DOCUMENT ID: 3ADR011525
REVISION: A
DATE: 2026-02-24

CYBER SECURITY ADVISORY

ABB Automation Builder Gateway for Windows with insecure defaults

CVE ID: CVE-2024-41975

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

All Automation Builder versions prior to version 2.9.0 are affected by this vulnerability.

Vulnerability ID

CVE-2024-41975

Summary

ABB is aware of vulnerabilities in the product versions listed above.

The Windows gateway is accessible remotely by default. Unauthenticated attackers can therefore search for PLCs, but the user management of the PLCs prevents the actual access to the PLCs – unless it is disabled

Recommended immediate actions

If remote access is not required, check the "LocalAddress" setting in the [CmpGwCommDrvTcp] section of the Gateway's configuration file as follows (restart of gateway required in case of changes):

```
[CmpGwCommDrvTcp]
LocalAddress=127.0.0.1     ; allow access only from the local computer
```

The gateway configuration file can be located at (example for Automation Builder 2.8):
%ProgramFiles%\ABB\AB2.8\AutomationBuilder\GatewayPLC\Gateway.cfg

Starting with Automation Builder version 2.9.0 the vulnerability is closed by setting the default for the gateway to local access. Automation Builder 2.9.0 is available for download from the related download site.

Vulnerability severity and details

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-2024-41975: Gateway for Windows with insecure defaults

The gateway serves as a communication channel for various clients to AC500 PLCs. By default, the gateway listens on all available network adapters on port 1217 and can therefore be accessed remotely. However, remote access to the gateway is only required in certain network configurations. Since the gateway is usually accessed locally, many users are unaware of this remote access option, which can enable scanning of and access to restricted PLC networks. Unauthenticated attackers can therefore search for PLCs, but the user management of the PLCs prevents the actual access to the PLCs – unless it is disabled.

Please note that the gateway for Windows can be installed as a separate setup or as part of other setups such as the CODESYS Development System V3 setup or the CODESYS OPC DA Server setup.

CVSS

CVSS v3.1 Base Score:	5.3 (medium)
CVSS v3.1 Temporal Score:	4.9 (medium)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C
CVSS v4.0 Score	6.9 (medium)
CVSS v4.0 Vector:	AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

CWE

CWE-1188: Initialization of a Resource with an Insecure Default

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-41975

[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/.

Workarounds

Workarounds are specific measures that a user can take to help block an attack, for example, temporarily disabling the vulnerable feature may remove the exposure with well-known impact on functionality. ABB has tested the following workarounds. Although these workarounds will not correct the underlying vulnerability, they can help block known attack vectors. When a workaround reduces functionality, this is identified below as “Impact of workaround”.

The vulnerability can be closed by enabling local access only. See chapter “Recommended immediate actions” for details.

Frequently asked questions

What causes the vulnerability?

Refer to section “Vulnerability severity and details“.

What is the ABB Automation Builder?

The ABB Automation Builder is the programming and commissioning tool mainly for the ABB PLC AC500 and the operator panels CP600.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could scan for connected PLCs.

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 setting the defaults of the gateway to local access.

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

Yes, this vulnerability has been publicly disclosed.

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 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.

References

For the vulnerability an advisory from Codesys is available from the Codesys website:

- 2025-02: CODESYS (Edge) Gateway for Windows insecure default

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	2026-02-24