

---

CYBER SECURITY ADVISORY

# **ABB Ability Camera Connect Vulnerabilities in outdated 3rd party component (SQLite 3.2.4)**

## **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

ABB Ability Camera Connect 2.0.0.42 and below

## Vulnerability IDs

CVE-2025-6965, CVE-2025-3277, CVE-2023-7104, CVE-2022-35737, CVE-2020-15358, CVE-2020-13632, CVE-2020-13631, CVE-2020-13630, CVE-2020-13435, CVE-2020-13434, CVE-2020-11656, CVE-2020-11655, CVE-2019-19646, CVE-2019-19645, CVE-2018-20506, CVE-2018-20505, CVE-2018-20346, CVE-2018-8740, CVE-2017-10989, CVE-2016-6153, CVE-2015-6607, CVE-2015-5895, CVE-2015-3717, CVE-2015-3416, CVE-2015-3415.

## Summary

ABB is aware of public reports of vulnerabilities in a 3<sup>rd</sup> party dependency SQLite Version 3.2.4 which was delivered together with the installation package of Camera Connect Version 2.0.0.42 and below. An update is available that resolves a privately reported outdated 3<sup>rd</sup> party component with vulnerabilities in the product versions listed above.

An attacker who successfully exploited any of these vulnerabilities in the 3<sup>rd</sup> party component could potentially compromise the system in different ways.

## Recommended immediate actions

The problem is corrected in the following product versions:

ABB Ability Camera Connect 2.0.0.49.

The easiest path to mitigate the problem is an update of ABB Ability Camera Connect system by the customer. ABB recommends that customers apply the update at earliest convenience.

## Vulnerability severity and details

Vulnerabilities existent in the 3<sup>rd</sup> party component SQLite included in the product versions listed above.

The following CVEs and their descriptions were consulted in the CVE<sup>1</sup> website as well as the Common Vulnerability Scoring System (CVSS) for both v3.1<sup>2</sup> and v4.0<sup>3</sup> and the indicated Common Weakness Enumerations (CWE).

### CVE-2025-6965

There exists a vulnerability in SQLite versions before 3.50.2 where the number of aggregate terms could exceed the number of columns available. This could lead to a memory corruption issue. We recommend upgrading to version 3.50.2 or above.

#### CVSS

CVSS v3.1 Base Score: N/A  
CVSS v3.1 Temporal Score: N/A  
CVSS v3.1 Vector: N/A

CVSS v4.0 Score: 7.2  
CVSS v4.0 Vector: **CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:L/VI:H/VA:L/SC:L/SI:H/SA:L/S:N/A  
U:N/R:U/V:D/RE:L/U:Green**

#### CWE

CWE-197: Numeric Truncation Error

#### CVE

NVD Summary Link: <https://nvd.nist.gov/vuln/detail/CVE-2025-6965>

<sup>1</sup> [www.cve.org](http://www.cve.org)

<sup>2</sup> For the CVSS v3.1 scoring only the CVSS Base Score and the Temporal Score (if information is available) are considered in this advisory. 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.

<sup>3</sup> For the CVSS v4.0 scoring only the CVSS Base Metrics and the CVSS Supplemental Metrics (if information is available) are considered in this advisory. The CVSS Environmental and Threat Metrics, which can affect the vulnerability severity, are not provided in this advisory since they reflect the potential impact of a vulnerability within the end-user organizations' computing environment and over time depending on the vulnerability exploit maturity. Therefore, end-user organizations are recommended to analyze their situation and specify the Environmental and Threat Metrics.

### Mitigating Factor

Camera Connect is deployed as an OT solution typically operating in ISA-95 Level 2 (control/supervisory level) environments. This deployment architecture provides inherent risk mitigation:

- **Network Segmentation:** The solution operates within isolated industrial control networks, separated from IT networks and the internet by firewalls and demilitarized zones (DMZs).
- **Access Control:** Access to the Camera Connect system is restricted to authorized plant operators and maintenance personnel through role-based access controls and authentication mechanisms.
- **Limited Attack Surface:** The CVSS v4.0 vector indicates Network attack vector (AV:N), High attack complexity (AC:H), and requires Low privileges (PR:L), significantly reducing the likelihood of exploitation in a controlled OT environment.
- **Physical Security:** Level 2 systems are typically located in secure facilities with physical access controls.
- **Operational Monitoring:** Industrial environments maintain operational monitoring that can detect anomalous behavior.

Given these factors, successful exploitation would require an authenticated attacker with specific knowledge of the system, positioned within the control network, making this vulnerability Low risk in properly segmented OT deployments.

### CVE-2025-3277

An integer overflow can be triggered in SQLite's `concat_ws()` function. The resulting, truncated integer is then used to allocate a buffer. When SQLite then writes the resulting string to the buffer, it uses the original, untruncated size and thus a wild heap buffer overflow of size ~4GB can be triggered. This can result in arbitrary code execution.

### CVSS

CVSS v3.1 Base Score: N/A  
CVSS v3.1 Temporal Score: N/A  
CVSS v3.1 Vector: N/A

CVSS v4.0 Score: 6.9  
CVSS v4.0 Vector: **CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:L/SI:L/SA:L**

### CWE

CWE-122: Heap-based Buffer Overflow

### CVE

NVD Summary Link: <https://nvd.nist.gov/vuln/detail/CVE-2025-3277>

### Mitigating Factor

While this vulnerability has a CVSS v4.0 score of 6.9 and theoretically allows arbitrary code execution, Camera Connect's deployment model provides significant protection:

1. **Function-Specific Vulnerability:** The vulnerability requires specific use of the `concat_ws()` SQL function, which is not utilized in Camera Connect's standard database operations.
2. **Input Validation:** Camera Connect implements input validation and sanitization mechanisms that limit the ability to craft malicious SQL queries.
3. **Network Isolation:** As an ISA-95 Level 2 OT solution, Camera Connect operates within protected industrial networks with limited external connectivity.
4. **Authenticated Access Required:** Database operations in Camera Connect require user authentication and are performed within the context of the application's business logic rather than through direct user-supplied SQL.
5. **Memory Protection:** Modern operating systems deployed in industrial environments typically include memory protection mechanisms (DEP, ASLR) that make heap exploitation more difficult.

