DOCUMENT ID: 9AKK108470A9494
REVISION: B
DATE: 2025-03-27

CYBER SECURITY ADVISORY

Low Voltage DC Drives and Power Controllers 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.

© Copyright 2025 ABB. All rights reserved.

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 ABB low-voltage DC drive and power controller products (DCS880, DCS880 H2, DCT880 and DCS580) contain a vulnerable version of the CODESYS Runtime. Exploitation, of those vulnerabilities, however, is only possible if an IEC 61131-3 license is provisioned to the memory unit.

To check if your system is affected you can check the id number of the memory unit. The memory units in the following table contain affected IDs.

Description	ID
DCT880 memory unit incl. ABB Drive Application Builder license (IEC 61131-3)	3ADT786242R0101
DCT880 memory unit incl. Power Optimizer	3ADT786242R0201
DCS880 memory unit incl. ABB Drive Application Builder license (IEC 61131-3)	3ADT786251R0101
DCS880 memory unit incl. DEMag	3ADT786251R0201
DCS880 memory unit incl. DCC	3ADT786251R0401

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

© Copyright 2025 ABB. All rights reserved.

Summary

CODESYS group published several vulnerabilities regarding the CODESYS Runtime System, which is included in the firmware of ABB LV DC drives and power controllers. It is used to implement a selection of features and to provide IEC 611131-3 programming capabilities.

These vulnerabilities include memory corruption issues that could lead to out-of-bound memory access. Subsequently, a successful exploit could allow attackers to trigger a denial-of-service condition or execute arbitrary code over the fieldbus interfaces. Exploiting these vulnerabilities requires an IEC 61131-3 license being present on the memory unit of the drive or power controller.

Recommended immediate actions

If the drive or power controller is in an exploitable configuration, ABB recommends immediately applying the mitigations described in the *Workarounds* section.

Vulnerability severity and details

The following information has been taken directly from the corresponding security advisories by the CODESYS group. They are listed in the *References* section for further details.

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].

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

---

[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/.

© Copyright 2025 ABB. All rights reserved.

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

© Copyright 2025 ABB. All rights reserved.

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

The vulnerabilities only pose a threat if an IEC 61131-3 license is provisioned to the memory unit.

The exploitation can be triggered via USB on the panel or via fieldbus or Ethernet using a fieldbus connector. If none of these are connected exploitation is not possible. For network based attacks the attacker needs to be able to reach the drive or power controller via the network.

© Copyright 2025 ABB. All rights reserved.

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*.

Activate User Lock and disable file upload

To mitigate the exploitability of the vulnerabilities ABB recommends disabling the upload of firmware, including IEC 61131-3 programs to the drive or power controller. Additionally, it is recommended to close the User Lock and enable the Parameter Lock, so an attacker is not able to unblock the firmware upload over fieldbus.

The settings can be applied via the Drive Composer tool. For the user lock to be effective and the parameter lock bound to the user lock, the following steps need to be performed:

DCS880

- Enter the default user pass code 10000000 in 96.07 Pass code
- Change the default user pass code to a **random** number using 96.100 Change user pass code and 96.101 Confirm user pass code
- In 96.102 User lock functionality set bits 0, 2, 3 and 6 to 1 (high)
  - Bit 0: Disable ABB access levels
  - Bit 2: Disable file download
  - Bit 3: Disable Fieldbus write to hidden parameters
  - Bit 6: Protect AP
- Enter any invalid pass code in 96.07 Pass code to close the lock
- To enable the parameter lock set 96.07 Pass code = 358
  - In 96.04 Access Levels Active Bit 14 (parameter lock) is set
- Enter your user pass code in 96.07 Pass code to open the lock
- In 96.102 User lock functionality set bit 1 to 1 (high) to freeze the parameter lock state
- Enter any invalid pass code in 96.07 Pass code to close the lock

DCT880

- Enter the default user pass code 10000000 in 96.02 Pass code
- Change the default user pass code to a **random** number using 96.100 Change user pass code and 96.101 Confirm user pass code
- In 96.102 User lock functionality set bits 0, 2, 3 and 6 to 1 (high)
  - Bit 0: Disable ABB access levels
  - Bit 2: Disable file download
  - Bit 3: Disable Fieldbus write to hidden parameters
  - Bit 6: Protect AP

© Copyright 2025 ABB. All rights reserved.

