DOCUMENT ID: 9AKK108467A9754
REVISION: A
DATE: 2023-03-21

CYBER SECURITY ADVISORY

Flow-X disclosure of sensitive information to unauthenticated users

CVE ID: CVE-2023-1258

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

ABB has determined that Flow-X firmware versions up to 3.2.6 are affected.

Vulnerability IDs

CVE-2023-1258

Summary

A vulnerability regarding the exposure of sensitive information over the Flow-X web API has been reported.

ABB is aware of a vulnerability regarding the exposure of sensitive information over the Flow-X web API for the versions listed above.

The sensitive information includes the 'enumeration of authorized users' and 'extended device information'.

The vulnerability is considered as medium risk. An update for the Flow-X firmware is being prepared but is not available yet. This document also describes some mitigations that can help concerned users limit their risk.

Recommended immediate actions

To minimize the risk of unauthorized access to sensitive information, ABB recommends to apply the mitigations in the "Mitigating Factors" section.

Furthermore, the unauthorized access to the 'enumeration of authorized users' has been partially addressed in version 3.1.0 of the Flow-X firmware (available as of September 2019). ABB recommends to install at least version 3.1.0 or a newer whenever possible.

A complete fix for this vulnerability will be available in version 4.0.0 of the firmware that is planned for release in Q4 of 2023.

Vulnerability severity and details

An attacker could exploit this vulnerability to obtain an overview of the usernames which can login into the device and device information such as the firmware version and the application running on the device.

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

CVE-2023-1258

CVSS v3.1 Base Score:	5.3 (out of 10)
CVSS v3.1 Temporal Score:	5.3 (out of 10)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:U/RC:C[1]
CVSS v3.1 Vector Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:U/RC:C/CR:L/IR:X/AR:X/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:L/MI:N/MA:N&version=3.1
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2023-1258

Mitigating factors

To minimize the risk of unauthorized access to sensitive information, ABB recommends to only operate Flow-X flow computers in secure networks.

Additionally, ABB recommends that HTTPS is used to communicate with the Flow-X web server. HTTPS support has been implemented since version 1.2.2 (available as of June 2016) and is enabled by default since version 3.2.0 (available as of September 2020).

To minimize the risk of exposed security information on one device leading to unauthorized access on other devices, ABB recommends that customers change the usernames and passwords that are part of the standard application and to use different usernames and password on different devices.

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

[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.

Frequently asked questions

What is the scope of the vulnerability?

The web API of the Flow-X flow computer.

What causes the vulnerability?

The vulnerability is caused by insufficient authentication on the web API.

What is Flow-X?

Flow-X is a series of flow computers with a powerful and versatile automation platform and especially designed for the custody transfer of liquid and gas.

What might an attacker use the vulnerability to do?

Exploiting this vulnerability could make it easier for an attacker to impersonate a user or find vulnerable devices.

How could an attacker exploit the vulnerability?

An attacker can remotely call the web API. 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 industrial 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?

No. An attacker still would need to find a matching password or a known exploit for an existing version.

What does the update do?

As of version 3.1.0 of the Flow-X firmware, authentication is required to access the ‘enumeration of authorized users’. However, the audit logs which include the names users that have logged in, and ‘extended device information’ is still accessible without authentication. A solution for these remaining vulnerable web API endpoints will be provided in version 4.0.0 of the firmware.

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.
- Configure the Flow-X web server to only be available over HTTPS. HTTPS has been available since Flow-X 1.2.2 and using only HTTPS is the default since Flow-X 3.2.0.
- For authentication of users, always use strong passwords. Use different passwords for the same user on different devices.
- Change the usernames and passwords of users that are included in the default application.

More information on recommended practices can be found in the operation and configuration manual that is part of the Flow-Xpress configuration software installation: SPIRITIT FLOW-X OPERATION & CONFIGURATION MANUAL.

Acknowledgement

ABB would like to thank the following for working with us to help protect customers:

Paul Smith of SCADAfence for reporting this vulnerability following coordinated disclosure.

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	2023-03-10
B	All	Released version	2023-03-27