DOCUMENT ID: 9AKK108471A7808
REVISION: A
DATE: 2025-10-07

CYBER SECURITY ADVISORY

EIBPORT Reflected XSS

CVE ID: CVE-2021-22291

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

Product Name	Description	ABB Product ID	Affected firmware Version
EIBPORT V3 KNX	EIBPORT LAN gateway	2CLA963710W1001; 2CSM256242R2001	<3.9.2
EIBPORT V3 KNX GSM	EIBPORT LAN gateway + GSM	2CLA963720W1001	<3.9.2

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

Vulnerability IDs

No.	CVE ID	Title	Affected SW version	Fixed in Version
1	CVE-2021-22291	reflected XSS	<3.9.2	3.9.2

Summary

ABB is aware of vulnerabilities in the product versions listed above. A firmware update is available that resolves these privately reported vulnerabilities in the product versions listed above.

An attacker who successfully exploited these vulnerabilities could access sensitive information stored inside the device and can change the configuration of the device.

Recommended immediate actions

ABB recommends that customers apply the update at the earliest convenience.

Vulnerability severity and details

No.	CVE ID	Title	
1	CVE-2021-22291	reflected XSS	
	Source	Researcher	
	Status	Fixed	
	Description	The vulnerability allows the successful attacker to receive a copy of the session id.	
	CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	
	CVSS v3.1	Base Score:	8.0
		Temporal Score:	8.0
		Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H
	CVSS v4.0	Score	8.5
		Vector:	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
	NVD	https://nvd.nist.gov/vuln/detail/CVE-2021-22291	

Mitigating factors

Recommended security practices and firewall configurations can help protect a process control network from attacks that originate from outside the network. Such practices include that process control systems are 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 have to be evaluated case by case. Process control systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system.

More information on recommended practices can be found in the documents listed in the Reference section.

Frequently asked questions

What causes the vulnerability?

The session management of vulnerable FW versions of EIBPORT, fails to maintain a secure session management.

What is EIBPORT?

EIBPORT is a building management system allowing to automate buildings based on the KNX standards.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited these vulnerabilities can gain access to the EIBPORT device without authenticating her-, himself.

Could the vulnerability be exploited remotely?

No, recommended practices include that building automation 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. Following these best practices, an attacker cannot exploit the vulnerability remotely. Unfortunately, ABB became aware that some customers have commissioned EIBPORT not according to these best practices but have made the IP address to the device accessible over the Internet or other untrusted networks. ABB emphasizes that this configuration is against the intended use of the system.

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

No. EIBPORT is not designed as a functional safety device.

What does the update do?

The update removes the vulnerabilities by modifying the way that the device firmware verifies login credentials and token or session identifiers. Furthermore, it hardens the product configuration wherever possible.

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

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

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 EIBPORT product line, we strongly recommend the following (non-exhaustive) list of cyber security practices:

- Ensure that all EIBPORT products are upgraded to the latest firmware version. Please find the latest version of EIBPORT 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 EIBPORT 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
- Authorized users shall change all default credentials during commissioning of an EIBPORT system. If credentials have not been changed during commission state, ABB advises to change each changeable credential at the earliest

–

More information on recommended practices can be found in the documents listed in the Reference section.

Acknowledgement

One of the finders and reporters of the vulnerabilities listed above have chosen to remain anonymous but being mentioned under a pseudonym. ABB respects this decision and thanks these professional working people to help protect its customers.

ABB thanks the following for working with us to help protect customers:

Psytester, for describing the findings and helping to verify the resolving implementation

References

ID	Title	URL	Provider
1	Supplier of Firmware	https://bab-technologie.com/	Bab-Tec
2	Hardening guide for EIBPORT	https://bab-tec.de/itsecurity	Bab-Tec
2	System Manual 1	ABB Library Link	ABB
3	System Manual 2	ABB Library Link	ABB

ID	Title	URL	Provider
4	ABB Hardening guide for general EIB and other products	Smart Home Guide for network security in building systems control.	ABB

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	2025-10-07