DOCUMENT ID: 2CKA000073B5403
REVISION: A
DATE: 2023-06-01

CYBER SECURITY ADVISORY

ASPECT® Control Engines (ACE)

CVE ID: CVE-2023-0635, CVE-2023-0636

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

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

Vulnerability IDs

CVE-2023-0635, CVE-2023-0636

Summary

ABB is aware of reports of vulnerabilities in the product versions listed above.

An attacker who successfully exploited these vulnerabilities could take remote control of the product and insert and run arbitrary code.

Note: In order to exploit an ASPECT Control Engine, an attacker would need a misconfigured system, exposed to the internet without firewalling and with default port configurations.

Recommended immediate actions

CVE-2023-0635 and CVE-2023-0636 are corrected in the following product versions:

Platform	Model number	ABB Product ID	Firmware Version
ASPECT®-Enterprise	ASP-ENT-x	2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021	3.07.01 and newer
NEXUS Series	NEX-2x, NEXUS-3-x	2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021	3.07.01 and newer
MATRIX Series	MAT-x	2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021	3.07.01 and newer

Weakness-1 shall be mitigated by manually changing default credentials with strong passwords.

Vulnerability severity and details

Weakness-1 Default credentials are not forced to be changed during initial configuration on 3.07.01 or earlier, so that a successful attacker could access the device interface and access the underlying database from the device login in case the credentials have not been manually changed.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1[1].

CVE-2023-0635 Privilege escalation to root

The successful attacker can open a shell and escalate access privileges to root.

CVSS v3.1 Base Score: 7.8
CVSS v3.1 Temporal Score: 7.4
https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:W/RC:C
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:W/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2023-0635

[1] 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.

CVE-2023-0636 Remote code execution

The successful attacker is able to leverage a vulnerable network diagnostic component of the ASPECT interface, to perform Remote Code Execution.

CVSS v3.1 Base Score: 7.2
CVSS v3.1 Temporal Score: 7.0
https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:F/RC:C
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:F/RC:C
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2023-0636

Mitigating factors

Always use the latest Software version available for the devices listed in section Affected products.

ASPECT devices are not intended to be internet-facing, vulnerabilities listed here will be mitigated by placing the device behind a properly configured Firewall and restricting network access to the devices to authorized personnel only.

In general customers are encouraged to harden the device by only opening ports for services they need to successfully operate the product.

ASPECT v3.07.01 and later provides an option to close any port on the target, mitigating access to the device UI (by closing 8245, 3306 and 30144) and the underlying database (port 30144 is no longer open for any installation).

ASPECT v 3.07.01 closes the vulnerability that allowed access to the Operating System, and escalation to Root as well as the option for remote code execution.

Workarounds

ABB recommends updating the product to its latest supported Firmware Version. In case this is not acceptable the following workarounds shall be considered.

Although these workarounds will not correct the underlying vulnerability, they can help blocking known attack vectors. When a workaround reduces functionality, this is identified below as “Impact of workaround”.

The most secure approach is to expose nothing to the Internet, and to use VPN to access a corporate network. This is the preferred method of providing remote access and it delivers the most comfortable balance of convenience and security.

However, on any large network it is also recommended to secure the ASPECT device as follows:

1. Upgrade to the latest version of ASPECT.
2. Purchase an SSL certificate from a trusted CA (Certificate Authority) and install it on your ASPECT devices.
3. Configure a firewall to block ALL port access to your ASPECT devices except port 443, the default SSL port.
4. Configure the device to close ports 8245, 3306 and 30144.

5. Configure your ASPECT device to force the default access page to be the “Aspect First Instance” i.e. the main page for the first configured ASPECT project on the device. This bypasses the ASPECT System Administration pages, allowing access to your project page using the following URL format: https://<hostname>/ng/. To configure the device in this way, open the System Administration > Web Server SSL Configuration page, and select *Use First Aspect Instance*.
6. Change the credentials on any device that is using default passwords as shipped from the factory to ensure strong passwords are used. Configure the device to have automated access to “yum” security upgrade patches.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited these vulnerabilities could take control of an affected device and insert and run arbitrary code in an affected system node.

What causes the vulnerability?

Weakness-1 Information about the product version and the underlying Operating System can be returned from the device Interface.

Weakness-2 Default credentials are not forced to be changed during initial configuration on v3.07.01 or earlier, so that a successful attacker can access the device interface and access the underlying database from the device login, in case the credentials have not been manually changed.

CVE-2023-0635 Privilege escalation to root. The successful attacker can open a shell and escalate access privileges to root.

CVE-2023-0636 Remote code execution. The successful attacker is able to leverage a vulnerable network diagnostic component of the ASPECT interface, to perform Remote Code Execution.

What is the ASPECT Control Engine?

The ASPECT Control Engine is part of the supervision network for the Building Management System.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited these vulnerabilities would be able to gain access to the underlying operating system, and from here elevate their user permissions to root. As a root user they would be able to install and run arbitrary code, including the modification of the existing firmware in place.

How could an attacker exploit the vulnerability?

An attacker with network access to the device could try to exploit these vulnerabilities by using default credentials. This would require that the attacker has access to the system network, by connecting to the local network, or that (s)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 above.

Could the vulnerability be exploited remotely?

We have no indication that devices which are installed and configured according to all of ABB recommended practices, can be exploited remotely by the above-mentioned 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 the vulnerability by modifying the way that the ASPECT Control verifies input data and by allowing individual ports to be closed.

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 evidence 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). Disable unnecessary services or features that could expose the system to potential attacks.

Install physical controls so unauthorized personnel are hindered to access your devices, components, peripheral equipment, and networks, with strong access controls, secure configuration, and necessary safeguards.

Never connect programming software or computers containing programing software to any network other than the network for the devices that it is intended for.

Ensure frequent security reviews are conducted within your environment, before installation of any update with additional scanning using automated tools to identify and remediate vulnerabilities.

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. Products in scope of this advisory are not intended to be connected to 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. Also, understand that VPNs are only as secure as the connected devices.

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

HT0038 ASPECT, FBXi, CBXi System Network Security Best Practice

Acknowledgement

ABB would like to thank Prism Infosec for identifying this vulnerability in its products and for dealing with it in a professional manner.

References

HT0038 ASPECT, FBXi, CBXi System Network Security Best Practice, available from ABB Library

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	31/05/2023