The risk is further reduced by operational procedures requiring change management and validation testing before any modifications to the system configuration or database queries.

### CVE-2023-7104

A vulnerability was found in SQLite SQLite3 up to 3.43.0 and classified as critical. This issue affects the function `sessionReadRecord` of the file `ext/session/sqlite3session.c` of the component `makealltest Handler`. The manipulation leads to heap-based buffer overflow. It is recommended to apply a patch to fix this issue.

### CVSS

CVSS v3.1 Base Score: 5.5  
CVSS v3.1 Temporal Score: 5.5  
CVSS v3.1 Vector: **CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L**

CVSS v4.0 Score: N/A  
CVSS v4.0 Vector: N/A

### CWE

CWE-122 Heap-based Buffer Overflow

### CVE

NVD Summary Link: <https://nvd.nist.gov/vuln/detail/CVE-2023-7104>

### Mitigating Factor

This vulnerability affects the SQLite session extension (FTS3), which is an optional component:

1. **Component Usage:** Camera Connect's implementation do not utilize the SQLite session extension functionality, rendering this vulnerability non-applicable to the actual deployment.
2. **Adjacent Network Attack:** The CVSS vector indicates Adjacent Network access (AV:A) is required, meaning the attacker must be on the same local network segment. In OT environments, network segmentation at ISA-95 Level 2 restricts access to authorized personnel only.
3. **Authentication Required:** Low privilege credentials (PR:L) are still required to exploit this vulnerability, providing an additional barrier in Camera Connect's access-controlled environment.

4. **Limited Impact:** The CVSS score of 5.5 (MEDIUM) reflects limited impact to confidentiality, integrity, and availability (C:L/I:L/A:L).
5. **Extension-Specific:** The vulnerability is in the make all test handler of the session extension, which is typically not used in production deployments.

Camera Connect's restricted operational environment and limited use of optional SQLite features significantly reduce the exploitability of this vulnerability.

## CVE-2022-35737

SQLite 1.0.12 through 3.39.x before 3.39.2 sometimes allows an array-bounds overflow if billions of bytes are used in a string argument to a C API.

### CVSS

CVSS v3.1 Base Score:	7.5
CVSS v3.1 Temporal Score:	7.5
CVSS v3.1 Vector:	<b>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H</b>
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

### CWE

CWE-129                      Improper Validation of Array Index

### CVE

NVD Summary Link            <https://nvd.nist.gov/vuln/detail/CVE-2022-35737>

### Mitigating Factor

This vulnerability has specific prerequisites that limit its applicability to Camera Connect:

1. **Resource Requirements:** The vulnerability requires "billions of bytes" to be used in a string argument, representing an extreme edge case that exceeds typical operational parameters in industrial control systems.
2. **C API Specific:** This vulnerability affects direct C API calls to SQLite. Camera Connect uses higher-level database access patterns through managed code or SQL queries, not direct low-level C API manipulation.
3. **Memory Constraints:** Industrial systems running Camera Connect typically operate within defined memory boundaries and resource allocation limits that would prevent the allocation of multi-gigabyte strings.
4. **Input Validation:** Application-level input validation and size restrictions in Camera Connect prevent the submission of abnormally large data values.
5. **Practical Impossibility:** In the context of Camera Connect's use case (camera connectivity and video management), there are no legitimate operational scenarios requiring billion-byte string parameters.

The extreme resource requirements and specific attack vector make this vulnerability impractical to exploit in Camera Connect's typical deployment environment.

## CVE-2020-15358

In SQLite before 3.32.3, select.c mishandles query-flattener optimization, leading to a multiSelectOrderBy heap overflow because of misuse of transitive properties for constant propagation.

### CVSS

CVSS v3.1 Base Score: 5.5  
CVSS v3.1 Temporal Score: 5.5  
CVSS v3.1 Vector: **CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H**

CVSS v4.0 Score: N/A  
CVSS v4.0 Vector: N/A

### CWE

CWE-787 Out-of-bounds Write

### CVE

NVD Summary Link <https://nvd.nist.gov/vuln/detail/CVE-2020-15358>

### Mitigating Factor

This vulnerability involves specific SQL query patterns and optimization edge cases:

1. **Query Complexity:** The vulnerability requires specific use of complex multi-select queries with ORDER BY clauses that trigger the query-flattener optimization. Camera Connect's database queries are typically straightforward CRUD operations for camera configuration and video metadata.
2. **Limited Query Construction:** Users of Camera Connect do not have direct SQL query construction capabilities; all database interactions occur through the application's predefined data access layer.
3. **Query Review:** Database queries in Camera Connect are part of the application codebase and undergo development review and testing, reducing the likelihood of crafted malicious query patterns.
4. **Heap Overflow Protection:** Modern operating systems and runtime environments include heap overflow protection mechanisms that can detect and prevent exploitation attempts.
5. **Operational Context:** The specific query pattern required to trigger this vulnerability is unlikely to occur in Camera Connect's operational use cases related to camera management and video streaming.

The constrained database access model and typical query patterns in Camera Connect operations make this vulnerability extremely unlikely to be triggered in practice.

## CVE-2020-13632

ext/fts3/fts3\_snippet.c in SQLite before 3.32.0 has a NULL pointer dereference via a crafted matchinfo() query.

