DOCUMENT ID: 2CMT006099
REVISION: A
DATE: 2023-03-27

CYBER SECURITY ADVISORY

ABB RCCMD – Use of default password

CVE ID: CVE-2022-4126

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.

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

Affected product	Versions
RCCMD	All versions before 4.40 230207

Vulnerability IDs

CVE-2022-4126

ABBVREP0090

Summary

A software update is available that resolves a privately reported vulnerability in the product versions listed above. The version number of the update is 4.40 230207.

An attacker who successfully exploited this vulnerability could take control of the computer the software runs on and possibly insert and run arbitrary code.

Recommended immediate actions

The problem is corrected in the following product version:

RCCMD version 4.40 230207.

ABB recommends that customers apply the update at earliest convenience. For more information, please get in contact with Digital Service Support ch.ups.digital@abb.com.

Vulnerability severity and details

A vulnerability exists in the access control included in the product versions listed above. An attacker could exploit the vulnerability by accessing the system with default login credentials, allowing the attacker to take control of the product and insert and run arbitrary code.

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

CVE-2022-4126 Use of Default Password

CVSS v3.1 Base Score:	9.6 (Critical)
CVSS v3.1 Temporal Score:	8.9 (High)
CVSS v3.1 Vector:	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2022-4126

Mitigating factors

Refer to section “General security recommendations” for further advise on how to keep your system secure.

Workarounds

ABB has tested the following workaround. Although this workaround will not correct the underlying vulnerability, it can help block known attack vectors. When a workaround reduces functionality, this is identified below as “Impact of workaround”.

Replace the default password to reduce risk for unauthorized access to the system.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could cause legitimate access to an affected system node, remotely cause an affected system node to stop, take control of an affected system node and insert and run arbitrary code in an affected system node.

[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.

What causes the vulnerability?

The vulnerability is caused by RCCMD that uses default password without properly implemented mitigation to reduce risk for exploitation.

What is affected product?

The RCCMD (Remote Control Command) is a software solution. It must be able to distinguish between a real server and a virtual machine whose content appears within the IT infrastructure as a real server and take into account the inevitable dependencies. The main use case is where flexible software solutions for emergency shutdowns are needed. RCCMD runs platform-independent and can connect physical machines to fully virtualized environments to ensure a structured shutdown.

RCCMD can be flexibly adapted to almost any scenario, if for example:

- extensibility and platform-independent flexibility are required
- Special shutdown routines in micromanagement are required
- Highly networked systems need to migrate to other data centers
- Individual script solutions are required in heterogeneous systems
- Mutual dependencies require exact time management

RCCMD starts individual scripts, can pass control commands and information to other RCCMD clients, send feedback, shut down systems, trigger migrations, control and stop server processes, detect redundancies, start tools and pass parameters and much more.

The RCCMD Software Client is a system solution that runs transparently in the background after installation and only becomes active when a valid sender sends a personalized control signal.

Valid transmitters are for example:

- CS141 based device
- Another RCCMD client

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause legitimate access to an affected system node, remotely cause an affected system node to stop, take control of an affected system node and insert and run arbitrary code in an affected system node.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by accessing the RCCMD with the default password, which is proposed by the RCCMD in the installation process. 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.

What does the update do?

The update mitigates the vulnerability by recommending change of default password and to show warning message when default password is used.

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

No, ABB received information about this vulnerability through responsible disclosure.

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 net-work 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.

Acknowledgement

ABB thanks Pablo Valle Alvear from Titanium Industrial Security for finding the vulnerability and protecting our customers.

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	2023-03-27