DOCUMENT ID: 9AKK108472A9037
REVISION: A
DATE: 2026-07-30

CYBER SECURITY ADVISORY

ABB Ability™ zenon Security Risk Due to End-of-Life MongoDB Component

CVE IDs: CVE-2025-14847, CVE-2020-7928, CVE-2020-7921, CVE-2020-7925, CVE-2020-7929, CVE-2020-7923, CVE-2021-20330, CVE-2021-32036, CVE-2021-32040, CVE-2021-20333, CVE-2020-7924, CVE-2021-20328, CVE-2021-20334

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

The vulnerability affects zenon platform installations that include IIoT Services utilizing the MongoDB-based Persistence Service. Specifically, all product versions that bundle MongoDB version 4.2 as part of the IIoT Services are affected. Systems where IIoT Services are not installed or not in use are not impacted by this vulnerability.

Vulnerability IDs

CVE-2025-14847, CVE-2020-7928, CVE-2020-7921, CVE-2020-7925, CVE-2020-7929, CVE-2020-7923, CVE-2021-20330, CVE-2021-32036, CVE-2021-32040, CVE-2021-20333, CVE-2020-7924, CVE-2021-20328, CVE-2021-20334

Summary

ABB is aware of publicly reported vulnerabilities affecting MongoDB 4.2, which is bundled within the IIoT Services of the affected product versions. MongoDB 4.2 has reached end-of-life and contains multiple known security vulnerabilities. An attacker who successfully exploits these vulnerabilities could potentially access sensitive information, cause denial of service, or disrupt system availability.

Recommended immediate actions

ABB recommends the following mitigation measures:

- Replace bundled MongoDB with a supported version if IIoT services are required:

    - Where IIoT functionality is required, the bundled MongoDB instance can be replaced with a supported and patched version through manual configuration.
    - The following zenon online help section explains the process of installing and using your own MongoDB database: zenHelpViewer
- Uninstall IIoT Services wherever it's not required:
    - If IIoT Services are not required, they can be removed using the Control panel uninstaller. This eliminates the dependency on MongoDB without affecting other zenon components.

Vulnerability severity and details

Multiple vulnerabilities exist in the MongoDB component included in the affected systems. The issue arises due to the use of **MongoDB version 4.2**, which has reached end-of-life (EOL) status and is no longer supported by the vendor. As a result, this version does not receive security updates or patches, leaving it exposed to multiple publicly known vulnerabilities.

An attacker could exploit these vulnerabilities by interacting with the affected system over the network, potentially allowing unauthorized access to sensitive information or causing disruption to system services, leading to reduced availability.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) for both v3.1 and v4.0. Since this advisory addresses the use of an unsupported component with multiple known vulnerabilities rather than a single specific CVE, a representative severity range is provided.

CVE-2025-14847 - Zlib compressed protocol header length confusion may allow memory read

Description:
Mismatched length fields in Zlib compressed protocol headers may allow a read of uninitialized heap memory by an unauthenticated client. This issue affects all MongoDB Server v7.0 prior to 7.0.28 versions, MongoDB Server v8.0 versions prior to 8.0.17, MongoDB Server v8.2 versions prior to 8.2.3, MongoDB Server v6.0 versions prior to 6.0.27, MongoDB Server v5.0 versions prior to 5.0.32, MongoDB Server v4.4 versions prior to 4.4.30, MongoDB Server v4.2 versions greater than or equal to 4.2.0, MongoDB Server v4.0 versions greater than or equal to 4.0.0, and MongoDB Server v3.6 versions greater than or equal to 3.6.0.

CVSS

CVSS v3.1 Base Score:	7.5
CVSS v3.1 Temporal Score:	7.5
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSS v4.0 Score	8.7
CVSS v4.0 Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

CWE
CWE - CWE-130: Improper Handling of Length Parameter Inconsistency (4.20)

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2025-14847

CVE-2020-7928 - Improper neutralization of null byte leads to read overrun

Description:
A user authorized to perform database queries may trigger a read overrun and access arbitrary memory by issuing specially crafted queries. This issue affects MongoDB Server v4.4 versions prior to 4.4.1; MongoDB Server v4.2 versions prior to 4.2.9; MongoDB Server v4.0 versions prior to 4.0.20 and MongoDB Server v3.6 versions prior to 3.6.20.

