3.08.03
CVE-2024-51554	off-by-one-error	3.08.03
CVE-2024-51555	Force Change of Default Credentials	3.08.00
CVE-2024-11316	Filesize Check	3.08.03
CVE-2024-11317	PHP Session Fixation	3.08.03

Summary

ABB became aware of vulnerabilities in the product versions listed above.

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

An attacker can successfully exploit these vulnerabilities and could take remote control of the product and potentially insert and run arbitrary code.

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

Note: In order to exploit an 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.

Required 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 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.

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 to ABB specifications, ASPECT should never be exposed to the Internet!

CVE ID	Title	
CVE-2024-6209	Unauthorized Access	
Description	Unauthorized file access in WEB Server in ASPECT <=3.08.01 allows Attacker to access files unauthorized	
CVSS v3.1	Base Score:	10.0
	Temporal Score:	9.7
	Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:F/RL:U/RC:C
CVSS v4.0	Score	10
	Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/AU:Y/R:I/V:C/RE:H/U:Red
CVE-2024-6298	Remote Code Execution	
Description	Improper Input Validation vulnerability in ASPECT allows Remote Code Inclusion. <=3.08.01	
CVSS v3.1	Base Score:	10.0
	Temporal Score:	9.4
	Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:U/RC:C

[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.

CVE ID	Title	
CVSS v4.0	Score	10
	Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/AU:Y/R:I/V:C/RE:H/U:Red
CVE-2024-6515	Clear Text Passwords	
Description	Web browser interface may manipulate application username/password in clear text or Base64 encoding in ABB ASPECT providing a higher probability of unintended credentails exposure. <=3.08.02	
CVSS v3.1	Base Score:	9.6
	Temporal Score:	8.9
	Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N/E:F/RL:O/RC:C
CVSS v4.0	Score	8.7
	Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:N/S:N/AU:N/V:D/RE:L
CVE-2024-6516	Cross Site Scripting XSS	
Description	Cross Site Scripting vulnerabilities where found in ABB ASPECT providing a potential for malicious scripts to be injected into a client browser. <=3.08.02.	
CVSS v3.1	Base Score:	9.0
	Temporal Score:	8.6
	Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:L/E:H/RL:O/RC:C
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/S:N/AU:N/R:U/V:D/RE:L/U:Red
CVE-2024-6784	SSRF Server Side Request Forgery	
Description	Server-Side Request Forgery vulnerabilities were found in ASPECT providing a potential for access to unauthorized resources and unintended information disclosure. <=3.08.02.	
CVSS v3.1	Base Score:	9.9
	Temporal Score:	9.2
	Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O/RC:C
CVSS v4.0	Score	8.7
	Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L/S:N
CVE-2024-48843	SQL Injection	
Description	SQL injection vulnerabilities were found in ASPECT providing a potential for unintended information disclosure. This issue affects ASPECT <=3.08.02	
CVSS v3.1	Base Score:	8.2
	Temporal Score:	7.6
	Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N/E:F/RL:O/RC:C
CVSS v4.0	Score	7.6
	Vector:	CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:L/SI:L/SA:L/S:N/U:Red
CVE-2024-48844	Denial of Service, DoS	
Description	Denial of Service vulnerabilities where found in ASPECT providing a potiential for device service disruptions. This issue affects ASPECT <=3.08.02	