### CVSS

CVSS v3.1 Base Score: 5.5  
CVSS v3.1 Temporal Score: 5.5

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

CVSS v4.0 Score N/A

CVSS v4.0 Vector: N/A

### CWE

CWE-476 NULL Pointer Dereference

### CVE

NVD Summary Link <https://nvd.nist.gov/vuln/detail/CVE-2020-13632>

### Mitigating Factor

This vulnerability affects the SQLite Full-Text Search (FTS3) extension with specific conditions:

1. **FTS3 Extension:** Camera Connect do not utilize SQLite's Full-Text Search capabilities, as the solution is primarily focused on camera connectivity, configuration, and video management rather than full-text search operations.
2. **Specific Function:** The vulnerability requires use of the `matchinfo()` function, which is a specialized FTS3 query function which is not part of Camera Connect's database access patterns.
3. **Denial of Service Impact:** This is a NULL pointer dereference leading to application crash (denial of service), not remote code execution. In an OT environment, application crashes are detected and can trigger automatic restart mechanisms.
4. **Access Control:** Crafting the specific malicious query would require authenticated database access and knowledge of the database schema.
5. **Feature-Specific:** The FTS3 is not enabled or compiled into the SQLite build used by Camera Connect, so this vulnerability is not present.

The specialized nature of this vulnerability and its limitation to a specific extension function that Camera Connect likely does not utilize significantly reduces the risk.

### CVE-2020-13631

SQLite before 3.32.0 allows a virtual table to be renamed to the name of one of its shadow tables, related to `alter.c` and `build.c`.

### CVSS

CVSS v3.1 Base Score: 5.5

CVSS v3.1 Temporal Score: 5.5

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

CVSS v4.0 Score N/A

CVSS v4.0 Vector: N/A

### CWE

N/A N/A

## CVE

NVD Summary Link <https://nvd.nist.gov/vuln/detail/CVE-2020-13631>

### Mitigating Factor

This vulnerability involves database schema manipulation:

1. **Administrative Privilege Requirement:** Renaming tables requires database administrative privileges, which are not granted to normal Camera Connect users.
2. **Virtual Table Usage:** This vulnerability specifically affects virtual tables, which are an advanced SQLite feature. Camera Connect's database schema uses standard tables for its operational data.
3. **Schema Stability:** In industrial OT environments, database schemas are static and controlled through formal change management processes. Dynamic table creation and renaming are not typical operational activities.
4. **Limited Impact:** Even if exploited, the impact is primarily on database integrity rather than system availability or confidentiality. Database backups and recovery procedures in industrial environments provide restoration capabilities.
5. **Application Logic:** Camera Connect's application layer mediates all database interactions, preventing direct DDL (Data Definition Language) operations by end users.

The requirement for administrative access and the uncommon use case of dynamic schema modification in OT environments make this vulnerability low risk for Camera Connect.

## CVE-2020-13630

ext/fts3/fts3.c in SQLite before 3.32.0 has a use-after-free in fts3EvalNextRow, related to the snippet feature.

### CVSS

CVSS v3.1 Base Score: 7.0  
CVSS v3.1 Temporal Score: 7.0  
CVSS v3.1 Vector: **CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H**

CVSS v4.0 Score: N/A  
CVSS v4.0 Vector: N/A

## CWE

CWE-416 Use After Free

## CVE

NVD Summary Link <https://nvd.nist.gov/vuln/detail/CVE-2020-13630>

### Mitigating Factor

This is another FTS3 extension-specific vulnerability:

1. **FTS3 Extension Dependency:** The vulnerability exists only in the FTS3 (Full-Text Search) extension. Camera Connect does not enable or use FTS3 functionality, so this vulnerability is not applicable.

2. **Snippet Feature:** The use-after-free specifically affects the snippet feature of FTS3, which generates text snippets from search results - a specialized feature unlikely to be required in Camera Connect's video management operations.
3. **Memory Management:** Modern operating systems and runtime environments include heap management protections that can detect use-after-free conditions and prevent exploitation.
4. **Crash vs. Exploitation:** While use-after-free vulnerabilities can potentially lead to code execution, successful exploitation requires precise memory manipulation. The more likely outcome is application crash (denial of service).
5. **Function-Specific:** The vulnerability is in `fts3EvalNextRow`, a specific internal function that would only be triggered through specialized FTS3 queries.

Camera Connect's non-existent use of advanced FTS3 features significantly reduces exposure to this vulnerability.

## CVE-2020-13435

SQLite through 3.32.0 has a segmentation fault in `sqlite3ExprCodeTarget` in `expr.c`.

### CVSS

CVSS v3.1 Base Score: 5.5  
CVSS v3.1 Temporal Score: 5.5  
CVSS v3.1 Vector: **CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H**

CVSS v4.0 Score: N/A  
CVSS v4.0 Vector: N/A

### CWE

CWE-476: NULL Pointer Dereference

### CVE

NVD Summary Link: <https://nvd.nist.gov/vuln/detail/CVE-2020-13435>

### Mitigating Factor

This vulnerability results in a segmentation fault (application crash):

1. **Denial of Service Impact:** A segmentation fault leads to application crash, representing a denial of service rather than data breach or code execution. In industrial environments, application monitoring and automatic restart mechanisms can quickly restore service.
2. **Query Complexity:** The vulnerability requires specific expression patterns in SQL queries. Camera Connect's predefined query templates and parameterized queries reduce the likelihood of triggering this condition.
3. **High Availability Design:** OT solutions typically incorporate redundancy and failover mechanisms to maintain operational continuity in the event of application failures.
4. **Limited Window:** In a segmentation fault scenario, the application terminates immediately, limiting any potential data exposure compared to vulnerabilities that allow sustained unauthorized access.
5. **Operational Monitoring:** Industrial control systems maintain operational monitoring that alerts operators to application failures, enabling rapid response.