CVSS

CVSS v3.1 Base Score:	6.5
CVSS v3.1 Temporal Score:	6.5
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
CVSS v4.0 Score	NVD assessment not yet provided.
CVSS v4.0 Vector:	NVD assessment not yet provided.

CWE
CWE - CWE-158: Improper Neutralization of Null Byte or NUL Character (4.20)

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2020-7928

CVE-2020-7921 - Administrative action may disable enforcement of per-user IP whitelisting

Description:
Improper serialization of internal state in the authorization subsystem in MongoDB Server's authorization subsystem permits a user with valid credentials to bypass IP whitelisting protection mechanisms following administrative action. This issue affects MongoDB Server v4.2 versions prior to 4.2.3; MongoDB Server v4.0 versions prior to 4.0.15; MongoDB Server v4.3 versions prior to 4.3.3and MongoDB Server v3.6 versions prior to 3.6.18.

CVSS

CVSS v3.1 Base Score:	5.3
CVSS v3.1 Temporal Score:	5.3
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N
CVSS v4.0 Score	NVD assessment not yet provided.
CVSS v4.0 Vector:	NVD assessment not yet provided.

CWE
CWE - CWE-863: Incorrect Authorization (4.20)
CWE - CWE-182: Collapse of Data into Unsafe Value (4.20)

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2020-7921

CVE-2020-7925 - Denial of Service when processing malformed Role names

Description:
Incorrect validation of user input in the role name parser may lead to use of uninitialized memory allowing an unauthenticated attacker to use a specially crafted request to cause a denial of service. This issue affects MongoDB Server v4.4 versions prior to 4.4.0-rc12; MongoDB Server v4.2 versions prior to 4.2.9.

CVSS

CVSS v3.1 Base Score:	7.5
CVSS v3.1 Temporal Score:	7.5
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CVSS v4.0 Score	NVD assessment not yet provided.
CVSS v4.0 Vector:	NVD assessment not yet provided.

CWE
CWE - CWE-475: Undefined Behavior for Input to API (4.20)

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2020-7925

CVE-2020-7929 - Specially crafted regex query can cause DoS

Description:
A user authorized to perform database queries may trigger denial of service by issuing specially crafted query contain a type of regex. This issue affects MongoDB Server v3.6 versions prior to 3.6.21 and MongoDB Server v4.0 versions prior to 4.0.20.

CVSS

CVSS v3.1 Base Score:	6.5
CVSS v3.1 Temporal Score:	6.5
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
CVSS v4.0 Score	NVD assessment not yet provided.
CVSS v4.0 Vector:	NVD assessment not yet provided.

CWE
CWE - CWE-185: Incorrect Regular Expression (4.20)

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2020-7929

CVE-2020-7923 - Specific GeoQuery can cause DoS against MongoDB Server

Description:
A user authorized to perform database queries may cause denial of service by issuing specially crafted queries, which violate an invariant in the query subsystem's support for geoNear. This issue affects MongoDB Server v4.4 versions prior to 4.4.0-rc7; MongoDB Server v4.2 versions prior to 4.2.8 and MongoDB Server v4.0 versions prior to 4.0.19.

CVSS

CVSS v3.1 Base Score: 6.5
CVSS v3.1 Temporal Score: 6.5
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVSS v4.0 Score NVD assessment not yet provided.
CVSS v4.0 Vector: NVD assessment not yet provided.

CWE
CWE - CWE-248: Uncaught Exception (4.20)

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2020-7923

CVE-2021-20330 - Specific replication command with malformed oplog entries can crash secondaries

Description:
An attacker with basic CRUD permissions on a replicated collection can run the applyOps command with specially malformed oplog entries, resulting in a potential denial of service on secondaries. This issue affects MongoDB Server v4.0 versions prior to 4.0.27; MongoDB Server v4.2 versions prior to 4.2.16; MongoDB Server v4.4 versions prior to 4.4.9.

