Schneider Electric Security Notification

homeLYnk (Wiser For KNX) and spaceLYnk

11 May 2021

Overview

Schneider Electric is aware of multiple vulnerabilities in its homeLYnk (Wiser For KNX) and spaceLYnk products.

HomeLYnk (Wiser for KNX) products are personalized energy efficiency solutions, offering a complete system based on open protocols: KNX, Modbus, BACnet and IP.

spaceLYnk connects building control functions, thus achieving a complete building management solution for small and medium as well as large buildings.

Failure to apply the remediations and mitigations provided below may risk a variety of attacks, which could result in remote access to the product.

Affected Products and Versions

- homeLYnk (Wiser For KNX) V2.60 and prior
- spaceLYnk V2.60 and prior

Vulnerability Details

CVE ID: **CVE-2021-22732**

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

A *CWE-269: Improper Privilege Management* vulnerability exists that could cause a code execution issue when an attacker loads unauthorized code on the web server.

CVE ID: **CVE-2021-22733**

CVSS v3.1 Base Score 7.2 | High | CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H

A *CWE-269: Improper Privilege Management* vulnerability exists that could cause shell access when unauthorized code is loaded into the system folder.

CVE ID: **CVE-2021-22734**

CVSS v3.1 Base Score 6.8 | Medium | CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H

A *CWE-347: Improper Verification of Cryptographic* Signature vulnerability exists that could cause remote code execution when an attacker loads unauthorized code.

Schneider Electric Security Notification

CVE ID: **CVE-2021-22735**

CVSS v3.1 Base Score 6.8 | Medium | CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H

A *CWE-347: Improper Verification of Cryptographic Signature* vulnerability exists that could allow remote code execution when unauthorized code is copied to the device.

CVE ID: **CVE-2021-22736**

CVSS v3.1 Base Score 5.7 | Medium | CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:H/A:H

A *CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')* vulnerability exists that could cause a denial of service when an unauthorized file is uploaded.

CVE ID: **CVE-2021-22737**

CVSS v3.1 Base Score 5.6 | Medium | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L

A *CWE-522: Insufficiently Protected Credentials* vulnerability exists that could cause unauthorized access of when credentials are discovered after a brute force attack.

CVE ID: **CVE-2021-22738**

CVSS v3.1 Base Score 5.6 | Medium | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L

A *CWE-327: Use of a Broken or Risky Cryptographic Algorithm* vulnerability exists that could cause unauthorized access when credentials are discovered after a brute force attack.

CVE ID: **CVE-2021-22739**

CVSS v3.1 Base Score 5.0 | Medium | CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L

A *CWE-200: Information Exposure* vulnerability exists that could cause a device to be compromised when it is first configured.

CVE ID: **CVE-2021-22740**

CVSS v3.1 Base Score 4.2 | Medium | CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:N/A:N

A *CWE-200: Information Exposure* vulnerability exists that could cause information to be exposed when an unauthorized file is uploaded.

Remediation

CVE	Remediation
CVE-2021-22732 CVE-2021-22734 CVE-2021-22735 CVE-2021-22736 CVE-2021-22739 CVE-2021-22740	Version 2.61 of homeLYnk (Wiser For KNX) and spaceLYnk include a fix for these vulnerabilities and are available for download below: homeLYnk (Wiser For KNX) V2.61 - https://www.se.com/ww/en/product/LSS100100/wiser-for-knx-logic-controller/#pdp-software spaceLYnk V2.61 - https://www.se.com/ww/en/product/LSS100200/spacelynk-logic-controller/#pdp-software Note: Reboot is needed after installation. Please check the version number in the configuration to confirm the update.
CVE-2021-22733 CVE-2021-22737 CVE-2021-22738	Due to hardware limitations, these CVEs will not be fixed and customers should immediately apply the recommendations provided in the System Hardening Guide to reduce the risk of exploit. System Hardening Guide for homeLYnk (Wiser For KNX) : https://download.schneider-electric.com/files?p_Doc_Ref=AN002_107 System Hardening Guide for spaceLYnk: https://download.schneider-electric.com/files?p_Doc_Ref=AN2_107_SL

Customers should use appropriate patching methodologies when applying 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:

- Secure this device to prevent unauthorized personnel from accessing this device
- Use the System Hardening Guides to protect the network and device

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 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 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.

Acknowledgements

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

CVE	Researcher
CVE-2021-22732, CVE-2021-22733, CVE-2021-22734, CVE-2021-22735, CVE-2021-22736, CVE-2021-22737, CVE-2021-22738, CVE-2021-22739, CVE-2021-22740	Sharon Brizinov of Claroty

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 Notification

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.

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 *11 May 2021*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2021.05.08 20:14:06 -04'00'