
CYBER SECURITY ADVISORY

AWIN Gateways Vulnerabilities in Embedded Webserver

CVE IDs:

CVE-2025-13777

CVE-2025-13778

CVE-2025-13779

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

Platform	Model number	ABB Product ID	Firmware Version
AWIN	AWIN GW100 rev.2	3BNP102988R1	2.0-0
			2.0-1
	AWIN GW120	3BNP103003R1	1.2-0
			1.2-1

Please Note. The subsequent document will refer to these models as AWIN gateways.

Vulnerability IDs

No	CVE ID	Title	Version Fixing the issue
1	CVE-2025-13777	Authentication Bypass due to Improper Session Validation	AWIN GW100 rev2: v2.1-0 AWIN GW120: v2.0-0
2	CVE-2025-13778	Device Reboot Control	AWIN GW100 rev2: v2.1-0 AWIN GW120: v2.0-0
3	CVE-2025-13779	Configuration Data Spill	AWIN GW100 rev2: v2.1-0 AWIN GW120: v2.0-0

Summary

ABB is aware of the vulnerabilities in the product versions listed above. An update is available that resolves the reported vulnerabilities in the product versions listed above.

AWIN gateways are not intended to be internet-facing.

An attacker who successfully exploited this vulnerability could take remote control of the product and reboot the device, potentially causing a denial of service. It can also reveal system specific configuration.

ABB requires, as noted in the User Manual, that AWIN gateways should not be exposed to the internet or any other insecure network.

Note. To exploit this vulnerability the attacker needs access to the AWIN gateways. These gateways are installed on sites which often have perimeter security, and the gateways are installed behind firewalls.

Recommended immediate actions

Do the following actions:

- Stop and disconnect any AWIN gateways that are exposed directly to the Internet.
- Ensure that physical controls are in place, so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.
- Ensure that all AWIN gateways are upgraded to the latest firmware version. Please find the latest version of firmware on the respective product Release Notes.
- When remote access is required, only use secure methods.

The problem is corrected in the following product versions:

- AWIN GW100 rev2: v2.1-0
- AWIN GW120: v2.0-0

ABB recommends that customers contact ABB to obtain the updated firmware as soon as possible. ABB Service Support engineer shall apply the firmware update at earliest convenience.

Vulnerability severity and details

Vulnerabilities exist in the AWIN gateways, included in the product versions listed above. An attacker could exploit the vulnerability by sending a specially crafted message to the system node, causing the node to stop or become inaccessible.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS)¹ for both v3.1² and v4.0³.

The indicated Common Weakness Enumerations (CWE) have been selected from the MITRE CWE list⁴.

CVE-2025-13777 - Authentication Bypass due to Improper Session Validation

An unauthenticated query reveals data. Authentication Bypass due to Improper Session Validation.

CVSS

CVSS v3.1 Base Score: 8.3 / High
CVSS v3.1 Temporal Score: 8.1 / High
CVSS v3.1 Vector: **CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H/E:F/RL:U/RC:C**

CVSS v4.0 Score: 7.2 / High
CVSS v4.0 Vector: **CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:H/SC:N/SI:N/SA:N**

CWE

CWE-294: Authentication Bypass by Capture-replay

CVE

NVD Summary Link: <https://nvd.nist.gov/vuln/detail/CVE-2025-13777>

CVE-2025-13778 – Device Reboot Control

An unauthenticated query allows an attacker to remotely reboot the device, potentially causing a denial of service.

CVSS

CVSS v3.1 Base Score: 6.5 / Medium
CVSS v3.1 Temporal Score: 6.4 / Medium
CVSS v3.1 Vector: **CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:F/RL:U/RC:C**

CVSS v4.0 Score: 7.1 / High
CVSS v4.0 Vector: **CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N**

CWE

CWE-306: Missing Authentication for Critical Function

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

NVD Summary Link: <https://nvd.nist.gov/vuln/detail/CVE-2025-13778>

CVE-2025-13779 - Configuration Data Spill

An unauthenticated query reveals the system configuration, including sensitive details.

CVSS

CVSS v3.1 Base Score: 8.3 / High
CVSS v3.1 Temporal Score: 8.1 / High
CVSS v3.1 Vector: **CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H/E:F/RL:U/RC:C**

CVSS v4.0 Score: 7.2 / High
CVSS v4.0 Vector: **CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:H/SC:N/SI:N/SA:N**

CWE

CWE-306: Missing Authentication for Critical Function

CVE

NVD Summary Link: <https://nvd.nist.gov/vuln/detail/CVE-2025-13779>

Mitigating factors

AWIN gateways are NOT internet facing devices and should be installed behind firewalls.

These gateways are intended to be located between level 0 (process) and level 1 (basic control) hierarchy of the IEC 62443 reference model.

Ensure that physical controls are in place, so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.

Update the firmware on the gateways with the newer versions with the fix.

At the time of writing the following versions are latest:

- AWIN GW100 rev2: v2.1-0
- AWIN GW120: v2.0-0

Refer to the Release Notes and Product Bulletins for up-to-date information on the latest firmware releases.

Frequently asked questions

What causes vulnerability?

Authentication Bypass due to Improper Session Validation.

What are AWIN Gateways?

They are WirelessHART gateways. They are intended to be located between level 0 (process) and level 1 (basic control) hierarchy of the IEC 62443 reference model. They collect sensor data and provide this information to the host systems.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability can render the WirelessHART network unavailable.

How could an attacker exploit the vulnerability?

An attacker will have to first connect to the same local network where the gateway is present. This vulnerability can be exploited by sending a crafted HTTP GET request using a previously observed or valid time parameter value, regardless of the password used during the initial login attempt.

Could the vulnerability be exploited remotely?

No. Remote access is disabled in the gateways.

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

This product is not intended to be used in functional safety applications.

What does the update do?

It enforces HTTPS access. Unauthenticated requests are explicitly denied. Configuration data is not exposed anymore.

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

No, ABB received information about this vulnerability through responsible disclosure.

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.

More information on recommended practices can be found in the documents listed in the References section.

Acknowledgement

ABB acknowledges and thanks **Fred Alvarez** for responsibly disclosing the vulnerabilities and providing valuable input on product improvements.

References

- [3BNP102992](#) AWIN GW100 User Manual
- [4JNO000308](#) AWIN GW120 User Manual

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/cyber-security.

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	11-03-2026