DOCUMENT ID: SA25P004
VERSION: 1.0
DATE: 2026-01-19

CYBER SECURITY ADVISORY

Automation Studio
Insufficient Server Certificate Validation
CVE ID: CVE-2025-11043

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.

This document and parts hereof must not be reproduced or copied without written permission from B&R, 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

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

Automation Studio < 6.5

Vulnerability IDs

CVE-2025-11043

Summary

An update is available that resolves a vulnerability in the product versions listed above.

Successful exploitation of this vulnerability may enable an attacker to masquerade as a trusted party when B&R Automation Studio establishes a connection with a server via the ANSL over TLS or OPC-UA protocol.

Recommended immediate actions

The problem is corrected in the following product versions:

B&R Automation Studio version 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.

© Copyright 2026 B&R. All rights reserved.

Vulnerability severity and details

A vulnerability exists in the ANSL and OPC-UA clients included in the product versions listed above. An attacker could exploit a vulnerability by spoofing a trusted entity when Automation Studio is connecting to an ANSL or OPC-UA server.

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-2025-11043 Improper Server Certificate Validation in Automation Studio

An Improper Certificate Validation vulnerability in the OPC-UA client and ANSL over TLS client used in Automation Studio versions before 6.5 could allow an unauthenticated attacker on the network to position themselves to intercept and interfere with data exchanges.

CVSS

CVSS v3.1 Base Score:	7.4
CVSS v3.1 Temporal Score:	7.1
CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/RL:O/RC:C
CVSS v4.0 Score	9.1
CVSS v4.0 Vector:	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N

CWE

CWE-295: Improper Certificate Validation

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2025-11043

Mitigating factors

To exploit this vulnerability, an attacker would need to intercept and redirect the communication between B&R Automation Studio and the target server, as well as present manipulated certificates that

[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/.

© Copyright 2026 B&R. All rights reserved.

pass validation checks. B&R recommends operating B&R Automation Studio within Level 2 of the ABB ICS Cyber Security Reference Architecture when connecting to Level 1 devices via ANSL over TLS or OPC-UA. Operating in this trusted environment reduces the risk of successful exploitation drastically.

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

Frequently asked questions

What causes the vulnerability?

The vulnerability is caused by insufficient validation mechanisms for server certificates in the ANSL over TLS and OPC-UA client implementations.

What is B&R Automation Studio?

B&R Automation Studio is an environment for developing and executing automation solutions, ranging from control and motion technology to HMI, operation, and integrated safety technology.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could spoof a trusted server, potentially leading to the disclosure of confidential information or the alteration of data during transit.

How could an attacker exploit the vulnerability?

An attacker could attempt to exploit this vulnerability by generating a maliciously crafted server certificate and manipulating network routing or name resolution to redirect traffic through a compromised node under their control. This would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability. Recommended practices include that process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

What does the update do?

The update removes the vulnerability by modifying the way that the ANSL and OPC-UA clients are validating server certificates.

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

No, B&R discovered this vulnerability as a part of its own security analysis.

When this security advisory was issued, had B&R received any reports that this vulnerability was being exploited?

No, B&R had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued

© Copyright 2026 B&R. All rights reserved.

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	2026-01-19

© Copyright 2026 B&R. All rights reserved.