DOCUMENT ID: 9AKK108464A0803
REVISION: C
DATE: 2024-06-06

CYBER SECURITY ADVISORY

KNX Secure Devices
FDSK Leak and replay attack

CVE ID: CVE-2024-4008, CVE-2024-4009

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

Product ID	Product name	Affected versions
2TMA310010B0001	2,4" Display 55	1.00
2TMA310011B0001	2,4"' Display 55	1.00
2TMA310011B0002	2,4" Display 63	1.00
2TMA310010B0003	2,4" Display 63	1.00
2TMA310011B0003	RoomTouch 4”	1.00
2TMA310010B0004	RoomTouch 4"	1.00
2TMA310010B0006	2,4" Display 70	1.00
2TMA310011B0004	2,4" Display 70	1.00
2TMA310010W0001	RoomTouch 4"	1.00
2TMA310011W0001	RoomTouch 4"	1.00
2CKA006120A0079	BCU* KNX	1.3.0.33
2CKA006120A0080	BCU* KNX	1.3.0.33
2CKA006120A0081	BCU* KNX	1.3.0.33

Table 1: Affected Products

*) BCU=Bus Coupling Unit

Vulnerability IDs

CVE-2024-4008, CVE-2024-4009

Summary

An internal software audit has identified a vulnerability in the product versions listed in Table 1: Affected Products . A firmware (FW) update is available that resolves the vulnerabilities in the respective product versions.

The vulnerabilities concern exclusively KNX systems that apply the KNX Data Secure standard. KNX Systems that operate in classic KNX configurations (plain mode), are not affected.

These advisory handles two separate vulnerabilities concerning the same set of products.

First vulnerability:

An attacker, who successfully exploited this vulnerability, could become aware of the Factory Default Setup Key (FDSK) which is used during commissioning of an affected product to secure the transmission of the Tool-key. The Tool-key secures the logical connection between a KNX Secure device and the Engineering-Tool-Software (ETS).

Second vulnerability:

An attacker, who successfully exploited this vulnerability, could record and replay a KNX Secure telegram sent by a vulnerable device. The vulnerability is caused by failing to store sequence numbers in the moment of a bus power failure. While it is possible to replay a particular KNX telegram, it is not possible to craft any KNX telegram as it is assumed that the symmetric key, required for KNX group communication, is not at hand of the attacker.

Recommended immediate actions

ABB has resolved all CVE's referenced in this document with the software versions detailed in Table 2: Software versions resolving all .

Customers, who have purchased an affected product, are requested to follow the steps listed below to securely resolve the open issues when commissioning a KNX-Data-Secure network:

- Connect the affected product directly to a Personal Computer (PC) running the ETS in a Point-to-Point (P2P) fashion. This guarantees that there is no way that the communication between both devices can become intercepted. Customers, who can reasonably assume that their KNX Network is secure, can even connect the PC indirectly to the affected product via the KNX data secure network.
- Ensure that all symmetric keys, including the tool key for this device, are renewed[1].
- Update the firmware of the affected product using the standard KNX Secure update mechanism.
- Configure the KNX Secure device according to the KNX project as specified in the ETS project.

Now the device operates in KNX Data Secure mode and is secured for subsequent usage.

Note: Customers, who have reasons to assume that the FDSK of an affected device has become known to untrusted parties, must repeat the above-described process in case an affected device is set back to factory default. After successfully executing the above-described process, the devices operate securely.

Product ID	Product name	SW versions resolving all CVE's
2TMA310010B0001	2,4" Display 55	1.02 (and newer)
2TMA310011B0001	2,4"' Display 55	1.02 (and newer)
2TMA310011B0002	2,4" Display 63	1.02 (and newer)
2TMA310010B0003	2,4" Display 63	1.02 (and newer)
2TMA310011B0003	RoomTouch 4"	1.02 (and newer)

[1] Within the corresponding ETS project, switch the affected device once to KNX plain mode and then back to KNX Secure mode. Verify that the keys have been changed under: ETS/Reports, section: "Project Security Summary".

