Schneider Electric Security Notification

spaceLYnk & Wiser for KNX (formerly homeLYnk)

11 August 2020

Overview

Schneider Electric is aware of a vulnerability in the spaceLYnk and Wiser for KNX (formerly known as homeLYnk) products.

Affected Product(s)

All hardware versions of:

- spaceLYnk
- Wiser for KNX (formerly homeLYnk)

Vulnerability Details

CVE ID: **CVE-2020-7525**

CVSS v3.0 Base Score 7.5 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

A CWE-307: Improper Restriction of Excessive Authentication Attempts vulnerability exists which could allow an attacker to guess a password when brute force is used.

Remediation

This vulnerability is fixed in V2.5.1 and is available for download below:

spaceLYnk: https://www.se.com/ww/en/product/LSS100200/spacelynk-logic-controller/

Wiser for KNX (formerly homeLYnk): https://www.se.com/ww/en/product/LSS100100/wiser-for-knx-logic-controller/

The following workarounds and mitigations can be applied by customers to reduce the risk:

- Keep the spaceLYnk and Wiser for KNX (formerly homeLYnk) devices behind a firewall, create a firewall rule to whitelist only those devices allowed to access spaceLYnk and Wiser for KNX (formerly homeLYnk) devices; do not allow direct access to the internet.
- Follow the General Security Recommendations in the section below.

Product Information

Wiser for KNX (formerly known as homeLYnk) is a personalized home automation solution, offering a complete system based on open protocols: KNX, Modbus, BACnet and IP.

spaceLYnk allows efficient facility management thanks to the convenient web-based user interface with maintenance information.

Product Category - Residential and Small Business

Learn more about Schneider Electric's product categories here: https://www.se.com/us/en/all-products

How to determine if you are affected

All spaceLYnk and KNX (formerly homeLYnk) firmware versions before 2.5.1 are affected and should update to V2.5.1.

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Locate networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your components, peripheral equipment, and networks.
- Never connect configuration software to any network other than the network for the devices that it is intended for.
- 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 laptops 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 devices and systems; ensure that they are not accessible from the Internet.
- 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.

Acknowledgements

Schneider Electric recognizes the following researcher(s) for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher(s) Name
CVE-2020-7525	Ismail Tasdelen

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, please contact your local Schneider Electric representative and/or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

https://www.se.com/ww/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Legal Disclaimer

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND SUGGESTED MITIGATION ACTIONS, REMEDIATION, FIX, AND/OR GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN “AS-IS” BASIS WITHOUT WARRANTY OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **make the most of their energy and resources**, 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.

Schneider Electric Security Notification

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

www.se.com

Revision Control:

Version 1 *11 August 2020*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2020.08.08 18:13:29 -04'00'