DOCUMENT ID: 3ADR010997
REVISION: D
DATE: 2023-03-28

CYBER SECURITY ADVISORY

AC500 V3
Cyber Security Advisory

CVE-2022-1989, CVE-2022-22513, CVE-2022-22514, CVE-2022-22515, CVE-2022-22517, CVE-2022-22518, CVE-2022-22519, CVE-2022-30791, CVE-2022-30792

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 with firmware version smaller than 3.6.0 are affected by this vulnerability.

Vulnerability IDs

- CVE-2022-1989
- CVE-2022-22513
- CVE-2022-22514
- CVE-2022-22515
- CVE-2022-22517
- CVE-2022-22518
- CVE-2022-22519
- CVE-2022-30791
- CVE-2022-30792

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 the product to stop or make the product inaccessible.

Recommended immediate actions

ABB has developed a new firmware version 3.6.0 fixing these vulnerabilities. This firmware version is released for all AC500 V3 PLC types and available from Automation Builder 2.6.0. Automation Builder 2.6.0 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 available from our website for download (Manual for PLC automation with AC500 V3 and Automation Builder 2.6.0).

Vulnerability severity and details

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

CVE-2022-1989: AC500 V3 visualization

To secure the visualization screens or elements, AC500 V3 visualization has an integrated role-based user management. To authenticate at the user management, the AC500 V3 visualization provides a login-dialog. The login-dialog is downloaded to the HMI or PLC as part of the created visualizations and displayed by the AC500 V3 web visualization.

This dialog returns different feedback for invalid user and password, so that an attacker can determine whether a user exists or not.

CVSS v3.1 Base Score:	7.3 (High)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

CVE-2022-22513, CVE-2022-22514: AC500 V3 CODESYS communication servers

AC500 V3 PLCs contain communication servers for the CODESYS protocol to enable communication with clients like Automation Builder. These servers have the following vulnerabilities:

- CVE-2022-22513: CWE-476: NULL Pointer Dereference

  After successful authentication, crafted communication requests can cause a null pointer dereference in the CmpSettings component and lead to a crash of the affected products.

- CVE-2022-22514: CWE-822: Untrusted Pointer Dereference

  After successful authentication, crafted communication requests can force a read or write access to a dereferenced pointer contained in the request. The request is handled in the CmpTraceMgr component of the affected products. The accesses can subsequently lead to local overwriting of memory, whereby the attacker can neither gain the values read internally nor control the values to be written. If invalid memory is accessed, this results in a crash.

The crafted requests are only processed by the affected products, if the online user management is deactivated/not active or if the attacker has previously successfully authenticated himself at the device.

CVSS v3.1 Base Score:	7.1 (High)
CVSS v3.1 Vector:	AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/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-2022-22515: AC500 V3 configuration file access

The control program could utilize this vulnerability to read and modify the configuration file(s) of the affected products via CAA File, SysFile, SysFileAsync, or other IEC code libraries for file access.

Programming the controller is only possible, if the online user management is deactivated/not active or if the attacker has previously successfully authenticated himself at the controller.

CVSS v3.1 Base Score:	7.1 (High)
CVSS v3.1 Vector:	AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N

CVE-2022-22517: AC500 V3 CODESYS communication protocol

AC500 V3 PLCs contain communication servers for the CODESYS protocol to enable communication with clients like Automation Builder. The channel ID generated by these servers to identify the communication channels is insufficient.

Guessing the channel ID allows attackers to disrupt existing communication by injecting additional packets or to close this channel. Since the overlying session-bound services have additional integrity checks and further own identifiers used for authentication and authorization, injected packets are detected and also lead to the channel being closed.

CVSS v3.1 Base Score:	7.5 (High)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2022-22518: AC500 V3 online user management

AC500 V3 PLCs' central role based user management secures the devices for all online protocols and interfaces. Runtime components can register an anonymous login for their implemented protocols at the user management. This enables the programmer of the controller to allow anonymous access for these protocols and to configure the rights for this access even when the user management is enforced. In the case of OPC UA, for example, he can configure which variables the anonymous user can read or write. In addition, the runtime security policy can be configured in the communication settings of the Automation Builder. The policy pro-vides the option of allowing or denying anonymous access for all registered components.