CVE ID	Title	
CVSS v3.1	Base Score:	7.7
	Temporal Score:	7.1
	Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:H/E:F/RL:O/RC:C
CVSS v4.0	Score	7.2
	Vector:	CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:L/VI:L/VA:H/SC:L/SI:L/SA:H
CVE-2024-48845	Weak Password Rules/Strength	
Description	Weak Password Reset Rules vulnerabilities where found in Aspect providing a potential for the storage of weak passwords that could facilitate unauthorized admin/application access. This issue affects ASPECT <=3.07.02	
CVSS v3.1	Base Score:	9.4
	Temporal Score:	9.0
	Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L/E:H/RL:O/RC:C
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:L/SC:L/SI:L/SA:L
CVE-2024-48846	Cross Side Request Forgery, CSRF	
Description	Cross Site Request Forgery vulnerabilities where found in ASPECT providing a potential for exposing sensitive information or changing system settings. This issue affects ASPECT <=3.08.02	
CVSS v3.1	Base Score:	7.1
	Temporal Score:	6.6
	Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N/E:F/RL:O/RC:C
CVSS v4.0	Score	7.1
	Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:H/VA:N/SC:L/SI:L/SA:L
CVE-2024-48847	MD5 bypass operation	
Description	MD5 Checksum Bypass vulnerabilities where found in ASPECT exploiting a weakness in the way an application dependency calculates or validates MD5 checksum hashes. This issue affects ASPECT <= 3.08.01.	
CVSS v3.1	Base Score:	8.2
	Temporal Score:	7.6
	Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N/E:F/RL:O/RC:C
CVSS v4.0	Score	8.8
	Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:N/SC:L/SI:L/SA:L
CVE-2024-48839	Remote Code Execution, RCE	
Description	Improper Input Validation vulnerability in ASPECT allows Remote Code Execution. This issue affects ASPECT <=3.08.02	
CVSS v3.1	Base Score:	10.0
	Temporal Score:	9.3
	Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L/E:F/RL:O/RC:C
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:L/SC:L/SI:L/SA:L
CVE-2024-48840	Unauthorized Access	

CVE ID	Title	
Description	Unauthorized Access vulnerabilities in ASPECT allow Remote Code Execution. This issue affects ASPECT <= 3.08.02	
CVSS v3.1	Base Score:	10.0
	Temporal Score:	9.3
	Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L/E:F/RL:O/RC:C
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:L/SC:L/SI:L/SA:L
CVE-2024-51541	Local File Inclusion	
Description	Local File Inclusion vulnerabilities in ASPECT allow access to sensitive system information. This issue affects ASPECT <= 3.08.02	
CVSS v3.1	Base Score:	8.2
	Temporal Score:	7.6
	Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N/E:F/RL:O/RC:C
CVSS v4.0	Score	8.8
	Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:L/SI:L/SA:L
CVE-2024-51542	Configuration Download	
Description	Configuration Download vulnerabilities in ASPECT allow access to dependency configuration information. This issue affects ASPECT <= 3.08.02.	
CVSS v3.1	Base Score:	8.2
	Temporal Score:	7.6
	Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N/E:F/RL:O/RC:C
CVSS v4.0	Score	8.8
	Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:L/SI:L/SA:L
CVE-2024-51543	Information Disclosure	
Description	Information Disclosure vulnerabilities in ASPECT allow access to application configuration information. This issue affects <= 3.08.02.	
CVSS v3.1	Base Score:	8.2
	Temporal Score:	7.6
	Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N/E:F/RL:O/RC:C
CVSS v4.0	Score	8.8
	Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:L/SI:L/SA:L
CVE-2024-51544	Service Control	
Description	Service Control vulnerabilities in ASPECT allow access to service restart requests and vm configuration settings. This issue affects <= 3.08.02.	
CVSS v3.1	Base Score:	8.2
	Temporal Score:	7.6
	Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:F/RL:O/RC:C
CVSS v4.0	Score	8.8
	Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:H/SC:L/SI:L/SA:L
CVE-2024-51545	Username Enumeration	
Description	Username Enumeration vulnerabilities ASPECT allow access to application level username add, delete, modify and list functions. This issue affects ASPECT <= 3.08.02.	
CVSS v3.1	Base Score:	10.0