While denial of service is undesirable in OT environments, the impact is significantly less severe than vulnerabilities allowing unauthorized access or data manipulation.

## CVE-2020-13434

SQLite through 3.32.0 has an integer overflow in `sqlite3_str_vappendf` in `printf.c`.

### CVSS

CVSS v3.1 Base Score: 5.5  
CVSS v3.1 Temporal Score: 5.5  
CVSS v3.1 Vector: **CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H**

CVSS v4.0 Score: N/A  
CVSS v4.0 Vector: N/A

### CWE

CWE-476: NULL Pointer Dereference

### CVE

NVD Summary Link: <https://nvd.nist.gov/vuln/detail/CVE-2020-13434>

### Mitigating Factor

This vulnerability affects SQLite's internal `printf` functionality:

1. **Internal Function:** The vulnerability is in `sqlite3_str_vappendf`, an internal string formatting function. Camera Connect's use of SQLite typically occurs through higher-level database operations that don't directly expose this function.
2. **Integer Overflow Requirements:** Triggering an integer overflow requires carefully crafted input with extreme values, which would be constrained by Camera Connect's input validation and data type definitions.
3. **Format String Context:** The vulnerability occurs in `printf`-style formatting operations. Camera Connect's database interactions use parameterized queries and typed data binding rather than format string operations.
4. **Bounds Checking:** Application-level data validation limits the size and format of values passed to database operations, preventing the extreme conditions necessary to trigger this overflow.
5. **Limited Exposure:** The specific code path would need to be triggered through very specific database operations that may not occur in Camera Connect's normal operational workflow.

The internal nature of this vulnerability and Camera Connect's structured data access patterns make exploitation highly unlikely in practice.

## CVE-2020-11656

In SQLite through 3.31.1, the `ALTER TABLE` implementation has a use-after-free, as demonstrated by an `ORDER BY` clause that belongs to a compound `SELECT` statement.

### CVSS

CVSS v3.1 Base Score: 9.8

CVSS v3.1 Temporal Score: 9.8  
CVSS v3.1 Vector: **CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H**

CVSS v4.0 Score: N/A  
CVSS v4.0 Vector: N/A

#### CWE

CWE-416 Use After Free

#### CVE

NVD Summary Link <https://nvd.nist.gov/vuln/detail/CVE-2020-11656>

#### Mitigating Factor

This vulnerability involves database schema modification operations:

1. **Schema Modification:** The vulnerability is in ALTER TABLE operations. In OT environments, database schemas are static and managed through controlled change management processes, not dynamic runtime modifications.
2. **Administrative Operation:** ALTER TABLE requires elevated database privileges that are not granted to regular Camera Connect users or operational personnel.
3. **Compound Query Requirement:** The vulnerability specifically requires a compound SELECT statement with ORDER BY clause in the context of ALTER TABLE - an unusual and non-standard SQL pattern.
4. **Application-Mediated Access:** Camera Connect does not provide interfaces for direct SQL execution or schema modification to end users.
5. **Static Schema:** Camera Connect's database schema is established during installation and remains stable throughout operational use, with updates only occurring during planned software upgrades.

The administrative nature of ALTER TABLE operations and the absence of dynamic schema modification in normal Camera Connect usage effectively eliminate this attack vector.

#### CVE-2020-11655

SQLite through 3.31.1 allows attackers to cause a denial of service (segmentation fault) via a malformed window-function query because the AggInfo object's initialization is mishandled.

#### 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: N/A  
CVSS v4.0 Vector: N/A

#### CWE

CWE-665 Improper Initialization

## CVE

NVD Summary Link <https://nvd.nist.gov/vuln/detail/CVE-2020-11655>

### Mitigating Factor

This vulnerability involves SQL window functions:

1. **Window Function Usage:** Window functions (e.g., ROW\_NUMBER(), RANK(), LAG()) are advanced SQL features primarily used in analytical queries. Camera Connect's operational database queries typically use simpler CRUD operations and aggregations.
2. **Denial of Service Only:** The impact is a segmentation fault causing application crash, not data breach or code execution. In industrial environments, service interruption is managed through monitoring and automatic restart capabilities.
3. **Query Complexity:** Crafting a malformed window function query requires knowledge of the database schema and specific query construction - not accessible through Camera Connect's standard user interfaces.
4. **Controlled Environment:** In ISA-95 Level 2 deployments, any application crashes are immediately visible to operators and can be investigated through system logs and monitoring.
5. **Feature Utilization:** Camera Connect's queries do not utilize window functions, so this attack vector is not present in the application.

The specialized nature of window functions and the controlled operational environment limit the practical impact of this vulnerability.

## CVE-2019-19646

pragma.c in SQLite through 3.30.1 mishandles NOT NULL in an integrity\_check PRAGMA command in certain cases of generated columns.

### CVSS

CVSS v3.1 Base Score: 9.8  
CVSS v3.1 Temporal Score: 9.8  
CVSS v3.1 Vector: [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H](#)

CVSS v4.0 Score: N/A  
CVSS v4.0 Vector: N/A

## CWE

CWE-754 Improper Check for Unusual or Exceptional Conditions

## CVE

NVD Summary Link <https://nvd.nist.gov/vuln/detail/CVE-2019-19646>

### Mitigating Factor

This vulnerability involves SQLite's PRAGMA commands and generated columns:

1. **PRAGMA Commands:** PRAGMA commands are administrative database commands typically not accessible to end users. Camera Connect's application layer would not expose PRAGMA command execution to operators.

