DOCUMENT ID: 9AKK108470A9989
REVISION: A
DATE: 2025-04-10

CYBER SECURITY ADVISORY

ABB MV Drives Affected by CODESYS RTS (Runtime System) Vulnerabilities

CVE 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

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

Product Name	Type Code	Product sub-type	Affected Firmware Version	Patch Firmware Version
ACS6080	ACS6080-033-W-xxx-xx-xxx-xxxx	ACS6080 (UCU-26)	LAAAA 2.10.0 to LAAAB 5.06.1	LAAAB 5.07
ACS5000	ACS5000-xxx-xxxx-xx-xxx	Generation 3	LAAAB 4.03.0 to LAAAB 5.06.1	LAAAB 5.07
ACS6000	ACS6xxx	ACS6000 Modernized (UCU-26)	LAAAA 2.10.0 to LAAAB 5.06.1	LAAAB 5.07

© Copyright 2025 ABB. All rights reserved.

Vulnerability IDs

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

Summary

Multiple vulnerabilities regarding the CODESYS Runtime System from CODESYS Group have been publicly reported [1][2]. CODESYS Runtime System v.3.5.15.0 is utilized in the firmware of ABB MV ACS6080 and ACS5000 drives to provide IEC 61131 programming capabilities.

These vulnerabilities could lead to out-of-bound memory access. A successful exploit may result in a denial-of-service condition or arbitrary code execution.

Firmware updates are available to address the vulnerabilities listed above in the products mentioned above.

Recommended immediate actions

ABB recommends that customers apply a firmware update as soon as possible to the latest firmware, i.e. LAAAB v. 5.07 and higher, for the affected products. ABB has addressed the CODESYS Runtime System vulnerabilities by disabling the IEC online programming communication by default. As a result, CODESYS communication between affected products and the ABB Automation Builder or ABB Drive Application Builder tools is disabled.

It should be noted that the CODESYS application continues to run on the Drive and if it is necessary to establish communication with CODESYS RTS, for example to debug the CODESYS application, this is possible through the drive parameter configuration. Open the user lock via the "*96.02 Pass code*" parameter and make sure that **bit 9** "*Enable online IEC programming*" is set to TRUE in the "*96.102 User lock functionality*" parameter.

IMPORTANT: After this task, be sure to disable CODESYS communication by setting the bit back to FALSE.

A future firmware update is planned to update the CODESYS RTS library, which will further strengthen defenses for the vulnerabilities mentioned above.

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

Vulnerability severity and details

Overall impact of vulnerabilities mentioned above, if successfully exploited by an attacker, is:

The affected products may exhibit unexpected behavior, leading to trip or impacting performance of the Drive.

Attackers can exploit a single vulnerability for quick access or chain multiple vulnerabilities together for a more complex and devastating attack. Details of each vulnerability are available in the Appendix section, where temporal and environmental metrics are also presented. These scores are specific to the environment and the current state of the vulnerability, which can vary over time and across different contexts.

© Copyright 2025 ABB. All rights reserved.

Mitigating factors

To exploit these vulnerabilities, a successful login to the affected product is required. This can be achieved by one of the following methods:

- Connecting a computer to the Drive, that is running Drive Automation Builder (Automation Builder | ABB) or Drive Composer (Drive Composer - Software tools | ABB).
- Having access to the local network where the drive is located. In this case, an attacker could send malformed packets directly to the drive.

To make the attack more difficult and less likely to succeed, provide network isolation where the drive is located and ensure that no computer running Drive Automation Builder or Drive Composer is connected to the drive without proper security controls. Please refer to “General security recommendations” for further advise on how to keep drive secure.

Refer to the “General Security Recommendations” section at the end of this document for further mitigation actions.

Workarounds

For situations where the “Recommended immediate actions” are not feasible, ABB proposes the following workaround to mitigate this threat:

- Set bit 2 "Disable file download” to TRUE in the "96.102 User lock functionality" parameter.

Although these workarounds will not correct the underlying vulnerability, they can help block known attack vectors. Please refer to “Impact of workaround” section to understand possible reduced functionality of the drive.

IMPORTANT: Contact a qualified and certified ABB personnel if you need more information about the parameter handling of the affected products.

Impact of workaround

This workaround restricts the updating of IEC programs, but existing IEC programs on Drives can still be used. To update an IEC program, the operator must unlock the user lock and enable file download in a protected network environment. It is highly recommended to disable file download, as vulnerabilities are more easily 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 affected products.

What are the affected products?

