

Schneider Electric Security Notification

spaceLYnk, Wiser For KNX, fellerLYnk

08 February 2022 (08 March 2022)

Overview

Schneider Electric is aware of multiple vulnerabilities in its spaceLYnk, Wiser For KNX, and fellerLYnk products.

[spaceLYnk](#) is a centralized solution that reduces energy and maintenance costs, increases comfort and flexibility, and simplifies building management.

[Wiser for KNX](#), formerly known as homeLYnk, products are personalized energy efficiency solutions, offering a complete system based on open protocols: KNX, Modbus, BACnet and IP.

[fellerLYnk](#) offers more flexibility in visualization and trend recording as well as functions such as presence simulation or time switches that the end customer can easily manage.

Failure to apply the remediations provided below may risk a Cross-Site Request Forgery (CSRF), Missing Authentication, rate limit, or Stored Cross-Site Scripting (XSS) attack which could result in exfiltrated data and unauthorized access.

March 2022 Update: The CVSS score has been updated for CVE-2022-22811 and CVE-2022-22812.

Affected Products and Versions

Product	Version
spaceLYnk	V2.6.2 and prior
Wiser for KNX (formerly homeLYnk)	V2.6.2 and prior
fellerLYnk	V2.6.2 and prior

Vulnerability Details

CVE ID: **CVE-2022-22809**

CVSS v3.1 Base Score 9.1 | Critical | CVSS:3.1/ AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

A *CWE-306: Missing Authentication for Critical Function* vulnerability exists that could allow modifications of the touch configurations in an unauthorized manner when an attacker attempts to modify the touch configurations.

Schneider Electric Security Notification

CVE ID: **CVE-2022-22810**

CVSS v3.1 Base Score 8.6 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

A *CWE-307: Improper Restriction of Excessive Authentication Attempts* vulnerability exists that could allow an attacker to manipulate the admin after numerous attempts at guessing credentials.

CVE ID: **CVE-2022-22811**

CVSS v3.1 Base Score 9.3 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:H

A *CWE-352: Cross-Site Request Forgery (CSRF)* vulnerability exists that could induce users to perform unintended actions, leading to the override of the system's configurations when an attacker persuades a user to visit a rogue website.

CVE ID: **CVE-2022-22812**

CVSS v3.1 Base Score 9.3 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N

A *CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')* vulnerability exists that could cause a web session compromise when an attacker injects and then executes arbitrary malicious JavaScript code inside the target browser.

Remediations

Affected Product & Version	Remediation
spaceLYnk V2.6.2 and prior	Version 2.7.0 of the spaceLYnk product includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/product/LSS100200/spacelynk-logic-controller/ A reboot is needed after installation.
Wiser for KNX (formerly homeLYnk) V2.6.2 and prior	Version 2.7.0 of the Wiser for KNX product includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/product/LSS100100/wiser-for-knx-logic-controller/ A reboot is needed after installation.
fellerLYnk V2.6.2 and prior	Version 2.7.0 of the fellerLYnk product includes a fix for this vulnerability and is available for download here: https://online-katalog.feller.ch/download/index.php?menueidLev1=279&menueidLev2=662&menueidLev3=664 A reboot is needed after installation.

Schneider Electric Security Notification

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.

If customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit:

- The homeLYnk, spaceLYnk, Wiser For KNX, fellerLYnk products should only be used in your personal home network.
- The homeLYnk, spaceLYnk, Wiser For KNX, fellerLYnk products should not have a publicly accessible IP address.
- Do NOT use port forwarding to access these products from the public internet.
- These products should be on their own network segment. If your router supports a guest network or VLAN, it is preferable to locate the controller there.
- Use the strongest Wi-Fi encryption available.
- Use HTTPs in local network.
- Only visit trusted websites.

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the "Program" mode.
- 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.
- 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.

For more information refer to the Schneider Electric [Recommended Cybersecurity Best Practices](#) document.

Schneider Electric Security Notification

Acknowledgement

Schneider Electric recognizes the following researcher for identifying and helping to coordinate a response to these vulnerabilities:

CVE	Researcher
CVE-2022-22809, CVE-2022-22810, CVE-2022-22811, CVE-2022-22812	Tony Marcel Nasr

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>

LEGAL DISCLAIMER

THIS NOTIFICATION DOCUMENT, THE INFORMATION CONTAINED HEREIN, AND ANY MATERIALS LINKED FROM IT (COLLECTIVELY, THIS "NOTIFICATION") ARE 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 OR GUARANTEE OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES RELATING TO THIS NOTIFICATION, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SCHNEIDER ELECTRIC MAKES NO WARRANTY THAT THE NOTIFICATION WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, 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. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY RESULT FROM YOUR USE OF THIS NOTIFICATION. 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 **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

Schneider Electric Security Notification

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 1.0 <i>08 February 2022</i>	Original Release
Version 1.1 <i>08 March 2022</i>	The CVSS score has been updated for CVE-2022-22811 and CVE-2022-22812