DOCUMENT ID: 3ADR011211
REVISION: B
DATE: 2024-01-10

CYBER SECURITY ADVISORY

AC500 V3
Multiple RCE and DoS vulnerabilities in the CODESYS protocol

CVE-2022-47378, CVE-2022-47379, CVE-2022-47380, CVE-2022-47381, CVE-2022-47382, CVE-2022-47383, CVE-2022-47384, CVE-2022-47385, CVE-2022-47386, CVE-2022-47387, CVE-2022-47388, CVE-2022-47389, CVE-2022-47390, CVE-2022-47392, CVE-2022-47393

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 V3 products (PM5xxx) with firmware version earlier than 3.7.0 are affected by these vulnerabilities.

Vulnerability IDs

- CVE-2022-47378
- CVE-2022-47379
- CVE-2022-47380
- CVE-2022-47381
- CVE-2022-47382
- CVE-2022-47383
- CVE-2022-47384
- CVE-2022-47385
- CVE-2022-47386
- CVE-2022-47387
- CVE-2022-47388
- CVE-2022-47389
- CVE-2022-47390
- CVE-2022-47392
- CVE-2022-47393

Summary

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

After successful authentication, an attacker who exploited this vulnerability could cause denial-of-service conditions, memory being overwritten, or remote code executions.

Recommended immediate actions

ABB has developed a new firmware version 3.7.0 fixing these vulnerabilities. This firmware version is released for all AC500 V3 PLC types and available from Automation Builder 2.7.0. Automation Builder 2.7.0 is available for download from the related download site.

All affected products shall be used only as described in the manual in the chapter “Cyber security in AC500 V3 products” especially regarding defense in depth and secure operation. The manual is also available online (Manual for PLC automation with AC500 V3 and Automation Builder 2.7.0).

Vulnerability severity and details

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

CVE-2022-47378: Improper Validation of Consistency within Input

After successful authentication, specific crafted communication requests with inconsistent content can cause the CmpFiletransfer component to read internally from an invalid address, potentially leading to 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-2022-47379: Out-of-bounds Write

After successful authentication, specific crafted communication requests can cause the CmpApp component to write attacker-controlled data to memory, which can lead to a denial-of-service condition, memory being overwritten, or remote code execution.

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-2022-47380, CVE-2022-47381: Stack-based Buffer Overflow

After successful authentication, specific crafted communication requests can cause the CmpApp component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory being overwritten, or remote code execution.

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

[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-2022-47382, CVE-2022-47383, CVE-2022-47384, CVE-2022-47386, CVE-2022-47387, CVE-2022-47388, CVE-2022-47389, CVE-2022-47390: Stack-based Buffer Overflow

After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory being overwritten, or remote code execution.

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-2022-47385: Stack-based Buffer Overflow

After successful authentication, specific crafted communication requests can cause the CmpAppForce component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory being overwritten, or remote code execution.

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-2022-47392: Improper Validation of Consistency within Input

After successful authentication, specific crafted communication requests with inconsistent content can cause the CmpApp/CmpAppBP/CmpAppForce components to read internally from an invalid address, potentially leading to 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-2022-47393: Untrusted Pointer Dereference

After successful authentication, specific crafted communication requests can cause the CmpFiletransfer component to dereference addresses provided by the request for internal read access, which can lead to a denial-of-service situation.

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

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 to fix the vulnerabilities.

To exploit the vulnerabilities, 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 is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could cause denial-of-service conditions, memory being overwritten, or remote code executions.

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 the affected system node to stop or become inaccessible.

How could an attacker exploit the vulnerability?

After successful authentication , 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?

Yes, this vulnerability has 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.

References

- A Codesys advisory for these vulnerabilities are available from the Codesys website: Security update for CODESYS Control V3
- 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	2023-09-04
B	p4, p5	Added the information about availability of a fix to the chapters “Recommended immediate actions” and “Workarounds”	2024-01-10