- Enter any invalid pass code in 96.02 Pass code to close the lock
- To enable the parameter lock set 96.02 Pass code = 358
  - In 96.03 Access Levels Active Bit 14 (parameter lock) is set
- Enter your user pass code in 96.02 Pass code to open the lock
- In 96.102 User lock functionality set bit 1 to 1 (high) to freeze the parameter lock state
- Enter any invalid pass code in 96.02 Pass code to close the lock

Verification

Please be aware: If those steps are not performed in the correct order, the pass code might be circumvented. Setting the correct User Lock Functionality bits is not enough to secure the device. Please make sure the lock is closed (parameters 96.100 to 96.102 not visible).

If the User Lock is open, warning 1236 is set.

Impact of the workaround

After applying the workaround, the IEC 61131-3 programs can be used, but not uploaded to the drive anymore. To upload an IEC program the operator has to unlock the User Lock and disable the File Upload Lock.

If the parameter lock is applied no parameter of the drive can be changed. To change the parameter the operator has to unlock the User Lock and disable the parameter lock.

The disablement of the file downloads includes

- Firmware uploads
- Safety functions module FSO-21 configuration
- Parameter restore to default values. See parameter 96.15 for details.
- Loading of adaptive programs
- Loading and debugging application programs via Drive application builder
- Changing the home view of the control panel
- Editing drive texts
- Editing the favorite parameters list on the control panel
- Configuration settings done via control panel (time, date, etc.)

It is strongly recommended to only unlock the User Lock in a maintenance scenario, not during normal operation. Enabling upload of files and therefore an update of firmware during operation could lead to undesired behavior. As long as the User Lock is open the vulnerabilities are exploitable.

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 embedded in the low voltage DC drives and power controllers.

What are the affected LV DC Drives and Power Controllers?

The relevant systems are separated into two groups. Drives (DCS880) and thyristor power controllers (DCT880).

© Copyright 2025 ABB. All rights reserved.

DCS880 as an all-compatible drive family is designed to provide customers across industries and applications with unprecedented levels of compatibility and flexibility.

DCT880 is a thyristor power controller for precise control of resistive or inductive heaters and infrared heaters in applications for annealing, drying, melting or heating in glass, plastic or metal industry.

What is the CODESYS Runtime System?

The CODESYS Runtime System is a runtime embedded into the firmware of the drive and power controllers. It enables users and integrators to upload and execute their own IEC 61131-3-based applications, to customize the system's behavior for their needs and processes.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could execute arbitrary code on the drive or power controller, gaining full control over the system's firmware.

How could an attacker exploit the vulnerability?

An attacker could exploit the vulnerability by sending a specially crafted message to the drive or power controller. This can be done via USB, ethernet or fieldbus. Fieldbus and Ethernet-based attacks would require them to have network-level access to the system via a fieldbus adapter (e.g. FENA-11).

Could the vulnerability be exploited remotely?

Yes, if the drive is connected to a network via fieldbus interface, the exploitation is possible if the attacker is able to reach the system via the network.

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

Yes, as listed in the *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 no unauthorized personnel can access your devices, components, peripheral equipment, and networks.
- 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.

© Copyright 2025 ABB. All rights reserved.

– When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Also, understand that VPNs are only as secure as the connected devices.

References

3ADW000474R DCS880 Firmware Manual

3ADW000431R DCT880 Manual

For more details about the individual vulnerabilities see the following advisories by CODESYS Group

Name of Advisory	Number	URL
CDS-82457	2023-04	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17764&token=4b2f3cf3a800d076b22f18d49f278bd8883dbd46&download=
CDS-85189	2023-05	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17765&token=04e117e1408fdb8e02b4bc821aa3be819668aef4&download=

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

© Copyright 2025 ABB. All rights reserved.