DOCUMENT ID: 9AKK108469A6101
REVISION: B
DATE: 2024-06-26

CYBER SECURITY ADVISORY

ASPECT system
ASPECT system operating with default credentials while exposed to the Internet.

CVE ID: CVE-2024-4007 hard coded default credential contained in install package

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	Firmware version resolving the vulnerability
ASPECT®-Enterprise	ASP-ENT-x	2CQG103201S3021, 2CQG103202S3021, 2CQG103203S3021, 2CQG103204S3021	3	3.07.02 and newer
NEXUS Series	NEX-2x, NEXUS-3-x	2CQG100102R2021, 2CQG100104R2021, 2CQG100105R2021, 2CQG100106R2021, 2CQG100110R2021, 2CQG100112R2021, 2CQG100103R2021, 2CQG100107R2021, 2CQG100108R2021, 2CQG100109R2021, 2CQG100111R2021, 2CQG100113R2021	3	3.07.02 and newer
MATRIX Series	MAT-x	2CQG100102R1021, 2CQG100103R1021, 2CQG100104R1021, 2CQG100105R1021, 2CQG100106R1021	3	3.07.02 and newer

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

Vulnerability IDs

CVE-2024-4007 hard coded default credential contained in install package

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.

Note: In order to exploit an ASPECT Control Engine, an attacker would need a misconfigured system:

- Default password credentials, unchanged during first and subsequent commissioning,
- exposed to the Internet,
- without firewalling.

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.

Recommended immediate actions.

ABB Strongly recommends the following actions on any released SW version of ASPECT:

- Change the PHPmyAdmin Password according to the system manual:
    - All customers who operate the ASPECT System with its default password are recommended to replace this default password with a unique, secure password, containing a mix of characters, numbers, and special characters with at least 10 characters in length.
- Never expose open ports to the ASPECT product towards the Internet or any insecure network.
- 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.
- ABB recommends that customers shall apply the latest product update at the earliest convenience.

Vulnerability severity and details

ABB is aware that customers operate ASPECT systems without changing the default PHPmyAdmin password credential. As the default password is contained in the install package of earlier versions < 3.07, it is assumed that it is well known to the public.

If an ASPECT system is exposed to the Internet, operating with these default credentials, an attacker can get full access to the PHPmyAdmin tool inside ASPECT.

CVE-2024-4007 hard coded default credential contained in install package

CVSS v3.1

CVSS v3.1 Base Score: 8.8 (High)
CVSS v3.1 Temporal Score: 8.2 (High)

CVSS v3.1 Vector:
CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C/CR:H/IR:H/AR:H/MAV:A/MAC:L/MPR:N/MUI:N/MS:C/MC:H/MI:H/MA:H
First.org Summary Link: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C/CR:H/IR:H/AR:H/MAV:A/MAC:L/MPR:N/MUI:N/MS:C/MC:H/MI:H/MA:H

CVSS v4.0

CVSS v4.0 Score: 8.7 / High
CVSS v4.0 Vector:
CVSS:4.0/AV:A/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
First.org Summary Link: https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:A/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

Mitigating factors

ASPECT system shall not be connected directly to untrusted networks such as the Internet.

If remote access to an ASPECT system is a customer requirement, the system shall operate behind a firewall. User accessing ASPECT remotely shall do this using a VPN Gateway allowing access to the particular network segment where ASPECT is installed and configured in.

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.

Any default credentials shall be exchanged with a unique credential supporting adequate strength.

Frequently asked questions

What is the scope of the vulnerability?

An ASPECT system, that is exposed to the Internet while operating with default password credentials for the PHPmyAdmin tool, could become subject to attackers who then have read/write access to the ASPECT internal SQL database.

What causes the vulnerability?

The root cause of the vulnerability is that the commissioning process of ASPECT does not enforce to change password credentials during first commission. A future version of ASPECT is planned to implement such enforcement. Subsequently, if an ASPECT system is exposed to the internet and commissioned using default credentials, an attacker can take over control of the product. The attacker can tamper with the data collected by the product until then.

What might an attacker use the vulnerability to do?

If an ASPECT instance is exposed to the Internet and commissioned with default credentials for the PHPmyAdmin tool, an attacker can login to the system as if (s)he was an authorized user who is allowed to change the configuration or make changes to the content of data collected by the product.

It is therefore highly recommended to operate ASPECT protected by a firewall and only allow access to the system within a trusted network environment. Any remote access to the network segment where ASPECT is installed, must be protected by means of best industry network protection such as VPN connection setup.

Could the vulnerability be exploited remotely?

See: What might an attacker use the vulnerability to do?

Can functional safety be affected by an exploit of this vulnerability?

No, ASPECT is not designed to support functional safety. Recorded data shall not be used as input to subsequent systems, providing functional safety, where that safety of the subsystem depends on the integrity and confidentiality of that input data.

What does the update do?

The update removes the default PHPmyAdmin Password from the install package of ASPECT. This however, does not fix the broken confidentiality of the password as it is known to public since the first version was published. Therefore the password must be changed to become unique and supporting adequate strength.

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 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. 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 Rev 2	HT0038_Aspect_System_Network_Security_Best_Practice.pdf

Acknowledgement

ABB likes to thank https://divd.nl for reporting the vulnerability in responsible disclosure.

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	
B	all	Copyright year was 20244 is corrected to 2024	2024-06-26