DOCUMENT ID: 9AKK108470A5684
REVISION: G
DATE: 2025-02-14

CYBER SECURITY ADVISORY

FLXeon Controllers Multiple vulnerabilities

Several CVE's, see table inside document

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

Platform	Model number	ABB Product ID	Firmware Version	FW version improving the product
FBXi	FBXi-8R8-X96 FBXi-8R8-H-X96 FBXi-X256 FBXi-X48 FBXi-8R8-X96-S	2CQG201028R1011 2CQG201029R1011 2CQG201014R1021 2CQG201018R1021 2CQG201606R1011	9.3.4 and older	9.3.5
FBVi	FBVi-2U4-4T No Actuator/Strategy FBVi-2U4-4T-IMP FBVi-2U4-4T-SI	2CQG201015R1021 2CQG201016R1021	9.3.4 and older	9.3.5
FBTi	FBTi-7T7-1U1R (Generic - No Strategy) FBTi-6T1-1U1R (Generic - No Strategy)	2CQG201022R1011 2CQG201022R1011	9.3.4 and older	9.3.5
CBXi	CBXi-8R8 CBXi-8R8-H	2CQG201001R1021 2CQG201002R1021	9.3.4 and older	9.3.5

Please Note: All the Platforms listed above are defined as FLXEON in the subsequent document.

Vulnerability IDs

No.	CVE ID	Title	Status	Version fixing the Issue
1	CVE-2024-48841	Remote Code Execution (RCE) Vulnerabilities	<9.3.5	9.3.5
2	CVE-2024-48849	Authentication and Authorization Issues	<9.3.5	9.3.5
3	CVE-2024-48852	Information Disclosure	<9.3.5	9.3.5

Summary

ABB became aware of vulnerabilities in the product versions listed above.

FLXEON devices are not intended to be internet-facing. A product advisory issued in June 2023 informed customers of this parameter.

An attacker can successfully exploit these vulnerabilities and could take remote control of the product and potentially insert and run arbitrary code.

ABB requires, as noted in previous security advisories and user documentation, that FLXEON should not be exposed to the internet or any other insecure network.

Note: In order to exploit an FLXEON, an attacker would need a misconfigured system.

ABB strongly advises customers and system integrators to follow the instructions documented in: FBXi, CBXi and ASPECT® SOLUTIONS, which can be downloaded from the ABB library.

Recommended immediate actions

Please immediately do the following actions on any released SW version of FLXEON:

- Stop and disconnect any FLXEON products that are exposed directly to the Internet, either via a direct ISP connection or via NAT port forwarding
- Ensure that physical controls are in place, so no unauthorized personnel can access your devices, components, peripheral equipment, and networks
- Ensure that all FLXEON products are upgraded to the latest firmware version. Please find the latest version of FLXEON firmware on the respective product homepage
- When remote access is required, only use secure methods. If a Virtual Private Network (VPN) is used, ensure that the chosen VPN is secure i.e. updated to the most current version available and configured for secure access.

Vulnerability severity and details

ABB has become aware of vulnerabilities.

Customers who operate instances of FLXEON and exposing its ports through the Internet e.g. to support remote access, are requested to disconnect and isolate the devices immediately.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) for both v3.1[1] and v4.0[2].

The following CVSS v3.1 and CVSS v4.0 scores of below listed CVE's, rate the severity of the respective vulnerability based on an FLXEON system which is installed and configured in accordance with ABB specifications.

Note: In accordance with ABB specifications, FLXEON should never be exposed to the Internet!

No.	CVE ID	Title	
1	CVE-2024-48841	Remote Code Execution (RCE) Vulnerabilities	
	Description	Network access can be used to execute arbitrary code with elevated privileges. This issue affects FLXEON <=9.3.4	
	CWE	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')	
	CVSS v3.1	Base Score:	10.0
		Temporal Score:	9.0
		Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
	CVSS v4.0	Score	10
		Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
2	CVE-2024-48849	Authentication and Authorization Issues	
	Description	Session management was not sufficient to prevent unauthorized HTTPS requests. This issue affects FLXEON<= 9.3.4	
	CWE	CWE-1385: Missing Origin Validation in WebSockets	
	CVSS v3.1	Base Score:	9.4
		Temporal Score:	8.4
		Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C
	CVSS v4.0	Score	8.8
		Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N

—

[1] For the CVSS v3.1 scoring only the CVSS Base Score and the Temporal Score (if information is available) are considered in this advisory. 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.

