DOCUMENT ID: SA25P007
VERSION: 1.1
DATE: 2026-02-18

CYBER SECURITY ADVISORY

B&R Automation Studio Update of SQLite version

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by B&R.

B&R 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 B&R 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 B&R or its suppliers have been advised of the possibility of such damages.

Purpose

B&R 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, B&R 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 B&R 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 B&R'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

B&R Automation Studio < 6.5

Vulnerability IDs

The following CVEs were disclosed at the time this advisory was issued. Please note that the list is subject to change at any time, as it concerns a third-party component.

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-2019-8457, 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

Summary

An update is available that replaces an outdated third-party component affected by publicly disclosed vulnerabilities in the product versions listed above.

Although **no successful exploitation was observed during testing of the affected B&R products**, the identified vulnerabilities could present potential attack vectors that might enable unauthorized access, data exposure, or remote code execution.

Recommended immediate actions

The problem is corrected in the following product versions:

B&R Automation Studio 6.5

B&R recommends that customers apply the update at earliest convenience.

The process to install updates is described in the user manual. The step to identify the installed product version is described in the user manual.

Vulnerability severity and details

An update is available that replaces an outdated third-party component affected by publicly disclosed vulnerabilities in the product versions listed above.

Although **no successful exploitation was observed during testing of the affected B&R products**, the identified vulnerabilities could present potential attack vectors that might enable unauthorized access, data exposure, or remote code execution. The following information refers exclusively to data officially published in the NVD and does not reflect the actual exploitability of these vulnerabilities in B&R components.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS)[1] for both v3.1[2] and v4.0[3].

The indicated Common Weakness Enumerations (CWE) have been selected from the MITRE CWE list[4].

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.

CVSS v3.1 Base 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

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

CWE: CWE-197 (Numeric Truncation Error)

---

[1] Common Vulnerability Scoring System (CVSS), Forum of Incident Response and Security Teams, Inc., https://www.first.org/cvss/.

[2] 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.

[3] 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.

[4] Common Weakness Enumeration (CWE), The MITRE Corporation, https://cwe.mitre.org/.

CVE-2025-3277

An integer overflow vulnerability exists in SQLite's concat_ws() function that can lead to a massive heap buffer overflow. When triggered, the integer overflow results in a truncated size value being used for buffer allocation, while the original untruncated size is used for writing the resulting string, causing a heap buffer overflow of approximately 4GB.

CVSS v3.1 Base 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

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

CWE: CWE-122 (Heap-based Buffer Overflow)

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 make alltest Handler. The manipulation leads to heap-based buffer overflow.

CVSS v3.1 Base Score: 7.3

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

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

CWE: CWE-122 (Heap-based Buffer Overflow)

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 v3.1 Base 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

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

CWE: CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer)

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 v3.1 Base 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

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

CWE: CWE-787 (Out-of-bounds Write)

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 v3.1 Base Score: 5.5

CVSS v3.1 Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

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

CWE: CWE-476 (NULL Pointer Dereference)

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 v3.1 Base 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

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

CWE: NVD-CWE-noinfo

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 v3.0 Base Score: 7.0

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

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

CWE: CWE-416 (Use After Free)

CVE-2020-13435

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

CVSS v3.1 Base 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

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

CWE: CWE-476 (NULL Pointer Dereference)

CVE-2020-13434

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

CVSS v3.0 Base Score: 5.5

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

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

CWE: CWE-190 (Integer Overflow or Wraparound)

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 v3.1 Base 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

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

CWE: CWE-416 (Use After Free)

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 v3.1 Base 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

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

CWE: CWE-754 (Improper Check for Unusual or Exceptional Conditions)

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 v3.1 Base 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

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

CWE: CWE-754 (Improper Check for Unusual or Exceptional Conditions)

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 v3.1 Base 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

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

CWE: CWE-674 (Uncontrolled Recursion)

CVE-2019-8457

SQLite3 from 3.6.0 to and including 3.27.2 is vulnerable to heap out-of-bound read in the rtreenode() function when handling invalid rtree tables.

CVSS v3.1 Base 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

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2019-8457

CWE: CWE-125 (Out-of-bounds Read)

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 v3.0 Base 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

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

CWE: CWE-190 (Integer Overflow or Wraparound)

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 v3.0 Base 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

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

CWE: CWE-20 (Improper Input Validation)

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 v3.0 Base 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

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

CWE: CWE-190 (Integer Overflow or Wraparound)

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 v3.0 Base 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

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

CWE: CWE-476 (NULL Pointer Dereference)

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 v3.0 Base 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

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

CWE: CWE-125 (Out-of-bounds Read)

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 v3.0 Base 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

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

CWE: CWE-20 (Improper Input Validation)

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 v3.0 Base Score: 3.7

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

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2015-6607

CWE: CWE-264 (Permissions, Privileges, and Access Control)

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 v3.1 Base 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

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2015-5895

CWE: NVD-CWE-noinfo (no detailed classification)

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 v3.0 Base 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

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2015-3717

CWE: CWE-120 (Classic Buffer Overflow)

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 v3.0 Base Score: 7.8

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

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2015-3416

CWE: CWE-190 (Integer Overflow or Wraparound)

Mitigating factors

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

General security recommendations

For any installation of software-related B&R 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 programing software to any network other than the network for the devices that it is intended for.
- Scan all data imported into your environment before use to detect potential malware infections.

- Minimize network exposure for all 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:

Defense in Depth for B&R products

Support

For additional instructions and support please contact your local B&R service organization. For contact information, see https://www.br-automation.com/en/about-us/locations/.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.

Version history

Rev. Ind.	Page (p) Chapter (c)	Change description	Version. date
1.0	all	Initial version	2026-02-18
1.1	-	Publication date	2026-02-18