Product ID	Product name	SW versions resolving all CVE's
2TMA310010B0004	RoomTouch 4"	1.02 (and newer)
2TMA310010B0006	2,4" Display 70	1.02 (and newer)
2TMA310011B0004	2,4" Display 70	1.02 (and newer)
2TMA310010W0001	RoomTouch 4"	1.02 (and newer)
2TMA310011W0001	RoomTouch 4"	1.02 (and newer)
2CKA006120A0079	BCU* KNX	1.3.1_63 (and newer)
2CKA006120A0080	BCU* KNX	1.3.1_63 (and newer)
2CKA006120A0081	BCU* KNX	1.3.1_63 (and newer)

Table 2: Software versions resolving all CVE's.

ABB recommends that customers apply the update and renewed configuration at the earliest convenience.

Vulnerability severity and details

Two vulnerabilities exist in the products listed in Table 1: Affected Products.

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

CVE-2024-4008 FDSK Leak in KNX Secure Devices

Precondition: The vulnerability is only exploitable if the affected device is not running in KNX Secure mode.

In case one of the products is installed in a KNX system, an attacker could exploit the vulnerability by sending a specially crafted message to one of the products to become aware of the Factory Default Setup Key (FDSK). Subsequently, the attacker must be able to capture all telegrams exchanged between the affected device and the ETS. Once the messages are captured, the attacker is required to make use of the FDSK by decrypting the recorded information to extract all communication-relevant keys. As a result, the attacker can send KNX Secure telegrams on behalf of an affected device.

Exploiting the vulnerability has several limitations given the decentralized nature of the security architecture in KNX Data Secure. KNX Data Systems that have been configured, following best hardening practices, will not allow messages to cross line/area couplers if not needed to fulfill functional

[2] 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 depending on their individual security context.

requirements of a building. The exploitation allows sending KNX Telegrams on behalf of an affected device but only for the group addresses this device relates to.

CVSS v3.1/v4.0 scoring

CVSS v3.1 Base Score:	9.6 (critical)
CVSS v3.1 Temporal Score:	8.6 (high)
CVSS v3.1 Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:H/E:P/RL:O/RC:C/CR:M/IR:M/AR:M/MAV:P/MAC:L/MPR:N/MUI:N/MS:C/MC:H/MI:H/MA:H
CVSS v3.1 Summary link	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:H/E:P/RL:O/RC:C/CR:M/IR:M/AR:M/MAV:P/MAC:L/MPR:N/MUI:N/MS:C/MC:H/MI:H/MA:H
CVSS v4.0 Score:	7.3 (high)
CVSS v4.0 Vector	CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:L/VI:H/VA:H/SC:L/SI:H/SA:H/S:N/AU:N/V:D/RE:M/U:Green
CVSS v4.0 Summary link	https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:L/VI:H/VA:H/SC:L/SI:H/SA:H/S:N/AU:N/V:D/RE:M/U:Green

CVE-2024-4009 Replay Attack in KNX Secure Devices

In the event of a bus power failure, a vulnerable device fails to store sequence numbers of KNX Telegrams. In consequence an attacker may capture the last message sent and replay it with an incremented sequence number that the receiving device accepts.

CVSS v3.1/v4.0 scoring

CVSS v3.1 Base Score:	9.2 (critical)
CVSS v3.1 Temporal Score:	8.3 (high)
CVSS v3.1 Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:H/E:P/RL:O/RC:C/CR:M/IR:M/AR:M/MAV:P/MAC:L/MPR:N/MUI:N/MS:C/MC:H/MI:H/MA:H
CVSS v3.1 Summary link	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:H/E:P/RL:O/RC:C/CR:M/IR:M/AR:M/MAV:P/MAC:L/MPR:N/MUI:N/MS:C/MC:H/MI:H/MA:H
CVSS v4.0 Score:	7.3 (high)
CVSS v4.0 Vector	CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:N/VC:L/VI:H/VA:H/SC:L/SI:H/SA:H/S:N/AU:N/V:D/RE:M/U:Green
CVSS v4.0 Summary link	https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:N/VC:L/VI:H/VA:H/SC:L/SI:H/SA:H/S:N/AU:N/V:D/RE:M/U:Green