2. **Integrity Check Context:** The vulnerability specifically affects the integrity\_check PRAGMA, which is a database maintenance operation typically performed during development or maintenance windows, not during normal operation.
3. **Limited Impact:** Mishandling of NOT NULL in integrity checks would primarily affect database validation results rather than causing security breaches or service disruption.
4. **Administrative Access Required:** Execution of PRAGMA commands requires direct database access at an administrative level, which is restricted in production OT environments.

The specialized nature of this vulnerability and its limitation to administrative database maintenance operations make it non-applicable to Camera Connect's normal operational use.

## CVE-2019-19645

alter.c in SQLite through 3.30.1 allows attackers to trigger infinite recursion via certain types of self-referential views in conjunction with ALTER TABLE statements.

### CVSS

CVSS v3.1 Base Score: 5.5  
CVSS v3.1 Temporal Score: 5.5  
CVSS v3.1 Vector: **CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H**

CVSS v4.0 Score: N/A  
CVSS v4.0 Vector: N/A

### CWE

CWE-674 Uncontrolled Recursion

### CVE

NVD Summary Link <https://nvd.nist.gov/vuln/detail/CVE-2019-19645>

### Mitigating Factor

This vulnerability involves database views and schema modification:

1. **View Usage:** This vulnerability requires self-referential database views, which are advanced database constructs. Camera Connect's database schema uses standard tables and simple views without self-referential patterns.
2. **ALTER TABLE Requirement:** Triggering the vulnerability requires ALTER TABLE operations, which are administrative schema modification commands not available to normal users.
3. **Infinite Recursion Detection:** Modern operating systems and runtime environments typically include stack overflow protection and recursion detection that can terminate runaway processes.
4. **Schema Design:** Self-referential views represent poor database design practices that would be identified and corrected during development review.
5. **Static Schema:** Camera Connect's database schema is static and managed through formal change control, preventing the introduction of problematic self-referential view patterns.

The requirement for both specialized view design and administrative schema modification makes this vulnerability inapplicable to Camera Connect's operational environment.

## CVE-2018-20506

SQLite before 3.25.3, when the FTS3 extension is enabled, encounters an integer overflow (and resultant buffer overflow) for FTS3 queries in a "merge" operation that occurs after crafted changes to FTS3 shadow tables, allowing remote attackers to execute arbitrary code by leveraging the ability to run arbitrary SQL statements (such as in certain WebSQL use cases). This is a different vulnerability than CVE-2018-20346.

### CVSS

CVSS v3.0 Base Score: 8.1  
CVSS v3.0 Temporal Score: 8.1  
CVSS v3.0 Vector: **CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H**

CVSS v4.0 Score: N/A  
CVSS v4.0 Vector: N/A

### CWE

CWE-190 Integer Overflow or Wraparound

### CVE

NVD Summary Link <https://nvd.nist.gov/vuln/detail/CVE-2018-20506>

### Mitigating Factor

This vulnerability affects the FTS3 extension with specific attack requirements:

1. **FTS3 Extension:** Camera Connect do not utilize the Full-Text Search extension, making this vulnerability non-applicable.
2. **Shadow Table Manipulation:** The vulnerability requires crafted changes to FTS3 "shadow tables" (internal tables supporting FTS3 indexes). These shadow tables are not exposed through normal database operations and require direct low-level database access.
3. **Multi-Step Attack:** Exploitation requires multiple steps: enable FTS3, manipulate shadow tables, and then trigger a merge operation - each requiring specific database access and knowledge.
4. **ISA-95 Level 2 Deployment:** The "remote attackers" scenario is mitigated by network segmentation. Camera Connect operates in isolated control networks without direct internet exposure.

The combination of FTS3-specific requirements, shadow table manipulation, and network isolation makes this vulnerability low risk for Camera Connect deployments.

## CVE-2018-20505

SQLite 3.25.2, when queries are run on a table with a malformed PRIMARY KEY, allows remote attackers to cause a denial of service (application crash) by leveraging the ability to run arbitrary SQL statements (such as in certain WebSQL use cases).

### CVSS

CVSS v3.0 Base Score: 7.5  
CVSS v3.0 Temporal Score: 7.5  
CVSS v3.0 Vector: **CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H**

CVSS v4.0 Score N/A  
CVSS v4.0 Vector: N/A

## CWE

CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

## CVE

NVD Summary Link <https://nvd.nist.gov/vuln/detail/CVE-2018-20505>

## Mitigating Factor

This vulnerability is classified as CWE-89 (SQL Injection) in NVD, but exploitation still requires SQL execution paths that are not exposed in normal Camera Connect operation:

1. **Database Schema Validation:** Camera Connect's database schema is established during installation and validated through testing. A malformed PRIMARY KEY would be detected during development and corrected before deployment.
2. **DDL Access:** Creating or modifying PRIMARY KEY constraints requires database administrative privileges and DDL (Data Definition Language) access, which is not available to normal Camera Connect users.
3. **SQL Injection Controls:** Camera Connect uses parameterized queries and controlled query templates, which significantly reduce the likelihood of user-controlled SQL construction required for SQL injection exploitation.
4. **Denial of Service Impact:** The vulnerability leads to application crash rather than data breach or code execution. Industrial environments include application monitoring and automatic restart capabilities to maintain service availability.
5. **Static Schema:** Camera Connect's database schema remains static throughout operational use, with PRIMARY KEY definitions established and validated during initial installation.

The combination of SQL injection controls, restricted DDL access, and static schema management makes this vulnerability low risk in properly deployed Camera Connect systems.

## CVE-2018-20346

SQLite before 3.25.3, when the FTS3 extension is enabled, encounters an integer overflow (and resultant buffer overflow) for FTS3 queries that occur after crafted changes to FTS3 shadow tables, allowing remote attackers to execute arbitrary code by leveraging the ability to run arbitrary SQL statements (such as in certain WebSQL use cases), aka Magellan.

