DOCUMENT ID: 2NGA001801
REVISION: A
DATE: 2023-07-24

CYBER SECURITY ADVISORY

ABB Ability™ zenon
zenon directory permissions and internal function issues

CVE ID: CVE-2023-3321, CVE-2023-3322, CVE-2023-3323, CVE-2023-3324

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

Product / System line	Products and Affected Versions	Advisory
zenon	All versions up to version 11 build 106404	

Vulnerability IDs

CVE-2023-3321

CVE-2023-3322

CVE-2023-3323

CVE-2023-3324

Summary

These vulnerabilities affect the ABB Ability™ zenon. Subsequently, a successful exploit could allow attackers to execute programs on the zenon system. While the attackers need internal information from the zenon system and need to access the system via various means some of the zenon directories are accessible for low privileged users. These directories may be used further to carry out the attacks.

Recommended immediate actions

ABB recommends following the instructions in the mitigating factors. ABB recommends that customers apply the update at earliest convenience.

Vulnerability severity and details

A vulnerability exists by allowing low privileged users to read and update the data present in various directories used by the zenon system. An attacker could exploit the vulnerability by using specially crafted programs to exploit the vulnerabilities by allowing them to run on the zenon installed hosts.

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

CVE-2023-3321 Code Execution through Writable Mosquitto Configuration File

A low privileged user may update the contents of the file 'CDDataHub.conf' present in ABB service grid data hub directory 'C:\ProgramData\ABB\System\ServiceGrid\DataHub' allowing the users to access Mosquitto configuration files on the zenon system.

CVSS v3.1 Base Score:	7.0
CVSS v3.1 Temporal Score:	6.4
CVSS v3.1 Vector:	AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:W/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:W/RC:C&version=3.1

CVE-2023-3322 Code Execution through overwriting service executable in utilities directory

The vulnerability is caused by the weakly configured default directory permission for the ABB Utilities directory.

CVSS v3.1 Base Score:	7.0
CVSS v3.1 Temporal Score:	6.4
CVSS v3.1 Vector:	AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:W/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:W/RC:C&version=3.1

CVE-2023-3323 Code Execution through overwriting project file on zenon engineering studio system

The vulnerability is caused by the default directory permissions for the Zenon Projects directory in the engineering studio default workspace. By allowing access to all the users on the system, the attacker may alter the zenon project itself to load arbitrary zenon projects in the zenon runtime.

CVSS v3.1 Base Score:	5.9

[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.

CVSS v3.1 Temporal Score:	5.3
CVSS v3.1 Vector:	AV:P/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:P/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C&version=3.1

CVE-2023-3324 Insecure deserialization in zenon internal DLLs

The vulnerability is caused by the using deprecated deserialization functions and/or classes such as BinaryFormatter in the zenon internal graphic utility DLLs.

CVSS v3.1 Base Score:	6.3
CVSS v3.1 Temporal Score:	5.6
CVSS v3.1 Vector:	AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:H/A:H/E:U/RL:U/RC:R
NVD Summary Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:H/A:H/E:U/RL:U/RC:R&version=3.1

Mitigating factors

The zenon system installs and updates components in various directories on the zenon host machine. The vulnerabilities CVE-2023-3321, CVE-2023-3322, CVE-2023-3323 can be mitigated by restricting access to the low privileged users. The steps on how to reduce the access permission for certain directories in mentioned further.

The vulnerability CVE-2023-3324 can be mitigated by removing the specific graphics related file by following the steps mentioned further.

Refer to Zenon security guide for more detailed information and for further advise how to keep the system secure.

Workarounds

ABB recommends the following workarounds. Although these workarounds will not correct the underlying vulnerability, they block the known attack vectors.

