DOCUMENT ID: 2NGA001479
REVISION: A
DATE: 2022-07-26

CYBER SECURITY ADVISORY

ABB Ability TM Operations Data Management Zenon Zenon Log Server file access control

CVE ID: CVE-2022-34836, CVE-2022-34837, CVE-2022-34838

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.

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 8.20	

Vulnerability IDs

ABBVREP0079

CVE-2022-34836

CVE-2022-34837

CVE-2022-34838

Summary

These vulnerabilities affect the ABB Ability™ Operations Data Management Zenon. Subsequently, a successful exploit could allow attackers to log additional messages and access files from the Zenon system. While the passwords in the INI files are not stored in clear text, they can be subjected to further attacks against the hash algorithm.

Recommended immediate actions

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

Vulnerability severity and details

A vulnerability exists in the Log server included in the product versions listed above. An attacker could exploit the vulnerability by using specially crafted programs to exploit the vulnerabilities.

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

CVE-2022-34836 Zenon log server file upload vulnerability

A vulnerability exists in the Zenon log server that allow the user to access files on the Zenon system. The user also can add own log messages and e.g., flood the log entries.

CVSS v3.1 Base Score:	5.9
CVSS v3.1 Temporal Score:	5.4
CVSS v3.1 Vector:	AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N/E:P/RL:W/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N/E:P/RL:W/RC:C&version=3.1

CVE-2022-34837 Network Password is encrypted using a predictable key

The network password in the initialization file is protected with a predictable key. To exploit this vulnerability a special program is required.to extract the password.

CVSS v3.1 Base Score:	6.2
CVSS v3.1 Temporal Score:	5.7
CVSS v3.1 Vector:	AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:W/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L/E:P/RL:W/RC:C&version=3.1

CVE-2022-34838 Database Password is encrypted using a static encryption key

The SQL database password of the Zenon Configuration tool can be extracted to plain text with a special program when the algorithm is known.

CVSS v3.1 Base Score:	8.1
CVSS v3.1 Temporal Score:	7.4
CVSS v3.1 Vector:	AV:L/AC:H/PR:N/UI:N/S:C/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:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:W/RC:C&version=3.1

[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.

Mitigating factors

The Zenon system firewall rules to be used to allow access only to the required clients.

Users to choose complex passwords for the network password and the engineering database password.

It is recommended that the operational environment shall be separated from the Zenon project editor. This enables better control of the changes applied and reduces the risk of engineering database installation access.

Refer to Zenon's security guide for further advice on how to keep the system secure.

Consider starting Zenon operator workplaces in kiosk mode to avoid user access to WIN desktop.

Workarounds

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

- For single computer installations block network access to the Zenon log server:
    - To do this block all incoming connections to the host machine via the inbound firewall rules.
    - Update the logging service configuration from the start-up tool to the local host or loopback address
- For two computer installations:
    - To do this block all incoming connections to the host machine via the inbound firewall rules.
    - Update the logging service configuration from the start-up tool to the IP address and port where the service can be accessed. After doing this allow only the clients that may connect to the log service via the host machine inbound firewall rules. This will reject all arbitrary connections to the log service and allow only configured clients to access the Zenon log service.
- To protect the Zenon INI file the access to the directory by using the Security properties of the respective directories and choosing the access permissions such as allowing only authenticated users, etc., and providing various permissions such as Read, Write, etc. on the directory.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited the CVE-2022-34836 vulnerability could access the Zenon runtime activities such as the start and stop of various activity and the last error code etc. The attacker may also craft special private protocol information and perform random file readings on the Zenon system. However, a Zenon system can mitigate the risk by following better control of the access permission and restricting the access only to legitimate clients by using the inbound firewall rules on the Zenon log service

An attacker who successfully exploited CVE-2022-34837 may add more network clients that may monitor various activities of the Zenon. However, by reducing the access controls to the network password ini file the risk of attack scenario can be mitigated.

An attacker who successfully exploited CVE-2022-34838 may add or alter data points and corresponding attributes. Once such engineering data is used the data visualization will be altered for the end user. However, by separating the installation of the runtime environment from the engineering environment the risk of the engineering installation passphrase exposure can be mitigated.

What causes the vulnerability?

The CVE log server vulnerability is caused by allowing a client to connect to the Zenon log service. The log service access is not limited to log files only

Even though the passwords are not in plaintext, the CVE-2022-34837 and the CVE-2022-34838 are caused by not restricting the access to a minimal level and thus allowing random users logged in to the machine to read the passwords. With additional knowledge, the password from the INI files can be extracted.

What is the affected component – the Zenon log service?

The Zenon log service is used to understand the activity of the Zenon software and understand the last error state etc.

What is the Zenon System Network communication password?

The network communication password is sued for encrypting the network data for the Zenon server-client communication. The engineering tool database password protects the engineering configuration data point information and their attributes, tags, etc.

What is the Zenon engineering database password?

The engineering tool database password protects the engineering configuration data point information and their attributes, tags, etc.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited the CVE-2022-34836 vulnerability could access the Zenon runtime activities such as the start and stop of various activities and the last error code etc. The attacker may also craft special private protocol information and perform random file readings on the Zenon system.

However, a Zenon system can mitigate the risk by following better control of the access permission and restricting the access only to legitimate clients by using the inbound firewall rules on the Zenon log service. However, a Zenon system can mitigate the risk by following better control of the access permission and restricting the access only to legitimate clients by using the inbound firewall rules on the Zenon log service.

An attacker who successfully exploited the CVE-2022-34837 may add more network clients that may monitor various activities of the Zenon This does not affect user authentication.

However, by reducing the access controls to the network password INI file the risk of attack scenario can be mitigated.

An attacker who successfully exploited the exploited CVE-2022-34838 adds or alters data points and corresponding attributes. Once such engineering data is used the data visualization will be altered for the end user.

However, by separating the installation of the runtime environment from the engineering environment the risk of the engineering installation passphrase exposure can be mitigated.

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 a Zenon log service. 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 firewall.

For the network password and the engineering database password issues, the attacker needs the INI files. This also means that the attacker has prior information on the internals of the password generation to proceed with exploiting further.

The Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

CVE-2022-34836: 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.

CVE-2022-34837: Yes, to exploit this vulnerability an attacker would need to have access to an affected system node. Recommended practices include that directory access permissions are set with minimal levels to prevent random users read the INI file information.

CVE-2022-34838: No, to exploit this vulnerability an attacker would need to have physical access to an affected system node. Recommended practices include that directory access permissions are set with minimal levels to prevent random users read the INI file information. And isolate the engineering and runtime installations to reduce the risk of INI file access.

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:

- 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 programming 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 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 following documents:

Zenon Security Guide

Acknowledgment

ABB thanks Ruben Santamarta 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	26-July-2022