## CVSS

CVSS v3.0 Base Score: 8.1  
CVSS v3.0 Temporal Score: 8.1  
CVSS v3.0 Vector: **CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H**

CVSS v4.0 Score N/A  
CVSS v4.0 Vector: N/A

## CWE

CWE-190 Integer Overflow or Wraparound

### CVE

NVD Summary Link <https://nvd.nist.gov/vuln/detail/CVE-2018-20346>

### Mitigating Factor

This is the "Magellan" vulnerability, related to CVE-2018-20506:

1. **FTS3 Extension:** The vulnerability only affects installations where the FTS3 (Full-Text Search) extension is enabled. Camera Connect do not require or enable this extension.
2. **Shadow Table Manipulation:** Exploitation requires direct manipulation of FTS3 shadow tables, which are internal implementation details not exposed through standard SQL interfaces.
3. **Arbitrary SQL Execution:** The attack requires the "ability to run arbitrary SQL statements." Camera Connect uses parameterized queries and does not provide SQL injection points or direct SQL execution capabilities to users.
4. **OT Network Isolation:** The "remote attackers" threat model is mitigated by ISA-95 Level 2 network segmentation, which isolates the control network from external access.
5. **Multi-Stage Attack:** Successful exploitation requires multiple prerequisites: FTS3 enabled, ability to modify shadow tables, and ability to execute queries - each representing a significant barrier.

The specialized attack requirements and Camera Connect's deployment architecture make this high-profile vulnerability low risk in practice.

### CVE-2018-8740

In SQLite through 3.22.0, databases whose schema is corrupted using a CREATE TABLE AS statement could cause a NULL pointer dereference, related to build.c and prepare.c.

### CVSS

CVSS v3.0 Base Score: 7.5  
CVSS v3.0 Temporal Score: 7.5  
CVSS v3.0 Vector: **CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H**

CVSS v4.0 Score: N/A  
CVSS v4.0 Vector: N/A

### CWE

CWE-476 NULL Pointer Dereference

### CVE

NVD Summary Link <https://nvd.nist.gov/vuln/detail/CVE-2018-8740>

### Mitigating Factor

This vulnerability involves database schema corruption:

1. **Schema Corruption:** The vulnerability requires a corrupted database schema created via a CREATE TABLE AS statement. Camera Connect's database schema is established through controlled installation processes with validation and integrity checks.

2. **DDL Access:** CREATE TABLE statements require database administrative privileges, which are not available to normal Camera Connect users or operators.
3. **NULL Pointer Dereference:** The impact is a NULL pointer dereference causing application crash (denial of service), not data breach or code execution.
4. **Database Integrity:** Modern database deployments include integrity checking mechanisms that can detect corrupted schemas. Camera Connect likely includes database validation during startup.
5. **Backup and Recovery:** Industrial OT environments maintain database backups and recovery procedures that can restore a clean database schema if corruption is detected.

The requirement for database administrative access and the protective mechanisms around database schema integrity make this vulnerability low priority for Camera Connect deployments.

## CVE-2017-10989

The getNodeSize function in ext/rtree/rtree.c in SQLite through 3.19.3, as used in GDAL and other products, mishandles undersized RTree blobs in a crafted database, leading to a heap-based buffer over-read or possibly unspecified other impact.

### CVSS

CVSS v3.0 Base Score: 9.8  
CVSS v3.0 Temporal Score: 9.8  
CVSS v3.0 Vector: **CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H**

CVSS v4.0 Score: N/A  
CVSS v4.0 Vector: N/A

### CWE

CWE-125 Out-of-bounds Read

### CVE

NVD Summary Link <https://nvd.nist.gov/vuln/detail/CVE-2017-10989>

### Mitigating Factor

This vulnerability affects SQLite's R Tree extension:

1. **R Tree Extension:** This vulnerability is specific to the RTree (R-Tree spatial index) extension of SQLite. Camera Connect do not utilize spatial indexing capabilities, making this extension inactive.
2. **Crafted Database Requirement:** The vulnerability requires a specially crafted database with malformed RTree blobs. Camera Connect's database is generated and maintained by the application itself, not loaded from external sources.
3. **Spatial Data:** RTree indexes are used for spatial data queries (geographic/geometric data). Camera Connect's use case involves camera management and video streaming, which typically does not require spatial indexing.
4. **Limited Exposure:** The vulnerability requires both the RTree extension to be enabled and specific malformed data structures within the database.
5. **Database Source Control:** In OT environments, databases come from trusted sources and are protected by integrity checking mechanisms.

Camera Connect does not use the RTree extension, so this vulnerability is not applicable. Even if the extension is present, the controlled database environment significantly reduces risk.

## CVE-2016-6153

os\_unix.c in SQLite before 3.13.0 improperly implements the temporary directory search algorithm, which might allow local users to obtain sensitive information, cause a denial of service (application crash), or have unspecified other impact by leveraging use of the current working directory for temporary files.