- For CVE-2023-3321, CVE-2023-3322, CVE-2023-3323:
    - 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.
    - Remove the default directory permissions for ‘Everyone’ on the service grid, ABB utilities, and zenon_Projects directories and provide access only to specific users that are expected to access zenon.
    - Install the IIoT services, which is, the Service grid component on a separate system.
    - Secure the ZEE600 related executable files in ‘C:\ProgramData\ABB\ABBUtilities’ directory by removing the group named “Everyone”.
    - Ensure the group name “Everyone” should be removed from the following directory. ‘C:\ProgramData\ABB’.
    - Secure zenon_Projects directory by managing the access permissions. The project directory should have access only for the user group (Excluding administrator) which has the users to use zenon projects. Consider the following example:

  - Example: A user group named ‘zenonOwnersGroup’ to be created and it is the only group that has write access to the zenon_ Projects directory. If the system has 2 users such as test1(Part of zenonOwnersGroup) and test2 (not in zenonOwnersGroup). The project directory (C:\Users\Public\Documents\zenon_Projects) should have write access only for the zenonOwnersGroup and for no one else. Now, test1 should have write access the zenon_Project directory and test2 should not.

- For CVE-2023-3324:
  - The BinaryFormatter class used in implementation of zenon runtime is considered unsafe, as it allows users to create arbitrary classes not limited to the classes the developer intended to deserialize. By deserializing user-controlled content, it may be possible for attackers may potentially load and run random code.
  - The mitigation steps are as follows:
    - In the Engineering Studio application remove the .cdwpf files from the graphics folder of each project that contains .cdwpf files created by the 3D Configurator tool.
    - On the system with the Engineering Studio, for each affected project, remove the RT folder containing the Service Engine files
    - Compile new files in the Engineering Studio for each affected project
    - On the system with the Service Engine, remove the RT folder of each affected project
    - Transport to or place onto the system with the Service Engine the newly created Service Engine files that no longer contain the .cdwpf files

- Note: the vulnerability only exists if the 3D configurator tool is used to generate .cdwpf files that are used in screens in projects for display of 3D models

Frequently asked questions

What is the scope of the vulnerabilities?

An attacker who successfully exploited CVE-2023-3321, CVE-2023-3322, CVE-2023-3323 vulnerabilities could alter the Zenon runtime activities by modifying the contents of certain directories with weak access permissions. The attacker may also craft special executables and run them on the Zenon system. However, a zenon system can mitigate the risk by following better control of the access permissions and restrict the access only to legitimate users by configuring windows directory permissions as per the ‘Access Controls’ section in zenon security guideline.

For CVE-2023-3324 the attacker may potentially provide malicious data to a deserialization function by modifying the configuration data. This occurs only for a specific graphic control and this file can be removed from the zenon system to reduce risk of the vulnerability.

What causes the vulnerability?

The CVE-2023-3321 is caused by the weakly configured default directory permission for the ABB service grid data hub directory. This internally has Mosquitto broker configuration file that has ‘write’ permissions for non-admin users as well. This file can be manipulated to load arbitrary executables.

What are the affected components – Service Grid - Mosquitto Configuration file, ABB Utilities zenHelpCheck, zenon engineering studio workspace directory?

- zenon Service Grid uses event-oriented communication via the central Service Hub for data transfer between the services.

  CVE-2023-3321 : zenon Service Grid connects the Engineering Studio, Service Engine and Report Engine. These components can thus exchange data via the Service Grid and make it accessible to other Service Grid components.

  Note: For a normal Service Engine installation, the IIoT Services (Service Grid) would not be installed / used locally

  The Service Grid is an optional component for the Service Engine functionality. It is needed for some use cases for example: when using the Report Engine. It is recommended to install and use the Service Grid component on a different system other than the Service Engine.

- zenHelpCheck : Its main purpose is to check whether System Tray Helper is running when the user disables it from task manager and restart the PC. If the System Tray Helper is not running and the user tries to run zenon (Editor/Runtime), the service kills Zenon process and alert the user

  CVE-2023-3322 : zenonHelpCheck Windows Service is installed along with System Tray Helper. Its main purpose is to check whether the System Tray Helper is running after the user disabled it from task manager and restarted the PC.

