DOCUMENT ID: 3ADR011432
REVISION: A
DATE: 2025-07-23

CYBER SECURITY ADVISORY

# AC500 V2
# Buffer overread on Modbus protocol
CVE ID: CVE-2025-7745

## 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.

# 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 AC500 V2 PLCs with firmware version 2.5.2 or earlier are affected by this vulnerability.

# Vulnerability IDs

CVE-2025-7745

# Summary

ABB is aware of public reports of a vulnerability in the product versions listed above.

An attacker who successfully exploited this vulnerability could access fragments of Modbus telegrams that have been sent earlier by that PLC.

# Recommended immediate actions

The problem is corrected in the following product versions:

AC500 V2 firmware version 2.5.3 (released in 2016) and later.

ABB recommends that customers apply the update based on a review of the risks coming from this vulnerability.

# Vulnerability severity and details

A vulnerability exists in the Modbus TCP server functionality included in the product versions listed above. An attacker could exploit the vulnerability by calling an unsupported Modbus function code, causing the PLC answer by an invalid telegram.

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-2025-7745: Modbus TCP buffer overread

Sending unsupported function codes to the AC500 V2 Modbus server might result in invalid responses. Fragments of previous responses might be added to the end of the response.

**CVSS**

| | |
|---|---|
| CVSS v3.1 Base Score: | 5.8 (Medium) |
| CVSS v3.1 Temporal Score: | 5.6 (Medium) |
| CVSS v3.1 Vector: | AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N |
| | |
| CVSS v4.0 Score | 6.9 (Medium) |
| CVSS v4.0 Vector: | AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:L/SA:H |

**CWE**

CWE-126: Buffer Over-read

**CVE**

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2025-7745

[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/.

# Mitigating factors

Mitigating factors describe conditions and circumstances that make an attack that exploits the vulnerability difficult or less likely to succeed.

Regarding this vulnerability it is recommended to

- Do not use the Modbus server for sending any sensitive data, as fragments might be accessible even after the initial sending of the response.
- Only use supported Modbus function codes, as invalid responses to unsupported function codes might have negative effects on the requesting Modbus client.

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 requesting an unsupported function code from the Modbus server of the PLC.

### What is AC500 V2?

The AC500 V2 is a scalable range of Programmable Logic Controller (PLC). It provides solutions for small, medium and high-end applications. The AC500 V2 platform offers different performance levels and is a good choice for high availability, extreme environments, condition monitoring, motion control or safety solutions. It offers interoperability and compatibility in hardware and software from compact PLCs up to high end and safety PLCs.

AC500 V2 compact PLCs are already in the classic phase.

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

An attacker who successfully exploited this vulnerability could access fragments of Modbus telegrams that have been sent earlier by that PLC.

### How could an attacker exploit the vulnerability?

Refer to section “Vulnerability severity and details“.

### 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 unsupported Modbus function codes are processed. No additional buffer data will be sent.

### 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 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.

## Acknowledgement

ABB acknowledges and extends gratitude to Reid Wightman of Dragos, Inc for responsibly disclosing the vulnerability and providing valuable input on product improvements.

## 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 | 2025-07-23 |
| | | | |
| | | | |