CVSS

CVSS v3.1 Base Score: 6.5
CVSS v3.1 Temporal Score: 6.5
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVSS v4.0 Score NVD assessment not yet provided.
CVSS v4.0 Vector: NVD assessment not yet provided.

CWE
CWE - CWE-617: Reachable Assertion (4.20)

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-20330

CVE-2021-32036 - Denial of Service and Data Integrity vulnerability in features command

Description:
An authenticated user without any specific authorizations may be able to repeatedly invoke the features command where at a high volume may lead to resource depletion or generate high lock contention. This may result in denial of service and in rare cases could result in id field collisions. This issue affects MongoDB Server v5.0 versions prior to and including 5.0.3; MongoDB Server v4.4 versions prior to and including 4.4.9; MongoDB Server v4.2 versions prior to and including 4.2.16 and MongoDB Server v4.0 versions prior to and including 4.0.28

CVSS

CVSS v3.1 Base Score: 7.1
CVSS v3.1 Temporal Score: 7.1
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H

CVSS v4.0 Score NVD assessment not yet provided.
CVSS v4.0 Vector: NVD assessment not yet provided.

CWE
CWE - CWE-770: Allocation of Resources Without Limits or Throttling (4.20)

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-32036

CVE-2021-32040 - Large aggregation pipelines with a specific stage can crash mongod under default configuration

Description:
It may be possible to have an extremely long aggregation pipeline in conjunction with a specific stage/operator and cause a stack overflow due to the size of the stack frames used by that stage. If an attacker could cause such an aggregation to occur, they could maliciously crash MongoDB in a DoS attack. This vulnerability affects MongoDB Server v4.4 versions prior to and including 4.4.28, MongoDB Server v5.0 versions prior to 5.0.4 and MongoDB Server v4.2 versions prior to 4.2.16. Workaround: >= v4.2.16 users and all v4.4 users can add the --setParameter internalPipelineLengthLimit=50 instead of the default 1000 to mongod at startup to prevent a crash.

CVSS

CVSS v3.1 Base Score: 7.5
CVSS v3.1 Temporal Score: 7.5
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v4.0 Score NVD assessment not yet provided.
CVSS v4.0 Vector: NVD assessment not yet provided.

CWE
CWE - CWE-787: Out-of-bounds Write (4.20)
CWE - CWE-121: Stack-based Buffer Overflow (4.20)

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/cve-2021-32040

CVE-2021-20333 - Server log entry spoofing via newline injection

Description:
Sending specially crafted commands to a MongoDB Server may result in artificial log entries being generated or for log entries to be split. This issue affects MongoDB Server v3.6 versions prior to 3.6.20; MongoDB Server v4.0 versions prior to 4.0.21 and MongoDB Server v4.2 versions prior to 4.2.10.

CVSS

CVSS v3.1 Base Score: 5.3
CVSS v3.1 Temporal Score: 5.3
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVSS v4.0 Score NVD assessment not yet provided.

CVSS v4.0 Vector: NVD assessment not yet provided.

CWE
CWE - CWE-116: Improper Encoding or Escaping of Output (4.20)
CWE - CWE-117: Improper Output Neutralization for Logs (4.20)

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-20333

CVE-2020-7924 - Specific command line parameter might result in accepting invalid certificate

Description:
Usage of specific command line parameter in MongoDB Tools which was originally intended to just skip hostname checks, may result in MongoDB skipping all certificate validation. This may result in accepting invalid certificates.This issue affects: MongoDB Inc. MongoDB Database Tools 3.6 versions later than 3.6.5; 3.6 versions prior to 3.6.21; 4.0 versions prior to 4.0.21; 4.2 versions prior to 4.2.11; 100 versions prior to 100.2.0. MongoDB Inc. Mongomirror 0 versions later than 0.6.0.

CVSS

CVSS v3.1 Base Score: 6.5
CVSS v3.1 Temporal Score: 6.5
CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS v4.0 Score NVD assessment not yet provided.
CVSS v4.0 Vector: NVD assessment not yet provided.

