DOCUMENT ID: 9AKK108469A7497
REVISION: A
DATE: 2024-07-04

CYBER SECURITY ADVISORY

ASPECT system
ASPECT system RCE, unauthorized-Access vulnerabilities reported

CVE ID: CVE-2024-6209: unauthorized file access
CVE-2024-6298: remote code execution

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
ASPECT®-Enterprise	ASP-ENT-x	2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021	3.08.01 and earlier
NEXUS Series	NEX-2x, NEXUS-3-x	2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021	3.08.01 and earlier
MATRIX Series	MAT-x	2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021	3.08.01 and earlier

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

Vulnerability IDs

CVE ID	Title
CVE-2024-6209	unauthorized file access
CVE-2024-6298	remote code execution

Summary

ABB became aware of a vulnerability in the product versions listed above.

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

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

ABB strongly advises, 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: "HT0038_Aspect_System_Network_Security_Best_Practice.pdf", which can be downloaded from the product Online page.

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 allowing a successful attacker to execute arbitrary code on ASPECT products. In cases where ASPECT is exposed to the Internet or other insecure networks, the attacker may install arbitrary code on the device.

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. Even customer who have connected ASPECT in earlier times or only in defined time intervals are requested to take the device out of operation and replace it with a new, ABB delivered version, without delay.

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. This means in particular: its IP addresses and ports are not exposed to the Internet or other insecure networks. Presuming this as a precondition, the successful attacker can access and replace files or file content, stored on the file system of ASPECT if (s)he has access to the network segment where ASPECT is installed/configured (AV:A).

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

CVE-2024-6209 unauthorized file access

CVSS v3.1 Base Score:	9.6
CVSS v3.1 Temporal Score:	9.4
CVSS v3.1 Vector:	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:F/RL:U/RC:C
CVSS v4.0 Score	9.4
CVSS v4.0 Vector:	CVSS:4.0/AV:A/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

CVSS v3.1 Base Score:	9.6
CVSS v3.1 Temporal Score:	9.1
CVSS v3.1 Vector:	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:U/RC:C
CVSS v4.0 Score	9.4
CVSS v4.0 Vector:	CVSS:4.0/AV:A/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

[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.

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.

Workarounds

In case ASPECT is connected to a network considered insecure (e.g. Internet), disconnect it immediately.

Frequently asked questions

What causes the vulnerability?

The vulnerability is caused by a configuration issue allowing unauthorized access to a system folder on the ASPECT device and by insufficient input validation.

What is ASPECT?

ASPECT is a device 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?

ABB has become aware that a proof of concept to exploit this vulnerability exists. An attacker who has access to such proof of concept or being able to develop an exploit code on its own may be able to take over control of the product and even install/run arbitrary code.

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.

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?

No. ABB is currently working on a software update fixing the reported issues. In the meantime, ABB strongly recommends following the mitigating actions as described in this advisory.

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

ABB has become aware that a proof of concept to exploit this vulnerability exists.

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:

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 Rev 2	HT0038_Aspect_System_Network_Security_Best_Practice.pdf

References

HT0038 Rev 2	HT0038_Aspect_System_Network_Security_Best_Practice.pdf

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