DOCUMENT ID: 9AKK108470A9491
REVISION: B
DATE: 2025-03-27

CYBER SECURITY ADVISORY

ABB ACS880 +N8010 Drives CODESYS RTS Vulnerabilities

CVE ID: CVE-2023-37559, CVE-2023-37558, CVE-2023-37557, CVE-2023-37556, CVE-2023-37555, CVE-2023-37554, CVE-2023-37553, CVE-2023-37552, CVE-2023-37550, CVE-2023-37549, CVE-2023-37548, CVE-2023-37547, CVE-2023-37546, CVE-2023-37545, CVE-2022-4046

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

ACS880 Drives with +N8010 license are affected by the vulnerabilities mentioned in this document. All applications with +N8010 license based on ACS880 Primary Control Program before AINLX V3.47 are affected.

Exploitation of these vulnerabilities is only possible if an IEC 61131-3 programming license (+N8010) is provisioned to the memory unit.

Beside following listed products, any drive modules, or any separate control unit for drive modules, with +N8010 code labeled at device memory unit are affected as well.

Product Short Type Code	Product Name	Affected Versions
ACS880-xx+N8010	ACS880 Primary Control Program	AINLX prior to v3.47 YINLX prior to v1.30
ACS880-xx+N8010	ACS880 IGBT Supply Control Program	AISLX prior to v3.43 ALHLX prior to v3.43 YISLX prior to v1.30 YLHLX prior to v1.30
ACS880-xx+N5700	ACS880 Position Control Program	APCLX up to (including) v1.04.0.5
ACS880-xx+N5300 +N8010	ACS880 Test Bench Control Program	ATBLX up to (including) v3.44.0.0

Vulnerability IDs

CVE-2023-37559, CVE-2023-37558, CVE-2023-37557, CVE-2023-37556, CVE-2023-37555, CVE-2023-37554, CVE-2023-37553, CVE-2023-37552, CVE-2023-37550, CVE-2023-37549, CVE-2023-37548, CVE-2023-37547, CVE-2023-37546, CVE-2023-37545, CVE-2022-4046

Summary

Multiple vulnerabilities regarding the CODESYS Runtime System from CODESYS Group have been publicly reported. [1][2]CODESYS Runtime System is utilized in the firmware of ABB ACS880 drives to provide IEC 61131-3 programming capabilities.

These vulnerabilities could lead to out-of-bound memory access. Successful exploit may result in a denial-of-service condition or arbitrary code execution.
Firmware updates are available that mitigate the publicly reported vulnerabilities of the products listed above.

Recommended immediate actions

In latest firmware versions for the affected products, ABB has mitigated the CODESYS Runtime System vulnerabilities. IEC online programming communication is disabled by default. As a result, CODESYS tools communication with the drive is disabled.

ABB recommends that customers apply the firmware update at earliest convenience.

For situations where firmware update is not feasible, please refer to *'Workarounds'* section guidance.

Vulnerability severity and details

Vulnerabilities exist in the CODESYS Runtime component included in the product versions listed above. An attacker could exploit the vulnerability by sending a specially crafted message to the system, causing ABB ACS880 Drives to stop or become inaccessible, allowing the attacker to take control of the product as well as insert and run arbitrary code.

The following vulnerabilities publicly reported by CODESYS Group affect ABB ACS880 Drives.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS)[1] v3.1[2].

The indicated Common Weakness Enumerations (CWE) have been selected from the MITRE CWE list[3].

---

[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] Common Weakness Enumeration (CWE), The MITRE Corporation, https://cwe.mitre.org/.

CVE-2023-37559, CVE-2023-37558: CODESYS Improper Validation of Consistency within Input in multiple products

After successful authentication as a user in multiple CODESYS products in multiple versions, specific crafted network communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition.

(in NIST NVD, these CVEs are explicitly mentioned different from each other, but with same vulnerability description, CWE, CVSS etc.)

CVSS

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

CWE
CWE-20: Improper Input Validation

CVE
NVD Summary Link:
https://nvd.nist.gov/vuln/detail/CVE-2023-37559
https://nvd.nist.gov/vuln/detail/CVE-2023-37558

CVE-2023-37557 CODESYS Heap-based Buffer Overflow in multiple products

After successful authentication as a user in multiple CODESYS products in multiple versions, specific crafted remote communication requests can cause the CmpAppBP component to overwrite a heap-based buffer, which can lead to a denial-of-service condition.

