Schneider Electric Security Bulletin

Cyber Attacks against KNX Systems Improperly Exposed to the Internet

9 November 2021

Overview

Schneider Electric is aware of confirmed reports of cyber-attacks targeting KNX home and building automation systems utilizing a KNXnet/IP Ethernet to KNX gateway or router that has been improperly exposed to the Internet. The products used in these systems may come from a variety of different vendors, including Schneider Electric. The attackers take several malicious actions against the KNX system endpoints, such as changing control set points and device passwords, essentially making the endpoints useless and difficult, if not impossible, to recover. Please refer to the position paper from the KNX organization for more information.

Details

Based on our current understanding, the KNX systems under attack have been exposed to the Internet by enabling port forwarding on a system's Internet facing firewall/router to port 3671 of a KNXnet/IP Ethernet to KNX gateway or router, effectively connecting the KNXnet/IP Ethernet to KNX device directly to the Internet.

Such an architecture is not supported and is strictly recommended against; however, it is known to be used by system integrators to facilitate access to the KNX system for remote support and maintenance.

Recommended Mitigations

If a KNXnet/IP device is present on the system only to support remote programming, disconnect it from the network. Otherwise, immediate steps should be taken for all KNX systems utilizing a KNXnet/IP Ethernet to KNX gateway or router, regardless of brand, to disable all port forwarding from the system's Internet facing firewall/router to the KNXnet/IP Ethernet to KNX device. If unsure on how to accomplish this, the end user should contact a KNX system integrator for assistance.

If connection of the KNX system to Ethernet is required, as an extra layer of defense use only a gateway or router interface that implements KNXnet/IP Secure, such as the Schneider Electric SpaceLogic KNX Secure IP Router (MTN6500-0103) or SpaceLogic KNX Secure IP Interface (MTN6502-0105).

If it is suspected that your KNX system with Schneider Electric KNX endpoints has already been compromised, please contact the Schneider Electric Customer Care Center.

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be regularly updated

to the most current version available. Also, understand that VPNs are only as secure as the connected devices.
- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Never connect programming software to any network other than the network intended for that device.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow mobile devices that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and systems and ensure that they are not accessible from the Internet.

For more information refer to the Schneider Electric Recommended Cybersecurity Best Practices document.

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services: https://www.se.com/ww/en/work/solutions/cybersecurity/. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, visit the company's cybersecurity support portal page:
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

Schneider Electric Security Bulletin

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 *9 November 2021*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2021.11.09 09:37:07 -05'00'