- zenon_Projects is the workspace directory where the zenon projects are stored.

  CVE-2023-3323 : The configured default directory permission for the ‘zenon_Projects’ directory. This directory can be accessed by non-admin users on the host machine with ‘write’ permissions. It is also recommended to have engineering studio and service engine run different machines for better separation of functionalities.

What is the affected component – zenon graphics utility, `3dRuntimeControl.dll` ?

The affected component is used in zenon graphic utility 3D Configurator tool. The “3dRuntimeControl.dll” is loaded by the Service Engine on opening a screen that contains a specific WPF element. At this point the z3d file, an XML file, is loaded and deserialized with the BinaryFormatter Class. For the issue to be exploited, the project needs to contain that specific wpf file and the screen needs to contain a wpf element that is configured.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited the CVE-2023-3321, CVE-2023-3322 vulnerabilities could alter the zenon runtime activities by crafting special executable and run them.

An attacker who successfully exploited the CVE-2023-3323 vulnerability by having access to the zenon_Projects directory and load altered zenon engineering projects and execute the same.

An attacker who successfully exploited the CVE-2023-3324 vulnerability by deserializing user-controlled content, it may be possible for attackers to achieve code execution.

How could an attacker exploit the vulnerability?

For CVE-2023-3321, CVE-2023-3322: An attacker could try to exploit the vulnerability by creating a specially crafted executables and altering execution paths of a zenon service. This would require that the attacker has access to the system physically or via remote network, by connecting to the network either directly or through a wrongly configured or penetrated firewall. Not every installation of zenon by default installs the service grid component. The CVE-2023-3321 vulnerability to be exploitable service component and corresponding exploitable configuration files.

Note: The Service Grid is an optional component for the service engine functionality. It is needed for some use cases for example: when using the Report Engine. It is recommended to install and use the service grid component on a different system other than the service engine.

For CVE-2023-3323: An attacker could try to alter the zenon project and ensure that it gets loaded to and run on the zenon service engine. This would require that the attacker has access to the zenon system physically or via remote, by connecting to the network either directly or through a wrongly configured or penetrated firewall.

For CVE-2023-3324: An attacker could try to alter the deserialization content that is used by a weak deserialization function in a graphic utility. This would require that the attacker has access to the zenon system physically or via remote, by connecting to the network either directly or through a wrongly configured or penetrated firewall. This would also mean that the attacker has zenon internal knowledge prior to exploiting the vulnerability, as to how and where to load the corrupted deserialized data and against what controls such a vulnerability exists. The project must contain screens that contain a wpf control that is configured to use a cdwpf control for the 3D control, (created by the 3D configurator tool that requires a license) and this screen must be opened either automatically or by an operator to trigger the vulnerability.

Could the vulnerability be exploited remotely?

The attacker needs access to the zenon system via physical access or via remote access. Then an attacker who has network access and with ‘write’ permissions on the various affected zenon directories could exploit these vulnerabilities.

Recommended practices to protect against unauthorized remote login, if needed, include that process control systems are physically protected, have no direct connections to the Internet, or are separated from other networks by means of a firewall system that has a minimal number of ports exposed and other rules configured to accept connections only from trusted sources. When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). VPN itself may have vulnerabilities and should be updated to the most current version available.

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 we strongly recommend the following (non-exhaustive) list of cyber security practices:

- Reduce default permission and configure specific user groups to have write access to zenon directories.

- 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.
- Only install software components that are necessary for the role of the system. (e.g., do not install the engineering studio on systems where only the service engine is needed, and do not install the IIoT Services if they are not used)
- Never connect programming software or computers containing programing software to any network other than the network for the devices for which it is intended.
- Scan all data imported into your environment before use to detect potential malware infections.
- 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.
- 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 zenon Security Guide

Acknowledgement

ABB thanks Noam Moshe of Claroty Research - Team82, for helping to identify the vulnerabilities and protecting our customers.

References

Zenon Security Guide

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	24-July-2023