### CVSS

CVSS v3.0 Base Score: 5.9  
CVSS v3.0 Temporal Score: 5.9  
CVSS v3.0 Vector: **CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L**  
  
CVSS v4.0 Score: N/A  
CVSS v4.0 Vector: N/A

### CWE

CWE-20 Improper Input Validation

### CVE

NVD Summary Link <https://nvd.nist.gov/vuln/detail/CVE-2016-6153>

### Mitigating Factor

This vulnerability affects temporary file handling on Unix-based systems:

1. **Windows Deployment:** Camera Connect is primarily deployed on Windows operating systems in industrial environments (note: the vulnerability description specifically references os\_unix.c). Windows-based deployments are not affected by this Unix-specific implementation issue.
2. **Local Access Required:** The CVE describes "local users" as the threat actors, requiring authenticated local system access. In OT environments, local system access is restricted to authorized administrators.
3. **Temporary File Usage:** The vulnerability relates to temporary file creation. Modern SQLite versions and Camera Connect's configuration may specify explicit temporary directory locations rather than relying on the default search algorithm.
4. **File System Permissions:** Windows operating systems used in industrial environments typically implement proper file system permissions and user access controls.
5. **Sensitive Information Exposure:** Any sensitive information in temporary files would be limited to transient database operations and would not include long-term sensitive data.

The Unix-specific nature of this vulnerability and Camera Connect's typical deployment on Windows systems significantly reduces applicability.

## CVE-2015-6607

SQLite before 3.8.9, as used in Android before 5.1.1 LMY48T, allows attackers to gain privileges via a crafted application, aka internal bug 20099586.

## CVSS

CVSS v3.1 Base Score: N/A  
CVSS v3.1 Temporal Score: N/A  
CVSS v3.1 Vector: N/A

CVSS v4.0 Score: N/A  
CVSS v4.0 Vector: N/A

## CWE

CWE-264 Permissions, Privileges, and Access Controls

## CVE

NVD Summary Link: N/A

## Mitigating Factor

This vulnerability is specific to Android environments:

1. **Platform-Specific:** This CVE specifically affects Android operating systems (before version 5.1.1 LMY48T). Camera Connect is a Windows-based application for industrial environments, not an Android mobile application.
2. **Different Attack Surface:** The vulnerability involves Android's application sandbox and privilege model, which is fundamentally different from Windows desktop application security.
3. **Application Context:** As noted in the CVE description, it's "internal bug 20099586" - an Android-specific internal vulnerability in how Android handled SQLite.
4. **Non-Applicable Platform:** Since Camera Connect operates on Windows systems in OT environments rather than Android mobile devices, this CVE does not apply to Camera Connect deployments.

This CVE is effectively not relevant to Camera Connect due to platform incompatibility.

## CVE-2015-5895

Multiple unspecified vulnerabilities in SQLite before 3.8.10.2, as used in Apple iOS before 9, have unknown impact and attack vectors.

## CVSS

CVSS v3.1 Base Score: N/A  
CVSS v3.1 Temporal Score: N/A  
CVSS v3.1 Vector: N/A

CVSS v4.0 Score: N/A  
CVSS v4.0 Vector: N/A

## CWE

N/A: N/A

## CVE

NVD Summary Link N/A

### Mitigating Factor

This CVE has limited public information:

1. **Platform-Specific Context:** The CVE references Apple iOS before version 9, indicating these vulnerabilities were identified and fixed in the context of mobile iOS devices. Camera Connect operates on Windows platforms in industrial environments.
2. **Unspecified Details:** The CVE notes "unspecified vulnerabilities" with "unknown impact and attack vectors," suggesting these may be vendor-specific issues in Apple's SQLite implementation or integration rather than core SQLite vulnerabilities.
3. **Mobile vs. Desktop:** iOS and desktop Windows environments have fundamentally different security models, application sandboxing, and attack surfaces.
4. **Apple-Specific Fixes:** These vulnerabilities were addressed in iOS 9 through Apple-specific patches, which may have included iOS-specific security hardening rather than core SQLite fixes.
5. **Limited Applicability:** Without specific attack vector information, and given the iOS-specific context, there is insufficient evidence that these vulnerabilities affect Camera Connect on Windows platforms.

The mobile platform-specific nature and lack of detailed vulnerability information make risk assessment and mitigation difficult, but the platform differences suggest limited applicability.

## CVE-2015-3717

Multiple buffer overflows in the printf functionality in SQLite, as used in Apple iOS before 8.4 and OS X before 10.10.4, allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors.

### CVSS

CVSS v3.1 Base Score: N/A  
CVSS v3.1 Temporal Score: N/A  
CVSS v3.1 Vector: N/A

CVSS v4.0 Score N/A  
CVSS v4.0 Vector: N/A

## CWE

CWE-120 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

## CVE

NVD Summary Link N/A

### Mitigating Factor

This vulnerability affects printf functionality in Apple platforms:

1. **Apple Platform Context:** The CVE specifically references Apple iOS and OS X implementations. Camera Connect runs on Windows operating systems, which may have different SQLite implementations and security controls.
2. **Printf Functionality:** The vulnerability is in printf functionality, which is internal string formatting. Camera Connect uses parameterized database queries and typed data operations, limiting exposure to format string vulnerabilities.
3. **Remote Attackers:** The CVE mentions "remote attackers," but Camera Connect operates in isolated ISA-95 Level 2 networks with no direct remote access from the internet.
4. **Apple-Specific Fixes:** The vulnerability was addressed through Apple platform-specific security updates, which may have included platform-specific protections not present in or needed for Windows deployments.
5. **String Handling:** Modern development practices in Camera Connect likely use safe string handling APIs and input validation that reduce exposure to buffer overflow conditions.

The Apple platform-specific nature of this CVE and Camera Connect's Windows deployment environment suggest limited cross-platform applicability.

## CVE-2015-3416

The `sqlite3VXPrintf` function in `printf.c` in SQLite before 3.8.9 does not properly handle precision and width values during floating-point conversions, which allows context-dependent attackers to cause a denial of service (integer overflow and stack-based buffer overflow) or possibly have unspecified other impact via large integers in a crafted printf function call in a SELECT statement.

