DOCUMENT ID: 3BUS221709
REVISION: B
DATE: 2023-05-18

CYBER SECURITY ADVISORY

QCS 800xA
Vulnerability identified in system log files
CVE ID: CVE-2022-0010

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

ABB QCS 800xA all versions up to and including 6.1 SP2
ABB QCS AC450 all versions up to and including 5.1 SP2
ABB Platform Engineering Tools up to and including V2.3.0

Vulnerability IDs

CVE-2022-0010

Summary

An attacker, who already has local access to the QCS nodes, could successfully obtain the password for a system user account. Using this information, the attacker could have the potential to exploit this vulnerability to gain control of system nodes.

Recommended immediate actions

ABB recommends following the instructions provided in the Workarounds section of this vulnerability report.

The vulnerability has been corrected in the following product versions:

QCS 800xA – QCS 800xA 6.1 SP3

ABB Platform Engineering Tools – V2.4.0

Vulnerability severity and details

A vulnerability exists in system log files that are created, by the affected product versions, during installation. The log files created may contain confidential data that could be read by low privileged users. This could allow an attacker, who already has local access to the QCS nodes, to obtain a system password that could be used to take control of one or more system nodes.

CVE-2022-0010 and QCS – Information Disclosure

The severity assessment has been performed by using the National Vulnerability Database Common Vulnerability Scoring System Calculator CVSS Version 3.1. 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.

CVSS v3.1 Base Score:	7.8
CVSS v3.1 Temporal Score:	7.5
CVSS v3.1 Vector:	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2022-0010

Mitigating factors

An attacker needs to be able to login to an account in the system, so the primary mitigation against these attacks is to ensure that only authorized persons have access to user accounts on the system nodes. This also includes any user accounts accessing the system via remote tools like Remote Desktop.

Recommended baseline security practices and firewall configurations can help protect a network and its attached devices from attacks that originate from outside the network. For example, common practices are for process control systems to be physically protected from direct access by unauthorized personnel, 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, and others that must be evaluated case by case.

Process control and automation systems should not be used for general business functions (e.g. Internet browsing, email, etc.) which are not critical industrial processes. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system.

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

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".

ABB recommends that customers, who have the affected product versions installed, should:

1. Where possible, change the affected system user account password.
2. Delete the system log files that contain the vulnerability.

For additional details and assistance with these actions please contact your local ABB service organization referencing both this vulnerability notice and 3BUS221708 - “Field Notice - Vulnerability identified in system log files [CVE-2022-0010]”.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could take control of an affected system node.

What causes the vulnerability?

The vulnerability is caused by the product installation process writing confidential information into unsecured files.

What is the affected product or component?

The QCS products are responsible for controlling the quality of paper as it is being produced on a Paper Machine.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could be allowed to take control of system nodes.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability to take control of system nodes. This would first 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.

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

Functional safety should not be affected by this vulnerability.

What does the update do?

The update prevents superfluous confidential information being logged during future installations.

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 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 following documents:

<Document ID> <Document title>

Acknowledgement

References

1ABC123456 Document Title

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	20/04/2023
B	2,3,4,5,6	Removed watermark	18/05/2023