ACS6080
The primary function of ABB’s ACS6080 medium voltage AC variable speed drive [3] [4] is to provide precise motor control for industrial applications, such as test stands, marine propulsion and thrusters,

© Copyright 2025 ABB. All rights reserved.

rolling mills, mine hoists, conveyors, SAG and ball mills. It operates in the power range from 5.0 to 36.0 MW and offers features like speed and torque control, modular design, high reliability, and ABB Ability services.

ACS5000
The primary function of ABB's ACS5000 medium voltage AC variable speed drive [3][5] is to provide precise motor control for high power, high speed or special performance applications such as test stands, marine propulsion and thrusters, rolling mills, SAG and ball mills, large pumps, fans and compressors. It operates in the power range from 2.0 to 36.0 MW and offers features like speed and torque control, modular design, high reliability, and ABB Ability services.

Is this vulnerability exploitable if the drive is connected via Fieldbus or Gateway?

No, this vulnerability can't be exploited if the only connection is via Fieldbus or Gateway. It is necessary to have a direct connection between a computer and the drive.

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 which will cause drive to trip or reset. See more information about this in "Summary" and "Vulnerability severity and details" sections.

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 drive which is running vulnerable CODESYS RTS. 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. Furthermore, an attacker needs deep knowledge of CODESYS, ABB proprietary protocols and update package.

An attacker can also gain access to the drive from the computer where Drive Application Builder (DAB) or Drive Composer (DC) tool is present to send a crafted message to CODESYS RTS.

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.

Can functional safety be affected by an exploit of this vulnerability?

For the affected products, Functional Safety is ensured with hardware only solutions. This vulnerability does not affect Functional Safety.

What does the update do?

In the latest firmware versions i.e. LAAAB 5.07 and above 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 see [1] and [2].

© Copyright 2025 ABB. All rights reserved.

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.
- Install the drive in a secure location that is only accessible to authorized persons.
- Install physical controls so only authorized personnel can access devices connected to the drive (computers, peripheral equipment, and networks).
- Avoid connecting computers containing Drive Automation Builder programing software to any network other than the network for the devices that it is intended for.
- Ensure security controls are followed on computers connected to the Drive. For example, updated security patches, firewall, anti-virus are installed, and only authorized Software is running. It is customer responsibility to ensure these conditions.

More information on recommended practices can be found in the following document: Protecting operations through cyber security: ABB Drives solutions [6].

Abbreviations

RTS	Runtime system
DAB	Drive Application Builder
DC	Drive Composer

© Copyright 2025 ABB. All rights reserved.

Appendix

Severity Assessment of CVEs

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) [1] v3.1[2]. ABB has further calculated Temporal and Environmental score to get overall CVSS score. These scores are specific to environment and the current state of the vulnerability, which can vary over time and across different contexts. The indicated Common Weakness Enumerations (CWE) have been selected from the MITRE CWE list[3].

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

The CODESYS Control runtime system does not restrict the memory access. An improper restriction of operations within the bounds of a memory buffer allows an attacker with access to the drive with user privileges to gain full access of the drive.

CVSS

Overall CVSS Score: 6.3
CVSS Base Score: 8.8
CVSS Temporal Score: 7.8
CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:W/RC:C
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

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

Overall CVSS Score: 6.3
CVSS Base Score: 6.5
CVSS Temporal Score: 5.8
CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:W/RC:C
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-2023-37550
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-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

Overall CVSS Score: 6.3
CVSS Base Score: 6.5
CVSS Temporal Score: 5.8
CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:W/RC:C
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-2023-37557 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

Overall CVSS Score: 6.3
CVSS Base Score: 6.5
CVSS Temporal Score: 5.8
CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:W/RC:C
CWE
CWE-787: Out-of-bounds Write

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

© Copyright 2025 ABB. All rights reserved.

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

Overall CVSS Score: 6.3
CVSS Base Score: 6.5
CVSS Temporal Score: 5.8
CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:W/RC:C
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

References

[1] CODESYS Security Advisory 2023-04

[2] CODESYS Security Advisory 2023-05

[3] What is a variable speed drive | Drives | ABB

[4] ACS6080 - ABB medium voltage AC drives medium voltage AC drives | ABB

[5] ACS5000 - ABB medium voltage AC drives medium voltage AC drives | ABB

[6] Protecting operations through cyber security: ABB Drives solutions

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.

© Copyright 2025 ABB. All rights reserved.

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial Version applicable to affected MV Products.	25.03.2025

© Copyright 2025 ABB. All rights reserved.

© Copyright 2025 ABB. All rights reserved.