ABB DOC ID: 9AKK107992A7304
REVISION: B
DATE: 2021-09-07

CYBER SECURITY ADVISORY

EIBPORT several CVEs ABBVREP0049_R9120

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.

Affected Products

The following ABB products are affected by this vulnerability report:

Product name	Product ID	Description
EIBPORT V3 KNX	2CLA963710W1001	EIBPORT LAN gateway DIN-8M
EIBPORT V3 KNX GSM	2CLA963720W1001	EIBPORT LAN gateway + GSM
EIBPORT V3 KNX	6186-L	Gateway KNX/IP
EIBPORT V3 KNX GSM	6186-L+GSM	Gateway KNX/IP
EIBPORT V3 KNX	10104_E; 4260187360519	EIBPORT LAN KNX
EIBPORT V3 KNX GSM	10304; 4260187360618	EIBPORT LAN KNX + GSM Version 3
EIBPORT V3 KNX	BAB10104	EIBPORT v3 LAN EIBPORT Ver 3 Lan 64/64
EIBPORT V3 KNX EnOcean	BAB10504	EIBPORT v3 LAN/EnOcean EIBPORT LAN KNX KNX + EnOcean Version 3
EIBPORT V3 KNX	2CSM256242R2001	EIBPORT WEBSERVER
EIBPORT V3 KNX	BAB10104	EIBPORT v3 LAN EIBPORT Ver 3 Lan 64/64

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 access the device with root privileges.

Vulnerability Severity

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

CVE reference	CVSS 3.1 (https://www.first.org/cvss/calculator/)	CVSS Base Score	Comment	Status	Fixed in version
CVE-2021-28909	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	9.8	Unauthenticated access exploitable	Fixed	3.9.0

CVE-2021-28910	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C	7.5	Unauthenticated access exploitable	Fixed	3.9.1
CVE-2021-28911	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	9.8	Unauthenticated access exploitable	Fixed	3.9.0
CVE-2021-28912	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H/RL:O/RC:C	6.8	Requires authentication	Fixed	3.9.1
CVE-2021-28913	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	9.8	Unauthenticated access exploitable	Fixed	3.9.0
CVE-2021-28914	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H/RL:O/RC:C	6.8	Requires authentication	Fixed	3.9.0

Recommended immediate actions

The problem is corrected in the following product versions:

EIBPORT, firmware version: 3.9.1

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

ABB also recommends renewing the system administrator password with reasonable length (e.g. >8 characters) and an appropriate entropy (contains a random sequence of numbers, small/capital/special-characters).

Vulnerability Details

CVE-2021-28909

EIBPORT V3 3.8.3 and prior allow a brute force attack to the login service. The password could be weak and default username is known as "admin".

CVE-2021-28910

EIBPORT V3 3.8.3 and prior contains basic SSRF vulnerability.

CVE-2021-28911

EIBPORT V3 3.8.3 and prior allow unauthenticated attackers access to some sensitive data supporting the attacker in a brute force attack.

CVE-2021-28912

EIBPORT V3 3.8.3 and prior. A device specific security credential can be obtained.

CVE-2021-28913

EIBPORT V3 3.8.3 and prior. A device specific security credential can be obtained.

CVE-2021-28914

EIBPORT V3 3.8.3 and prior allow the user to set a weak password because the strength is shown in configuration tool, but finally not enforced.

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 following documents:

Smart Home Guide for network security in building systems control.

Frequently Asked Questions

What is the scope of the vulnerabilities?

An attacker who successfully exploited these vulnerabilities can gain access to the EIBPORT device with root privileges. In this case the attacker has full control to use the device.

What causes the vulnerability?

The device firmware contains a list of vulnerabilities. All these vulnerabilities together provide a set of options an attacker may use to take over control of the device.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited these vulnerabilities can gain access to the EIBPORT device with root privileges. In this case the attacker has full control to use the device.

How could an attacker exploit the vulnerability?

Since the EIBPORT is a device that requires manual steps to install firmware updates, it is expected that it will take some time until all legitimate users have updated their systems to the latest available firmware version. For this reason, the concrete attack options, that a potential attacker benefits from are taken off from this advisory for security reason.

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. Especially it is recommended not to use dynDNS-Services and such alike to remote control a device.

What does the update do?

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

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.

Acknowledgements

The finder and reporter of the vulnerabilities listed above have chosen to keep themselves anonymous but being mentioned under a pseudonym. ABB respects this decision and thanks these professional working people to help protect 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

Support

For additional information and support please contact your local ABB service organization. For contact information, see https://new.abb.com/contact-centers.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.