CVSS

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

CWE

CWE-787: Out-of-bounds Write

CVE
NVD Summary Link:
https://nvd.nist.gov/vuln/detail/CVE-2023-37557

CVE-2023-37556, CVE-2023-37555, CVE-2023-37554, CVE-2023-37553, CVE-2023-37552, CODESYS Improper Input Validation in CmpAppBP

In multiple versions of multiple CODESYS products, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition.

(in NIST NVD, these CVEs are explicitly mentioned different from each other, but with same vulnerability description, CWE, CVSS etc.)

CVSS

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

CWE
CWE-20: Improper Input Validation

CVE
NVD Summary Link:
https://nvd.nist.gov/vuln/detail/CVE-2023-37556
https://nvd.nist.gov/vuln/detail/CVE-2023-37555
https://nvd.nist.gov/vuln/detail/CVE-2023-37554
https://nvd.nist.gov/vuln/detail/CVE-2023-37553
https://nvd.nist.gov/vuln/detail/CVE-2023-37552

CVE-2023-37550, CVE-2023-37549, CVE-2023-37548, CVE-2023-37547, CVE-2023-37546, CVE-2023-37545 CODESYS: Improper Input Validation in CmpApp component

In multiple CODESYS products in multiple versions, after successful authentication as a user, specific crafted network communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition.

CVSS

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

CWE
CWE-20: Improper Input Validation

CVE
NVD Summary Link:
https://nvd.nist.gov/vuln/detail/CVE-2023-37550
https://nvd.nist.gov/vuln/detail/CVE-2023-37549
https://nvd.nist.gov/vuln/detail/CVE-2023-37548
https://nvd.nist.gov/vuln/detail/CVE-2023-37547
https://nvd.nist.gov/vuln/detail/CVE-2023-37546
https://nvd.nist.gov/vuln/detail/CVE-2023-37545

CVE-2022-4046 CODESYS: Improper memory restrictions for CODESYS Control

In CODESYS Control in multiple versions a improper restriction of operations within the bounds of a memory buffer allow an remote attacker with user privileges to gain full access of the device.

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-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

CVE
NVD Summary Link:
https://nvd.nist.gov/vuln/detail/CVE-2022-4046

Mitigating factors

Network communication between attacker and drives is needed to exploit the vulnerabilities. Thus, network isolation or protection will make the attack difficult and less likely to succeed.

Please refer to ‘General security recommendations for further advise on how to keep your system secure.

Workarounds

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”.

For situations where firmware update is not feasible, ABB recommends mitigating the threat by setting following parameters:

For IGBT supply control program devices:

set parameter 196.102 to bit 2 to disable file download (for further bit description, please refer to drive firmware manual [7])

For other devices:

set parameter 96.102 to bit 2 to disable file download (for further bit description, please refer to drive firmware manuals [3] [4]).

Impact of workaround:

This workaround restricts IEC programs update, but existing IEC programs in Drives can still be used. To update an IEC program, the operator has to unlock the user lock and enable file download in a protected network environment.

It is strongly recommended to disable file download. The vulnerabilities are exploitable when file download is enabled.

Warning! – The user lock cannot be opened even by ABB if the pass code is lost.

Frequently asked questions

What causes the vulnerability?

The vulnerabilities are caused by improper input validation, improper restriction of memory operations in the CODESYS Runtime System inside ABB ACS880 Drives.

What is ABB ACS880 Drive?

A drive is an electronic device used to regulate the performance of an electric motor. It works by controlling the power, frequency and current the motor draws from the grid. Drive is also referred to as a variable-speed motor drive. The basic function of a drive is to control the flow of energy from the mains to the process.[5] [6]

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause a denial-of-service condition, memory overwriting, or remote code execution.

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. Recommended practices help mitigate such attacks, see 'Mitigating Factors' section 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.

What does the update do?

In the latest firmware versions for the affected products, ABB has addressed the vulnerability by disabling IEC online programming communication by default. As a result, CODESYS tools communication with the drive is disabled.

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

Yes, this vulnerability has been publicly disclosed. Please refer to '*References' section.*

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 only authorized personnel can access your devices, components, peripheral equipment, and networks.
- Never connect programming software tools or computers containing programming software to any network other than the network where run 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 it.
- 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

[1] CODESYS Security Advisory 2023-04

[2] CODESYS Security Advisory 2023-05

[3] ACS880 primary control program (YINLX) Firmware manual

[4] ACS880 primary control program (AINLX) Firmware manual

[5] https://global.abb/group/en/media/resources/glossary

[6] https://new.abb.com/drives/what-is-a-variable-speed-drive

[7] ACS880 IGBT supply control program (YISLX and YLHLX) firmware 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/cybersecurity.

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	2025-03-26
B	all	Document ID update	2025-03-27