Due to a software flaw, disabling the previously enabled anonymous login in the runtime security policy settings only removes the associated users and groups for one component, but not for all registered components. If more than one component has registered by means of this, anonymous access with the previously configured rights remains permitted for all others.

The runtime itself registers the CmpOPCUAServer component by default, i.e. as soon as an-other component is registered, the issue may occur.

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

CVE-2022-22519: AC500 V3 web server

The AC500 V3 web server is used by the AC500 V3 WebVisu to display visualization screens in a web browser. Specific crafted HTTP or HTTPS requests may cause an internal buffer over-read, which could crash the web server task of the CODESYS Control runtime system.

CVSS v3.1 Base Score:	7.5 (High)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2022-30791, CVE-2022-30792: AC500 V3 CODESYS communication servers

AC500 V3 PLCs contain communication servers for the CODESYS protocol to enable communication with clients like Automation Builder. To limit resource consumption, the AC500 V3 runtime system allows a certain number of incoming TCP connections (CmpBlkDrvTcp) or channel connections (CmpChannelServer, CmpChannelServerEmbedded) of the CODESYS protocol. Once this limit is reached, it does not allow any new client connection. An unauthenticated attacker is able to block all available TCP connections or communication channels. If the attack is repeated, it can permanently prevent legitimate users or clients from establishing a new connection to the AC500 V3 runtime system. Existing connections are not affected and therefore remain intact.

- CVE-2022-30791: CmpBlkDrvTcp allows unauthenticated attackers to block all its available TCP connections.
- CVE-2022-30792: CmpChannelServer, CmpChannelServerEmbedded allow unauthenticated attackers to block all their available communication channels.

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

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.

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”.

- CVE-2022-1989

  ABB has currently found no workaround for this vulnerability. Therefore the PLCs shall only be used as described in the manual in the chapter “Cyber security in AC500 V3 products”.

- CVE-2022-22515

  To exploit these vulnerabilities, a successful login to the affected product is required to download and execute the malicious application code to the PLC. The online user management of the affected products therefore protects from exploiting these security vulnerabilities, even in the case that the software update is not applied.

  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.

- CVE-2022-22517

  ABB has currently found no workaround for this vulnerability. Therefore the PLCs shall only be used as described in the manual in the chapter “Cyber security in AC500 V3 products”.

- CVE-2022-22518

  This issue can be worked around by manually removing the corresponding users and groups, in case the software update is not applied:

  When allowing anonymous login, users and groups are automatically created for all components registered for anonymous access. After deactivating anonymous login in the runtime security policy settings, these can be manually removed again from the online user management of the device concerned. In Automation Builder this can be done in the "Users and Groups" device dialog. In case of this bug, after synchronization, users and groups with the prefix "Anonymous_" such as "Anonymous_OPCUAServer" or "Anonymous_PLCShellLinuxBackend" are present. After deleting these users and groups there, anonymous access is no longer possible.

- CVE-2022-22513, CVE-2022-22514

  To exploit these vulnerabilities, a successful login to the affected product is required to download and execute the malicious application code to the PLC. The online user management of the affected products therefore protects from exploiting these security vulnerabilities, even in the case that the software update is not applied.

  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.

- CVE-2022-22519

  ABB has currently found no workaround for this vulnerability. Therefore the PLCs shall only be used as described in the manual in the chapter “Cyber security in AC500 V3 products”.

- CVE-2022-30791, CVE-2022-30792

  ABB has currently found no workaround for this vulnerability. Therefore the PLCs shall only be used as described in the manual in the chapter “Cyber security in AC500 V3 products”.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could prevent legitimate access to an affected system node or remotely cause an affected system node to stop.

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?

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

Codesys advisories for these vulnerabilities are available from the Codesys website:

- Security update for CODESYS V3 Visualization
- Security update for CODESYS V3 web server
- Security update for several CODESYS V3 products containing a CODESYS communication server
- Security update for CODESYS Control V3 online user management
- Security update for various CODESYS V3 products using the CODESYS communication protocol
- Security update for CODESYS Control V3 configuration file access
- Security update for CODESYS V3 products containing a CODESYS communication server

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	2022-04-26
B	all	Some minor correction of the workarounds Updated to the latest version of the document template.	2022-04-28
C	all	Added CVE-2022-1989, CVE-2022-30791, CVE-2022-30792 Updated release date of fix	2022-07-14
D	p3, p6	Added information about software update closing all vulnerabilities	2023-03-28