DOCUMENT ID: 3ADR0111162
REVISION: A
DATE: 2023-03-28

CYBER SECURITY ADVISORY

AC500 V2
Cyber Security Advisory

CVE-2021-34595, CVE-2022-1965, CVE-2022-3192, CVE-2022-31805, CVE-2022-32136, CVE-2022-32137, CVE-2022-32138, CVE-2022-32139, CVE-2022-32140, CVE-2022-32141, CVE-2022-32142, CVE-2022-32143

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 AC500 V2 products with firmware version smaller than 2.8.6 are affected by this vulnerability.

Vulnerability IDs

- CVE-2021-34595
- CVE-2022-1965
- CVE-2022-3192
- CVE-2022-31805
- CVE-2022-32136
- CVE-2022-32137
- CVE-2022-32138
- CVE-2022-32139
- CVE-2022-32140
- CVE-2022-32141
- CVE-2022-32142
- CVE-2022-32143

Summary

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

An attacker who successfully exploited this vulnerability could cause a denial-of-service condition or local memory overwrite, e.g. of files.

Recommended immediate actions

ABB has developed a new firmware version 2.8.6 fixing these vulnerabilities except CVE-2022-31805. This firmware version is released for all AC500 V2 PLC types. It is available from Automation Builder 2.6.0 and there is also a memory card image available for download from our website.

All affected products shall be used only as described in the manual in the chapter "Cyber security in AC500 V2 products" especially regarding defense in depth and secure operation. The manual is available from our website for download (Manual for PLC Automation with AC500 V2 and Automation Builder 2.6.0).

General information about secure operation of the AC500 products is available from our white paper "Cyber Security in the AC500 PLC family".

Vulnerability severity and details

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1[1].

CVE-2021-34595: CWE-823: Use of Out-of-range Pointer Offset

A crafted request with invalid offsets may cause an out-of-bounds read or write access in the affected products, resulting in a denial-of-service condition or local memory overwrite.

CVSS v3.1 Base Score:	8.1 (High)
CVSS v3.1 Vector:	AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

CVE-2022-1965: CWE-755: Improper Handling of Exceptional Conditions

An invalid crafted request is not properly processed by the error handling of the affected products. As a result, the file referenced by the malicious request could be deleted if it exists on the controller.

CVSS v3.1 Base Score:	6.5 (Low)
CVSS v3.1 Vector:	AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVE-2022-3192: CWE-754: Improper Check for Unusual or Exceptional Conditions

An invalid crafted request is not properly processed by the error handling of the affected products, resulting in a denial-of-service condition on port 1200.

CVSS v3.1 Base Score:	5.3 (Medium)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

[1] 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.

CVE-2022-31805: CWE-523: Unprotected Transport of Credentials

The passwords between the communication clients and servers among the affected products are transmitted unprotected. This allows attackers to guess passwords if they are able to sniff the communication.

CVSS v3.1 Base Score:	9.8 (Critical)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE-2022-32136: CWE-824: Access of Uninitialized Pointer

A crafted request may cause an internal read access to an uninitialized pointer in the affected products, resulting in a denial-of-service condition.

CVSS v3.1 Base Score:	6.5 (Medium)
CVSS v3.1 Vector:	AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVE-2022-32137: CWE-122: Heap-based Buffer Overflow

A crafted request may cause a heap-based buffer overflow in the affected products, resulting in a denial-of-service condition or memory overwrite.

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

CVE-2022-32138: CWE-194: Unexpected Sign Extension

A crafted request with may cause an unexpected sign extension in the affected products, resulting in a denial-of-service condition or memory overwrite.

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

CVE-2022-32139: CWE-125: Out-of-bounds Read

A crafted request may cause an internal out-of-bounds read in the affected products, resulting in a denial-of-service condition.

CVSS v3.1 Base Score:	6.5 (Medium)
CVSS v3.1 Vector:	AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVE-2022-32140: CWE-130: Improper Handling of Length Parameter Inconsistency

A crafted request may contain an incorrect data length for the associated structured data of the request. Since the affected products do not handle the length correctly, this can lead to an internal buffer over-read causing a denial-of-service condition.

CVSS v3.1 Base Score:	6.5 (Medium)
CVSS v3.1 Vector:	AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVE-2022-32141: CWE-126: Buffer Over-read

A crafted request with invalid offsets may cause an internal buffer over-read in the affected products, resulting in a denial-of-service condition.

CVSS v3.1 Base Score:	6.5 (Medium)
CVSS v3.1 Vector:	AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVE-2022-32142: CWE-823: Use of Out-of-range Pointer Offset

A crafted request with invalid offsets may cause an internal out-of-bounds read or write access in the affected products, resulting in a denial-of-service condition or local memory overwrite.

CVSS v3.1 Base Score:	8.1 (High)
CVSS v3.1 Vector:	AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

CVE-2022-32143: CWE-552: Files or Directories Accessible to External Parties

The AC500 V2 file download and upload function also allows read and potentially write access to internal files in the working directory, e.g. firmware files of the PLC, since no filtering is performed.

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

Mitigating factors

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

Workarounds

ABB recommends using the available software update that fixes all vulnerabilities except CVE-2022-31805.

To exploit the vulnerabilities CVE-2021-34595, CVE-2022-1965, CVE-2022-32136, CVE-2022-32137, CVE-2022-32138, CVE-2022-32139, CVE-2022-32140, CVE-2022-32141, CVE-2022-32142 and CVE-2022-32143, a successful login to the affected product is required. A configured PLC password for password level 1 therefore protects against the exploitation of these vulnerabilities even in case the software update could not be applied.

To exploit the vulnerability CVE-2022-31805 network access is required to connect to the PLC. As a workaround this access have to be limited e.g. by separating this network them from any general purpose network (e.g. office or home networks).

There is no workarounds for CVE-2022-3192. But CVE-2022-3192 only affects the "ABB Tcp/Ip Level 2 AC” protocol on port 1200. Replacing this protocol by the “Tcp/Ip” protocol uses port 1201 instead of port 1200. Therefore a denial-of-service condition on port 1200 has no effect on the “Tcp/Ip” protocol”.

Frequently asked questions

What causes the vulnerability?

Refer to section “Vulnerability severity and details“

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause a denial-of-service condition or local memory overwrite, e.g. of files. For further details, please refer to section “Vulnerability severity and details“.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected system node. 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.

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

The vulnerabilities CVE-2021-34595, CVE-2022-1965, CVE-2022-31805, CVE-2022-32136, CVE-2022-32137, CVE-2022-32138, CVE-2022-32139, CVE-2022-32140, CVE-2022-32141, CVE-2022-32142 and CVE-2022-32143 have been publicly disclosed.

The vulnerability CVE-2022-3192 has not 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.

More information on recommended practices can be found in the white paper Cyber Security in the AC500 PLC family.

Acknowledgements

ABB thanks the following for working with us to help protect customers:

- CVE-2022-3192:
  Parul Sindhwad and Dr. Faruk Kazi of CoE CNDS lab, VJTI, Mumbai (India) for reporting this vulnerability following coordinated disclosure.

References

Codesys advisories are available

- for the vulnerabilities CVE-2022-1965, CVE-2022-32136, CVE-2022-32137, CVE-2022-32138, CVE-2022-32139, CVE-2022-32140, CVE-2022-32141, CVE-2022-32142 and CVE-2022-32143: Security update for CODESYS Control V2
- For the vulnerability CVE-2022-31805: Security update for CODESYS V2 password transport
- For the vulnerability CVE-2021-34595: Security update for CODESYS Control V2

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	2023-03-28