CVE ID	Title	
	Temporal Score:	9.0
	Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
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:L/SI:L/SA:L
CVE-2024-51546	Credentails Disclosure	
Description	Credentials Disclosure vulnerabilities in ASPECT allow access to on board project backup bundles. This issue affects ASPECT <= 3.08.02	
CVSS v3.1	Base Score:	7.5
	Temporal Score:	7.0
	Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C
CVSS v4.0	Score	8.7
	Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:L/SI:L/SA:L
CVE-2024-51548	Dangerous File Upload	
Description	Dangerous File Upload vulnerabilities in ASPECT allow upload of malicious scripts. This issue affects ASPECT <= 3.08.02	
CVSS v3.1	Base Score:	9.9
	Temporal Score:	9.2
	Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O/RC:C
CVSS v4.0	Score	8.7
	Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L
CVE-2024-51549	Absolute Path Traversal	
Description	Absolute File Traversal vulnerabilities in ASPECT allows access and modification of unintended resources. This issue affects ASPECT<= 3.08.02	
CVSS v3.1	Base Score:	10.0
	Temporal Score:	9.3
	Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L/E:F/RL:O/RC:C
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:L/SC:L/SI:L/SA:L
CVE-2024-51550	Data Validation / Sanitization	
Description	Data Validation / Data Sanitization vulnerabilities in ASPECT Linux allows unvalidated and unsanitized data to be injected in an Aspect device. This issue affects ASPECT <= 3.08.02	
CVSS v3.1	Base Score:	10.0
	Temporal Score:	9.3
	Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L/E:F/RL:O/RC:C
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:L/SC:L/SI:L/SA:L
CVE-2024-51551	Default Credentials	
Description	Default Credentail vulnerabilities in ASPECT on Linux allows access to an Aspect device using publicly available default credentials. This issue affects ASPECT <= through 3.07.02	
CVSS v3.1	Base Score:	10.0
	Temporal Score:	10.0
	Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v4.0	Score	9.3

CVE ID	Title	
	Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L
CVE-2024-51554	off-by-one-error	
Description	Off By One Error vulnerabilities in ASPECT allow an array out of bounds condition in a log script. This issue affects ASPECT <= 3.08.02	
CVSS v3.1	Base Score:	9.1
	Temporal Score:	8.4
	Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:L/E:F/RL:O/RC:C
CVSS v4.0	Score	8.8
	Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:L/SC:L/SI:L/SA:L
CVE-2024-51555	Force Change of Default Credentials	
Description	Default Credentail vulnerabilities in ASPECT allows access to an Aspect device using publicly available default credentials since the system does not require the installer to change default credentials. This issue affects ASPECT<= 3.07.02	
CVSS v3.1	Base Score:	10.0
	Temporal Score:	9.0
	Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
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:L/SI:L/SA:L
CVE-2024-11316	Filesize Check	
Description	Fileszie Check vulnerabilities in ASPECT allow a malicious user to bypass size limits or overload an Aspect device. This issue affects ASPECT<= 3.08.02	
CVSS v3.1	Base Score:	7.5
	Temporal Score:	7.0
	Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:O/RC:C
CVSS v4.0	Score	8.7
	Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:L/SI:L/SA:L
CVE-2024-11317	PHP Session Fixation	
Description	Session Fixation vulnerabilities in ASPECT allow an attacker to fix a users session identifier before login providing an opportunity for session takeover on an Aspect device. This issue affects ASPECT <= 3.08.02	
CVSS v3.1	Base Score:	10.0
	Temporal Score:	9.3
	Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N/E:F/RL:O/RC:C
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:L/SC:L/SI:L/SA:L

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 in order to protect customers 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 particular network segment where ASPECT is installed and configured.
- Note: it is crucial that the VPN Gateway and Network is setup in accordance with best industry standards and maintained in terms of security patches for all related components.
- ABB System Integrators shall change default passwords if they are still in use.
- 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

Workarounds

Users accessing ASPECT remotely shall do this using a VPN Gateway allowing access to the particular network segment where ASPECT is installed and configured.

Note: it is crucial that the VPN Gateway and Network is setup in accordance with best industry standards and maintained in terms of security patches for all related components.

Frequently asked questions

What causes the vulnerabilities?

The vulnerabilities are caused by configuration issues allowing the attacker to do various unintended, unauthorized actions on the target device. Please look at the description of the respective CVE’s for further details.

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?

If this vulnerability 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 could try to exploit the vulnerability by creating a specially crafted message and sending the message to ASPECT. This 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 security system.

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 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 exploit of this vulnerability?

ASPECT is not designed as a functional safety device.

Is a software update available fixing the problem?

Yes. ASPECT Version 3.08.03 or newer is fixing ~~many of~~ the issues listed in this advisory.

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

Yes.

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.

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

HT0038	FBXi, CBXi and ASPECT® SOLUTIONS

Acknowledgement

ABB likes to thank Gjoko Krstikj, Zero Science Lab, for reporting the 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	2024-07-03
B		Update of advisory due to availability of ASPECT version 3.08.02	2024-08-20
C		Update of advisory due to availability of ASPECT version 3.08.03	2024-11-28
D	Acknowledgement	Corrected the sir name of the reporting researcher	2024-12-05