Schneider Electric Security Bulletin

KNX Systems Publicly Available Exploit

26 April 2023

Overview

Schneider Electric is aware of a publicly available exploit affecting KNX home and building automation systems. The products used in these systems may come from a variety of different vendors, including Schneider Electric **spaceLYnk, Wiser for KNX (formerly homeLYnk), and FellerLYnk** products. The exploit consists of direct access to product functions and brute force attacks on the panel, which may lead to unauthorized access to product features.

Details

The exploit released takes advantage of two vulnerabilities affecting KNX home and building automation systems. Amongst the products targeted, Schneider Electric was able to identify its spaceLYnk and Wiser for KNX (formerly homeLYnk) products in the Proof-of-Concept details. FellerLYnk is impacted.

The first vulnerability is direct access to the product functions Touch, Schedulers, and Visualization without authentication. It was disclosed by Schneider Electric in February 2022 under CVE-2022-22809. The security notification SEVD-2022-039-04 provides remediation for both products in V2.7.0.

The second vulnerability is a brute force attack against the PIN panel. It was disclosed by Schneider Electric in August 2020 under CVE-2020-7525. The security notification SEVD-2020-224-02 provides remediation for both products in V2.5.1.

Both vulnerabilities were fixed in the latest version of spaceLYnk and Wiser for KNX (formerly homeLYnk), although old versions of products improperly exposed to the Internet by end-users have been reported.

In November 2021, Schneider Electric released a security bulletin when made aware of cyber-attacks on KNX products. This new exploit brings further attention to the recommended mitigations in that security bulletin.

Recommended Remediations

We urge our customers to follow the remediations and Wiser for KNX, SpaceLYnk- System Hardening Guideline to be safe from the attack.

We recommend upgrading to the latest products version to ensure the latest security features available:

- homeLYnk (Wiser For KNX) – https://www.se.com/ww/en/product/LSS100100/wiser-for-knx-logic-controller/#pdp-software

- spaceLYnk – https://www.se.com/ww/en/product/LSS100200/spacelynk-logic-controller/#pdp-software
- Fellerlynk – https://online-katalog.feller.ch/download/index.php?menueidLev1=279&menueidLev2=662&menueidLev3=664

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

Customers should use appropriate patching methodologies when applying these patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric's Customer Care Center if you need assistance removing a patch.

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

Schneider's purpose is to empower all to make the most of our energy and resources, bridging progress and sustainability for all. We call this Life Is On.

Our mission is to be your digital partner for Sustainability and Efficiency.

We drive digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the entire lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.

We are the most local of global companies. We are advocates of open standards and partnership ecosystems that are passionate about our shared Meaningful Purpose, Inclusive and Empowered values.
www.se.com

Revision Control:

Version 1.0 *26 April 2023*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2023.04.25 13:18:14 -04'00'