DOCUMENT ID: 7PAA007893
REVISION: A
DATE: 2023-03-27
SECURITY LEVEL: PUBLIC

CYBER SECURITY ADVISORY

SECURITY - My Control System (on-premise) Information Disclosure vulnerability

CVE ID: CVE-2023-0580

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 2023 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 (e.g. ICS-CERT).

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

My Control System (on-premise), versions 5.0 through 5.13.

Vulnerability ID

CVE-2023-0580

Summary

A vulnerability exists in My Control System (on-premise), for which an update is available, where confidential data is written into an unprotected file.

An attacker who successfully exploited this vulnerability could gain access to the protected application data or could take control of the application.

Of the services that make up the My Control System (on-premise) application the following ones are affected by this vulnerability:

User Interface

System Monitoring[1]

Asset Inventory

[1] System Monitoring is an optional service of the My Control System (on-premise) application and is not installed by default

© Copyright 2023 ABB. All rights reserved.

Recommended immediate actions

Update to My Control System (on-premise) 5.14 or newer.

Vulnerability severity and details

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) v3.1[2].

CVE-2023-0580 – My Control System (on-premise) leaking credentials

CVSS v3.1 Base Score:	5.4 (Medium)
CVSS v3.1 Temporal Score:	5.2 (Medium)
CVSS v3.1 Vector:	AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N/E:H/RL:O/RC:C
CVSS v3.1 Link:	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N/E:H/RL:O/RC:C
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2023-0580

Mitigating factors

No specific mitigating factors other than general security best practices exist which can remediate the effect of this vulnerability.

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

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could impersonate services of the My Control System (on-premise) application and use this to gain access to all data stored in the application databases for which the impersonated application has been granted access.

What causes the vulnerability?

The vulnerability is caused by unproper handling of application confidential information, assigned to a subgroup of the services that make up the My Control System (on-premise) application.

What is the User Interface?

The User Interface is the application service that hosts the webpage through which a user can interact with My Control System (on-premise).

[2] 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.

© Copyright 2023 ABB. All rights reserved.

What is System Monitoring?

System Monitoring is an optional service of the My Control System (on-premise) application. It collects and analyzes events from connected control systems.

What is Asset Inventory?

Asset Inventory is a service of the My Control System (on-premise) application. It tracks the assets belonging to the control system and its networks.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could gain access to the data stored in the My Control System (on-premise) application to which the affected services have access.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by retrieving and then using confidential information from of any of the affected services to access data stored in the My Control System (on-premise) application.

To retrieve the sensitive data from the application an attacker requires access to the file system of the computer.

Recommended practices will 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 removes the vulnerability by modifying the method by which the affected services handle their confidential information. It ensures that confidential information will always be properly secured.

The update will resolve this vulnerability for all new installations and also for installations that are updated from a version that contained the vulnerability.

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

No, this issue was discovered internally.

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.

Is My Control System (on-web) affected?

No, this vulnerability only affects My Control System (on-premise).

© Copyright 2023 ABB. All rights reserved.

General security recommendations

Control systems and the control network are exposed to cyber threats. In order to minimize these risks, the protective measures and best practices listed below are available in addition to other measures. ABB strongly recommends system integrators and asset owners to implement the measures they consider appropriate for their control system environment:

Place control systems in a dedicated control network containing control systems only.

Locate control networks and systems behind firewalls and separate them from any other networks like business networks and the Internet.

Block any inbound Internet traffic destined for the control networks/systems. Place remote access systems used for remote control system access outside the control network.

Limit outbound Internet traffic originating from control systems/networks as much as possible. If control systems must talk to the Internet, tailor firewall rules to required resources - allow only source IPs, destination IPs and services/destination ports which control systems definitely need to use for normal control operation.

If Internet access is required on occasion only, disable relevant firewall rules and enable them during the time window of required Internet access only. If supported by your firewall, define an expiry date and time for such rules – after the expiry date and time, the firewall will disable the rule automatically.

Limit exposure of control networks/systems to internal systems. Tailor firewall rules allowing traffic from internal systems to control networks/systems to allow only source IPs, destination IPs and services/destination ports which are definitely required for normal control operation.

Create strict firewall rules to filter malicious network traffic targeting control system vulnerabilities ("exploit traffic"). Exploit traffic may use network communication features like source routing, IP fragmentation and/or IP tunneling. If such features are not required for normal control operation, block them on your firewall.

If supported by your firewall, apply additional filters to allowed traffic which provide protection for control networks/systems. Such filters are provided by advanced firewall features like Application Control and Anti-Virus.

Use Intrusion Detection Systems (IDS) or Intrusion Preventions Systems (IPS) to detect/block control system-specific exploit traffic. Consider using IPS rules protecting against control system exploits.

When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Please ensure that VPN solutions are updated to the most current version available.

In case you want to filter internal control network traffic, consider using solutions supporting Intra-LAN traffic control like VLAN access control lists.

Harden your control systems by enabling only the ports, services and software required for normal control operation. Disable all other ports and disable/uninstall all other services and software.

If possible, limit the permissions of user accounts, software processes and devices to the permissions required for normal control operation.

Use trusted, patched software and malware protection solutions. Interact with trusted web sites and trusted email attachments only.

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.

© Copyright 2023 ABB. All rights reserved.

Protect control systems from physical access by unauthorized personnel e. g. by placing them in locked switch cabinets.

More information on recommended practices can be found in the referenced documents.

References

https://myportal.abb.com/home/my-control-system/#/documentation/release-notes

(Please review the entry for Version 5.14)

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	27-03-2023

© Copyright 2023 ABB. All rights reserved.