Schneider Electric Security Notification

Wiser Home Controller WHC-5918A

9 July 2024

Overview

Schneider Electric is aware of a vulnerability in its Wiser Home Controller WHC-5918A product.

The Wiser Home Controller WHC-5918A, a C-Bus based home automation controller, was discontinued on December 31, 2015.

Failure to apply the mitigations provided below may risk credentials being stolen, which could result in the Wiser Home Controller WHC-5918A being compromised.

Affected Products and Versions

Product	Version
Wiser Home Controller WHC-5918A	All Versions of Wiser Home Controller WHC-5918A

Vulnerability Details

CVE ID: **CVE-2024-6407**

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

CWE-200: Information Exposure vulnerability exists that could cause disclosure of credentials when a specially crafted message is sent to the device.

Note regarding vulnerability details: The severity of vulnerabilities was calculated using the CVSS Base metrics in version 3.1 (CVSS v3.1) without incorporating the Temporal and Environmental metrics. Schneider Electric recommends that customers score the CVSS Environmental metrics, which are specific to end-user organizations, and consider factors such as the presence of mitigations in that environment. Environmental metrics may refine the relative severity posed by the vulnerabilities described in this document within a customer's environment.

Affected Product	Mitigations
Wiser Home Controller WHC-5918A	The Wiser Home Controller WHC-5918A product has been discontinued and is out of support. Customers should consider upgrading to the latest product offering, C-Bus, Home Controller, SpaceLogic IP, Free Standing, 24V DC, 5200WHC2, or removing the Wiser Home Controller WHC-5918A from service.

Schneider Electric Security Notification

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Passwords should include upper case, lower case, number and special characters, a length of 20 characters is ideal.
- A default Admin password must be changed immediately when first received and after a factory reset.
- Device should only be used in a personal home network.
- Device should not have a publicly accessible IP address.
- Do NOT use port forwarding to access a device from the public internet.
- A device should be on its own network segment. If your router supports a guest network or VLAN, it is preferable to locate the device there.
- Use the strongest Wi-Fi encryption available, such as WPA3 or WPA2/3 with protected management frames.
- Schedule regular reboots of your routing device, smartphones, and computers.
- Ensure that unauthorized individuals cannot gain physical access to your devices (USB or LAN ports should be easily accessible.

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

Schneider Electric Security Notification

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 **create Impact** by empowering 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 the trusted partner in **Sustainability and Efficiency.**

We are a **global industrial technology leader** bringing world-leading expertise in electrification, automation and digitization to smart **industries**, resilient **infrastructure**, future-proof **data centers**, intelligent **buildings**, and intuitive **homes**. Anchored by our deep domain expertise, we provide integrated end-to-end lifecycle AI enabled Industrial IoT solutions with connected products, automation, software and services, delivering digital twins to enable profitable growth **for our customers.**

We are a **people company** with an ecosystem of 150,000 colleagues and more than a million partners operating in over 100 countries to ensure proximity to our customers and stakeholders. We embrace **diversity and inclusion** in everything we do, guided by our meaningful purpose of a **sustainable future for all**.

www.se.com

Revision Control:

Version 1.0.0 *09 July 2024*	Original Release

CPCERT

Digitally signed by CPCERT
Date: 2024.07.08 13:06:16 -04'00'