Mitigating factors

Following the advises made in section: Recommended immediate actions, vulnerable devices can still be commissioned with perfect security. In case the described recommendations cannot be followed, it shall be avoided to control sensitive devices by the vulnerable devices such as, but not limited to, access control to e.g. hotel rooms or other protected areas.

Workarounds

See section: Mitigating factors.

Frequently asked questions

What is an FDSK?

FDSK abbreviates Factory Default Setup Key. For further details please refer to the KNX Secure specification available on https://knx.org.

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could sent KNX Secure telegrams on behalf of an affected product. Depending on the overall HW and SW configuration of the KNX System, this enables the attacker to switch light, move blinds, change temperature, or unlock doors.

What causes the vulnerabilities?

The vulnerabilities are caused by software coding errors related to FDSK (CVE-2024-4008) and KNX Telegram Sequence Numbers (CVE-2024-4009).

What products or components are affected?

The products listed in section: Affected are compliant to the KNX Secure Standard. The nature of the standard allows connecting general purpose devices to control light, blinds, HVAC components as well as any actuators installed in a residential or commercial building.

What might an attacker use the vulnerability for?

The purpose of the KNX standard is to control any actuator connected to the KNX system in a given building. Therefore, a successful attacker may switch light, move blinds, control HVAC components or activate/deactivate actuators in general. The concrete options highly depend on how the KNX devices are used within the given building environment.

How could an attacker exploit the vulnerability?

Physical access to the respective KNX Network, at the right time, is required to successfully exploit the vulnerability.

The applicability of the vulnerable devices highly depends on how the devices are used and configured in a given KNX building automation system. In general, the successful attacker can send KNX telegrams on behalf of the vulnerable device. Therefore, it is fair to say that the attacker can send any message that the vulnerable device can send but without physical access to the device.

Could the vulnerability be exploited remotely?

The vulnerability cannot be exploited remotely, if the whole installation is protected against unauthorized remote access by applying the recommended KNX and IP security measures.

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

The products listed in section: Affected are not subject to functional safety.

What does the update do?

The firmware updates available to the products listed in section: Affected products, ensures that the FDSK cannot be read and that sequence numbers are stored upon bus power failure so that a replay attack is not possible. anymore.

Is there something the update cannot resolve?

An FDSK that became known to an untrusted party will remain known to the untrusted party. Section Recommended immediate actions explains how to securely commission a device even if the confidentiality of the FDSK is lost.

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

No, ABB R&D has detected the issue itself and has taken all necessary action to resolve it.

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

ABB strongly recommends customers to follow the steps described in section: Recommended immediate actions. In addition, it is recommended to:

Harden the KNX system by only allowing operations and services necessary for the specified functionality of that system.

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 net-work 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.

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

9AKK106713A5111 Smart Home. Guide for network security in building systems control https://search.abb.com/library/Download.aspx?DocumentID=9AKK106713A5111&LanguageCode=en&DocumentPartId=&Action=Launch

References

9AKK106713A5111 Smart Home. Guide for network security in building systems control https://search.abb.com/library/Download.aspx?DocumentID=9AKK106713A5111&LanguageCode=en&DocumentPartId=&Action=Launch

Glossary

Abbreviation	Full classified wording
BCU	Bus Coupling Unit
ETS	Engineering Tool Software
FDSK	Factory Default Setup Key

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	2024-06-05
B	Vulnerability severity and details	Correction of a URL link	2024-06-06
C	all	Corrected Copy Right year which contained a typo.	2024-06-14