### CVSS

CVSS v3.1 Base Score:	N/A
CVSS v3.1 Temporal Score:	N/A
CVSS v3.1 Vector:	N/A
CVSS v4.0 Score	N/A
CVSS v4.0 Vector:	N/A

### CWE

CWE-190 Integer Overflow or Wraparound

### CVE

NVD Summary Link N/A

### Mitigating Factor

This vulnerability involves printf-style formatting in SQL SELECT statements:

1. **Query Control:** The vulnerability requires crafting specific printf function calls with very large integer precision/width values within SELECT statements. Camera Connect's SQL queries are generated by the application code, not provided directly by untrusted users.
2. **Input Validation:** Any user inputs that influence query parameters undergo validation and sanitization before being incorporated into SQL statements, limiting the ability to inject malicious printf patterns.

3. **Parameterized Queries:** Camera Connect uses parameterized queries and prepared statements where possible, reducing exposure to SQL injection vectors that could be used to introduce malicious printf calls.
4. **Limited printf Usage:** The vulnerability specifically affects printf-style formatting functions in SQLite. Camera Connect's typical query patterns do not extensively use printf-style formatting operations.
5. **Stack Overflow Detection:** Modern compiler protections (stack canaries, ASLR) and operating system safeguards provide additional defense-in-depth against stack-based buffer overflow exploitation.

The controlled nature of SQL query generation in Camera Connect, combined with input validation and parameterized query usage, significantly reduces the practical exploitability of this vulnerability in production deployments.

## CVE-2015-3415

The `sqlite3VdbeExec` function in `vdbe.c` in SQLite before 3.8.9 does not properly implement comparison operators, which allows context-dependent attackers to cause a denial of service (invalid free operation) or possibly have unspecified other impact via a crafted `CHECK` clause, as demonstrated by `CHECK(0&O>O)` in a `CREATE TABLE` statement.

### CVSS

CVSS v3.1 Base Score: N/A  
CVSS v3.1 Temporal Score: N/A  
CVSS v3.1 Vector: N/A

CVSS v4.0 Score: N/A  
CVSS v4.0 Vector: N/A

### CWE

CWE-404: Improper Resource Shutdown or Release

### CVE

NVD Summary Link: N/A

### Mitigating Factor

This vulnerability involves malformed `CHECK` constraints that can trigger improper resource release behavior (CWE-404):

1. **CHECK Constraint:** The vulnerability requires a malformed `CHECK` constraint in a `CREATE TABLE` statement, such as `CHECK(0&O>O)`. `CHECK` constraints are part of database schema definition, not runtime queries.
2. **DDL Access Required:** Creating or modifying tables with `CHECK` constraints requires database administrative privileges and DDL access, which is not available to normal Camera Connect users.
3. **Schema Validation:** Camera Connect's database schema is established during installation and undergoes validation testing. Malformed `CHECK` constraints would be identified and corrected during development.

4. **Static Schema:** Camera Connect uses a predefined database schema that is not dynamically generated or modified during normal operation. New table creation does not occur during runtime.
5. **Development Detection:** The specific CHECK constraint pattern (bitwise operation in comparison) is clearly malformed and would be detected by code review and database testing procedures.
6. **DoS Containment:** Even if triggered, impact is typically process-level instability (invalid free/crash). OT deployments mitigate this with service monitoring, restart policies, and incident response procedures.

The requirement for schema-level modification access and the static nature of Camera Connect's database design effectively eliminate this vulnerability in deployed systems.

## Frequently asked questions

### What causes the vulnerability?

The vulnerabilities are caused by the use of SQLite version 3.2.4 in Camera Connect versions up to 2.0.0.42. The root causes vary and are presented in the CVEs in the previous section.

### What is the affected product or component?

The affected component is **SQLite version 3.2.4**, which is an embedded relational database engine used by Camera Connect versions up to 2.0.0.42.

### What might an attacker use the vulnerability to do?

The potential impacts vary depending on the specific CVE and each one of them are discussed in the previous sections however, it's important to note that the actual exploitability and impact are significantly reduced by Camera Connect's deployment in isolated OT networks with restricted access controls.

### How could an attacker exploit the vulnerability?

Exploitation methods vary by CVE but generally fall into these categories:

1. Database Query Manipulation (Most Common)
2. Database Schema Manipulation (Administrative Access Required)
3. Malformed Database Files
4. Extension-Specific Attacks

Exploitation Barriers in Camera Connect Deployments:

- No direct SQL query interface exposed to users
- Parameterized queries and input validation reduce injection risks
- Database administrative operations restricted to installation/upgrade processes
- Network segmentation limits attacker access to the system
- Authentication and authorization controls restrict unauthorized access

### **Could the vulnerability be exploited remotely?**

In properly configured Camera Connect deployments following industrial security best practices, remote exploitation is **highly unlikely**.

While the CVEs may reference remote exploitation, Camera Connect's architecture and typical OT deployment model make remote exploitation from outside the control network perimeter extremely difficult. The primary threat vectors are from malicious insiders or compromised systems already within the control network.

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

While exploitation of these vulnerabilities could degrade operational monitoring capabilities, properly designed industrial facilities maintain functional safety through independent, dedicated safety systems. Camera Connect should be considered an operational support tool rather than a safety-critical component. Organizations should ensure their safety management systems do not create dependencies on Camera Connect for safety-instrumented functions.

### **What does the update do?**

The update removes the vulnerability by providing a newer version of the affected component.

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

This vulnerability has been publicly disclosed for the 3<sup>rd</sup> party component, but not for the ABB product using this component

### **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.

## Support

For additional instructions and support please contact your local ABB service organization. For contact information, see [www.abb.com/contactcenters](http://www.abb.com/contactcenters).

Information about ABB's cyber security program and capabilities can be found at [www.abb.com/cyber-security](http://www.abb.com/cyber-security).

## Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	26/Mar/2026