DOCUMENT ID: 7PAA007517
REVISION: E
DATE: 2023-08-04
SECURITY LEVEL: PUBLIC

CYBER SECURITY ADVISORY

Freelance
SECURITY - Freelance AC 900F and AC 700F, multiple vulnerabilities

CVE IDs:
CVE-2023-0425, CVE-2023-0426

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 (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

The following table lists the affected Freelance versions and Freelance controllers and indicates which of the vulnerabilities these are affected by.

Freelance major version	Freelance controllers	CVE-2023-0425	CVE-2023-0426
V9.2 SP2 and prior	DCP		
	AC 700F	Yes	Yes
	AC 800F		
Freelance 2013 Freelance 2013 SP1 Freelance 2016 Freelance 2016 SP1 Freelance 2019 Freelance 2019 SP1 Freelance 2019 SP1 FP1	DCP		
	AC 700F	Yes	Yes
	AC 800F		
	AC 900F	Yes	Yes

Vulnerability IDs

CVE-2023-0425, CVE-2023-0426

Summary

ABB is aware of vulnerabilities in the product versions listed above. An update is available that resolves the reported vulnerabilities in the product versions under maintenance.

An attacker who successfully exploited one or more of these vulnerabilities could cause the product to stop or make the product inaccessible.

Recommended immediate actions

The Freelance system shall be used only as described in the manual 3BDD012560-111 “Getting Started” chapter 1.2.6.

The listed vulnerabilities are corrected in the following product versions:

- Freelance 2016 SP1 RU06
- Freelance 2019 SP1 RU02
- Freelance 2019 SP1 FP1 RU03

ABB recommends that customers apply the update at earliest convenience. End users who are unable to install the updates should immediately look to implement the Mitigation and Workarounds listed below as this will significantly restrict an attacker’s ability to compromise their installations.

Vulnerability severity and details

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

CVE-2023-0425: Buffer Overflow

An attacker could exploit the vulnerability by sending a specially crafted message to the controller, causing the controller to stop.

CVSS v3.1 Base Score:	8.6 (High)
CVSS v3.1 Temporal Score:	7.5 (High)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H/E:U/RL:O/RC:C
CVSS v3.1 Link:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H/E:U/RL:O/RC:C
NVD Summary:	NVD - CVE-2023-0425 (nist.gov)

CVE-2023-0426: Stack Overflow

An attacker could exploit the vulnerability by sending a specially crafted message to the controller, causing the controller to stop.

CVSS v3.1 Base Score:	8.6 (High)
CVSS v3.1 Temporal Score:	7.5 (High)
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H/E:U/RL:O/RC:C

[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 Link: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H/E:U/RL:O/RC:C
NVD Summary: NVD - CVE-2023-0426 (nist.gov)

Mitigating factors

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 vulnerabilities, they can help block known attack vectors.

CVE-2023-0425: Buffer Overflow

- We recommend disabling the webserver when not needed. The webserver is disabled by default from Freelance 2019 SP1 FP1 on (see Release Notes 2PAA124716-112).

CVE-2023-0426: Stack Overflow

- We recommend disabling the webserver when not needed. The webserver is disabled by default from Freelance 2019 SP1 FP1 on (see Release Notes 2PAA124716-112).

Frequently asked questions

What is the scope of the vulnerabilities?

An attacker who successfully exploited one ore more of these vulnerabilities could remotely cause an affected controller to stop.

What causes the vulnerabilities?

The vulnerabilities are caused by insufficient validation of input data in the HTTP communication and due to incorrect storage of authenticator data.

What is a Freelance controller?

A Freelance controller is the central unit of the Freelance DCS system like PM 783F or PM 803F or PM 904F.

What might an attacker use the vulnerabilities to do?

An attacker who successfully exploited the mentioned vulnerabilities could cause the affected controller to reboot or stop.

How could an attacker exploit the vulnerabilities?

An attacker could try to exploit these vulnerabilities by creating a specially crafted message and sending the message to an affected controller. 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 controller or otherwise infects the network with malicious software.

Could the vulnerabilities be exploited remotely?

Yes, an attacker who has network access to an affected controller could exploit this vulnerabilities. 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 these vulnerabilities. The stack overflow and buffer overflow isn't possible anymore. The storage of the credentials in the system is properly protected.

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

No, ABB received information about these vulnerabilities through responsible disclosure.

When this security advisory was issued, had ABB received any reports that these vulnerabilities was being exploited?

No, ABB had not received any information indicating that these vulnerabilities had been exploited when this security advisory was originally issued.

Acknowledgement

ABB thanks Nataliya Tlyapova and Denis Goryushev (Positive Technologies) for responsibly reporting the vulnerabilities and working with us as we addressed them.

References

3BDD012560-111	Getting started
2PAA124716-112	Release Notes for Freelance 2019 SP1 FP1 system release
2PAA109295-111	Mounting and Installation Instructions, AC 900F Controller
CVE-2023-0425	Buffer Overflow
CVE-2023-0426	Stack Overflow

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 Freelance products are always up to date in terms of installed software, operating system and firmware patches as well as anti-virus and firewall.
- 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 following documents:
  - 2PAA112641-111 Freelance Hardening Manual
  - 3BSE032547 Security for Industrial Automation and Control Systems
  - 2PAA122516 ABB Ability™ System 800xA, Symphony® Plus and Freelance System Hardening

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.