DOCUMENT ID: 3ADR011377
REVISION: A
DATE: 2025-01-07

CYBER SECURITY ADVISORY

AC500 V3
Multiple vulnerabilities

CVE IDs: CVE-2023-6357, CVE-2024-5000, CVE-2024-8175, CVE-2024-12429, CVE-2024-12430

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 V3 products (PM5xxx) with firmware version earlier than 3.8.0 are affected by these vulnerabilities.

Vulnerability IDs

CVE-2023-6357, CVE-2024-5000, CVE-2024-8175, CVE-2024-12429, CVE-2024-12430

Summary

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

An attacker who successfully exploited these vulnerabilities could call shell functions (CVE-2023-6357), crash the PLC (CVE-2024-5000), crash the web server of the PLC (CVE-2024-8175), grant read access to files (CVE-2024-12429) or enable command execution (CVE-2024-12430).

The vulnerabilities CVE-2023-6357, CVE-2024-12429 and CVE-2024-12430 require successful authentication.

Recommended immediate actions

The problem is corrected in the following product versions:

AC500 V3 firmware version 3.8.0

ABB recommends that customers apply the update at earliest convenience. This firmware version is released for all AC500 V3 PLC types and available from Automation Builder 2.8.0. Automation Builder 2.8.0 is available for download from the related download site.

Vulnerability severity and details

Multiple vulnerabilities exist in the AC500 V3 included in the product versions listed above. For details, please refer to the subchapters for the different CVEs.

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-2023-6357: Improper Neutralization of Special Elements used in an OS Command

A successfully authenticated control programmer could exploit this vulnerability to inject calls to additional operating system shell functions via the SysFile or CAA file system libraries.

CVSS

CVSS v3.1 Base Score:	8.8 (High)
CVSS v3.1 Vector:	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CWE

CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

CVE

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2023-6357

[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-2024-5000: Incorrect Calculation of Buffer Size

The OPC UA stack, implemented by the CmpOPCUAStack component, is an optional part of the runtime system. Both the OPC UA Server and the OPC UA Client of the runtime system use the OPC UA Stack as a common implementation. The OPC UA protocol enables data exchange between the runtime system and OPC UA clients such as SCADA or HMIs, or OPC UA servers such as PLCs or other devices.

If a runtime system containing the CmpOPCUAStack component receives a specially crafted request/response, the required buffer size in the OPC UA server/client may be incorrectly calculated. This can lead to a crash of the runtime system during the subsequent initialization of the receive buffer with zero.

An attacker can exploit this vulnerability by using a malicious OPC UA client to send a crafted request to the AC500 V3 PLC with an affected OPC UA server. Conversely, AC500 V3 PLCs with an affected OPC UA client can be crashed if they have connected to a malicious OPC UA server. The runtime systems usually contain both the OPC UA client and the server.

CVSS

CVSS v3.1 Base Score: 8.8 (High)
CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CWE
CWE-131: Incorrect Calculation of Buffer Size

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-5000

CVE-2024-8175: Improper Check for Unusual or Exceptional Conditions

The AC500 V3 web server, implemented by the CmpWebServer component, is an optional part of the runtime system. It is used by the AC500 V3 WebVisu to display visualization screens in a web browser. The AC500 V3 web server supports both the HTTP and HTTPS protocols. Because the AC500 V3 web server does not correctly check the return value of an underlying function, it reacts in a wrong way to specifically crafted TLS packets that are received via an HTTPS connection. This causes the AC500 V3 web server to access invalid memory and the web server task to crash.

CVSS

CVSS v3.1 Base Score: 7.5 (High)
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

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

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-8175

CVE-2024-12429: Directory traversal

AC500 V3 PLC has a slot for memory cards that can be used e.g. for logging purposes or for updating the firmware or the boot application. Because the AC500 V3 does not correctly validate the content of the memory card, a specifically crafted memory card can be used for directory traversal. A successfully authenticated attacker can use this vulnerability to read system-wide files and configuration.

CVSS

CVSS v3.1 Base Score:	4.3 (Medium)
CVSS v3.1 Vector:	AV:P/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
CVSS v4.0 Score	5.1 (Medium)
CVSS v4.0 Vector:	AV:P/AC:L/AT:N/PR:N/UI:P/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

CWE
CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-12429

CVE-2024-12430: Privilege escalation

After successfully exploiting CVE-2024-12429 (directory traversal), a successfully authenticated attacker can inject arbitrary commands into a specifically crafted file, which then will be executed by root user.

CVSS

CVSS v3.1 Base Score:	7.0 (High)
CVSS v3.1 Vector:	AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Score	7.3 (High)
CVSS v4.0 Vector:	AV:L/AC:H/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CWE
CWE-280: Improper Handling of Insufficient Permissions or Privileges

CVE
NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-12430

Mitigating factors

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

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”.

To exploit the vulnerabilities CVE-2023-6357, CVE-2024-12429 and CVE-2024-12430, successful authentication is required. Therefore, the affected products shall only be used with activated user management and by setting strong passwords. Details regarding the device user management are available from the application note “AC500 User Management with V3”.

ABB strongly recommends using the online user management. This not only prevents an attacker from downloading and execute malicious code, but also suppresses start, stop, debug, or other actions on a known working application that could potentially disrupt a machine or system.

Frequently asked questions

What causes the vulnerability?

Refer to section “Vulnerability severity and details“.

What is AC500 V3?

The AC500 V3 is a scalable range of Programmable Logic Controller (PLC). It provides solutions for small, medium and high-end applications. The AC500 V3 platform offers different performance levels and is the ideal 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.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited these vulnerabilities could call shell functions (CVE-2023-6357), crash the PLC (CVE-2024-5000), crash the web server of the PLC (CVE-2024-8175), grant read access to files (CVE-2024-12429) or enable command execution (CVE-2024-12430).

How could an attacker exploit the vulnerability?

Refer to section “Vulnerability severity and details“.

Could the vulnerability be exploited remotely?

CVE-2023-6357, CVE-2024-5000, CVE-2024-8175:
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.

CVE-2024-12429, CVE-2024-12430:
No, to exploit this vulnerability an attacker would need to have physical access to an affected system node.

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

CVE-2023-6357, CVE-2024-5000, CVE-2024-8175:
Yes, this vulnerability has been publicly disclosed.

CVE-2024-12429, CVE-2024-12430:
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

For CVE-2024-12429 and CVE-2024-12430 ABB acknowledges and extends gratitude to D. Blagojevic, S. Dietz and T. Weber of CyberDanube for responsibly disclosing the vulnerability and providing valuable input on product improvements.

References

For the following vulnerabilities advisories from Codesys are available from the Codesys website:

- CVE-2023-6357: CODESYS Control V3 on Linux and QNX operating systems
- CVE-2024-5000: CODESYS Control V3 - OPC UA Stack
- CVE-2024-8175: CODESYS Control V3 web server

Application note: AC500 User Management with V3

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	2025-01-07