Schneider Electric Security Notification

Schneider Electric C-Bus Home Automation Products

14 June 2022

Overview

Schneider Electric is aware of multiple vulnerabilities in the Schneider Electric C-Bus Home Automation products listed below.

The Schneider Electric C-Bus Home Automation products are fully integrated systems that can control and automate lighting and many other electrical systems and products.

Failure to apply the remediations provided below may risk unauthorized access, which could allow an unauthorized individual to control the device.

Affected Products and Versions

Product	Version
Schneider Electric C-Bus Network Automation Controller, LSS5500NAC	V1.10.0 and prior
Schneider Electric Wiser for C-Bus Automation Controller, LSS5500SHAC	V1.10.0 and prior
Clipsal C-Bus Network Automation Controller, 5500NAC	V1.10.0 and prior
Clipsal Wiser for C-Bus Automation Controller, 5500SHAC	V1.10.0 and prior
SpaceLogic C-Bus Network Automation Controller, 5500NAC2	V1.10.0 and prior
SpaceLogic C-Bus Application Controller, 5500AC2	V1.10.0 and prior

Vulnerability Details

CVE ID: **CVE-2022-32513**

CVSS v3.1 Base Score 9.8 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A *CWE-521: Weak Password Requirements* vulnerability exists that could allow an attacker to gain control of the device when the attacker brute forces the password.

CVE ID: **CVE-2022-32514**

CVSS v3.1 Base Score 9.8 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A *CWE-287: Improper Authentication* vulnerability exists that could allow an attacker to gain control of the device when logging into a web page.

Remediation

Affected Product & Version	Remediation
Schneider Electric C-Bus Network Automation Controller LSS5500NAC *V1.10.0 and prior*	Version 1.11.0 of Schneider Electric C-Bus Network Automation Controller includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/product/LSS5500NAC/spacelogic-cbus-network-automation-controller-bacnet-modbus-ip-6m-din-mount-24v-dc/ A reboot is required. After logging into the device, go to the configurator page and the firmware version is displayed in the lower left corner.
Schneider Electric Wiser for C-Bus Automation Controller LSS5500SHAC *V1.10.0 and prior*	Version 1.11.0 of Schneider Electric Wiser for C-Bus Automation Controller includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/product/LSS5500SHAC/spacelogic-cbus-automation-controller-rs232-485-ethernet-din-mount-24v-dc/ A reboot is required. After logging into the device, go to the configurator page and the firmware version is displayed in the lower left corner.
Clipsal C-Bus Network Automation Controller 5500NAC *V1.10.0 and prior*	Version 1.11.0 of Clipsal C-Bus Network Automation Controller includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/product/5500NAC/cbus-network-automation-controller-bacnet-modbus-ip-6m-din-mount-24v-dc/ A reboot is required. After logging into the device, go to the configurator page and the firmware version is displayed in the lower left corner.
Clipsal Wiser for C-Bus Automation Controller 5500SHAC *V1.10.0 and prior*	Version 1.11.0 of Clipsal Wiser for C-Bus Automation Controller includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/product/5500SHAC/wiser-for-cbus-automation-controller-rs232-485-ethernet-din-mount-24v-dc/ A reboot is required. After logging into the device, go to the configurator page and the firmware version is displayed in the lower left corner.

SpaceLogic C-Bus Network Automation Controller 5500NAC2 *V1.10.0 and prior*	Version 1.11.0 of SpaceLogic C-Bus Network Automation Controller includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/product/5500NAC2/network-automation-controller-spacelogic-cbus-bacnet-modbus-ip-6m-din-mount-24v-dc/ A reboot is required. After logging into the device, go to the configurator page and the firmware version is displayed in the lower left corner.
SpaceLogic C-Bus Application Controller 5500AC2 *V1.10.0 and prior*	Version 1.11.0 of SpaceLogic C-Bus Application Controller includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/product/5500AC2/application-controller-spacelogic-cbus-rs232-485-ethernet-din-mount-24v-dc/ A reboot is required. After logging into the device, go to the configurator page and the firmware version is displayed in the lower left corner.

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:

- These controller 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.

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

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 *14-June-2022*	Original Release

Product Security Office Digitally signed by Product Security Office
Date: 2022.06.10 17:18:45 -04'00'