CWE
CWE - CWE-295: Improper Certificate Validation (4.20)

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2020-7924

CVE-2021-20328 - MongoDB Java driver client-side field level encryption not verifying KMS host name

Description:
Specific versions of the Java driver that support client-side field level encryption (CSFLE) fail to perform correct host name verification on the KMS server’s certificate. This vulnerability in combination with a privileged network position active MITM attack could result in interception of traffic between the Java driver and the KMS service rendering Field Level Encryption ineffective. This issue was discovered during internal testing and affects all versions of the Java driver that support CSFLE. The Java async, Scala, and reactive streams drivers are not impacted. This vulnerability does not impact driver traffic payloads with CSFLE-supported key services originating from applications residing inside the AWS, GCP, and Azure network fabrics due to compensating controls in these environments. This issue does not impact driver workloads that don’t use Field Level Encryption.

CVSS

CVSS v3.1 Base Score: 6.8
CVSS v3.1 Temporal Score: 6.8
CVSS v3.1 Vector: CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS v4.0 Score	NVD assessment not yet provided.
CVSS v4.0 Vector:	NVD assessment not yet provided.

CWE
CWE - CWE-295: Improper Certificate Validation (4.20)

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-20328

CVE-2021-20334 - Local privilege escalation in MongoDB Compass for Windows

Description:
A malicious 3rd party with local access to the Windows machine where MongoDB Compass is installed can execute arbitrary software with the privileges of the user who is running MongoDB Compass. This issue affects: MongoDB Inc. MongoDB Compass 1.x version 1.3.0 on Windows and later versions; 1.x versions prior to 1.25.0 on Windows.

CVSS

CVSS v3.1 Base Score:	7.8
CVSS v3.1 Temporal Score:	7.8
CVSS v3.1 Vector:	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Score	NVD assessment not yet provided.
CVSS v4.0 Vector:	NVD assessment not yet provided.

CWE
CWE - CWE-250: Execution with Unnecessary Privileges (4.20)

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2021-20334

Mitigating factors

Refer to section “General security recommendations” for further advise on how to keep your system secure.

Frequently asked questions

What causes this vulnerability?

The vulnerability is caused by the use of an outdated MongoDB 4.2 component, which contains known security weaknesses.

What are IIoT Services?

IIoT Services are a set of distributed software components designed to enable industrial data collection, processing, and integration across multiple systems. They can be deployed on separate machines or in

the cloud, and use web-based technologies to ensure easy access, interoperability, and support across different devices.

What might an attacker use the vulnerability to do?

An attacker exploiting these vulnerabilities could read sensitive memory contents or crash the MongoDB service, causing denial of service. Since v4.2 is end of life and multiple CVEs have been disclosed publicly, exposed instances risk unauthenticated data exfiltration, not just downtime.

How could an attacker exploit this vulnerability?

An attacker could attempt to interact with the MongoDB service through network access or malicious input to exploit known vulnerabilities.

Could this vulnerability be exploited remotely?

Yes, an attacker with network access to the affected system could attempt exploitation.

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

No direct impact on functional safety is expected. However, system availability may be affected.

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

Yes, the MongoDB 4.2 CVEs are publicly disclosed. However, zenon's specific exposure, bundling this vulnerable version has not itself been publicly disclosed; it was identified during this assessment.

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

The following should be taken into consideration when planning system protection.

- Recognizing and familiarizing all parts of the system and the system's communication links.
- Removing all unnecessary communication links in the system.
- Rating the security level of remaining connections and improving them with applicable methods to reach the required security level.
- Hardening the system by removing or deactivating all unused processes, communication ports, and services.
- Checking that the whole system has valid backups available from all applicable parts.
- Collecting and storing backups of the system components and keeping those up to date.
- Removing all unnecessary user accounts.
- Define the role-based access right and follow the principle of least privilege.
- Defining password policies.
- Changing default passwords and using strong passwords.

- Checking that the link from a substation to an upper-level system uses strong encryption and authentication.
- Segregating public networks (untrusted) from automation networks (trusted).
- Segmenting traffic and networks.
- Using firewalls and demilitarized zones.
- Assessing and patching the system periodically.
- Using malware protection in workstations and keeping those up to date.

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	2026-07-30