[2] For the CVSS v4.0 scoring only the CVSS Base Metrics and the CVSS Supplemental Metrics (if information is available) are considered in this advisory. The CVSS Environmental and Threat Metrics, which can affect the vulnerability severity, are not provided in this advisory since they reflect the potential impact of a vulnerability within the end-user organizations' computing environment and over time depending on the vulnerability exploit maturity. Therefore, end-user organizations are recommended to analyze their situation and specify the Environmental and Threat Metrics.

3	CVE-2024-48852	Information disclosures.	
	Description	Some information may be improperly disclosed through https access. This issue affects FLXEON<= 9.3.4	
	CWE	CWE-532: Insertion of Sensitive Information into Log File	
	CVSS v3.1	Base Score:	9.4
		Temporal Score:	8.4
		Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C
	CVSS v4.0	Score	6.9
		Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Mitigating factors

The vulnerabilities reported in scope of this document are only exploitable if attackers can access the network segment where FLXEON is installed and exposed directly to the internet. ABB therefore recommends the following guidelines in order to protect customers networks:

- FLXEON devices should never be exposed directly to the Internet either via a direct ISP connection nor via NAT port forwarding. If remote access to a FLXEON system is a customer requirement, the system shall operate behind a firewall. Users accessing FLXEON remotely shall do this using a VPN Gateway allowing access to the particular network segment where FLXEON is installed and configured.
- Note: it is crucial that the VPN Gateway and Network is setup in accordance with best industry standards and maintained in terms of security patches for all related components.
- ABB System Integrators shall change default passwords if they are still in use.
- Ensure that all FLXEON products are upgraded to the latest firmware version. Please find the latest version of FLXEON firmware on the respective product homepage

Workarounds

Users accessing FLXEON remotely shall do this using a VPN Gateway allowing access to the particular network segment where FLXEON is installed and configured.

Note: it is crucial that the VPN Gateway and Network is setup in accordance with best industry standards and maintained in terms of security patches for all related components.

Frequently asked questions

What causes the vulnerabilities?

The vulnerabilities are caused by configuration issues allowing the attacker to do various unintended, unauthorized actions on the target device. Please look at the description of the respective CVE's for further details.

What is FLXEON?

FLXEON is a device intended to collect energy data. Based on the values of the collected energy data, FLXEON may trigger controls to optimize energy consumption in a building.

What might an attacker use the vulnerability to do?

If this vulnerability has been successfully exploited by an attacker, this could allow the attacker to take control of the system node. Furthermore, it allows the attacker to insert and run arbitrary code.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to FLXEON. 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 security system.

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 nor any other untrusted network, 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?

FLXEON is not designed as a functional safety device.

Is a software update available fixing the problem?

Yes. FLXEON Version 9.3.5 or newer is fixing the issues listed in this advisory.

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

No. ABB is not aware of any report about public disclosure of the vulnerabilities listed in this advisory.

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 and especially for products in scope of the FLXEON product line, we strongly recommend the following (non-exhaustive) list of cyber security practices:

- Ensure that all FLXEON products are upgraded to the latest firmware version. Please find the latest version of FLXEON firmware on the respective product homepage
- 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 FLXEON ports and endpoints to ensure that they are not accessible directly from the Internet.
- 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.

More information on recommended practices can be found in the following documents:

HT0038	FBXi, CBXi and ASPECT® SOLUTIONS

Acknowledgement

ABB likes to thank Gjoko Krstikj, Zero Science Lab, for reporting the vulnerabilities in responsible disclosure.

References

HT0038 FBXi, CBXi and ASPECT® SOLUTIONS

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	2025-01-20
B	all	Fixing file name	2025-01-20
C	all	Fixing page formatting when converting to pdf	2025-01-20
D	4	CVE-2024-48841, corrected severity	2025-01-23
E	all	Resolved minor fixes, typos	2025-01-29
F	all	Copyright year and CVSS value typo	2025-01-29
G	4	CWE value and description corrected	14.02.2025