Schneider Electric Security Notification

Wiser Smart

10 May 2022

Overview

Schneider Electric is aware of multiple vulnerabilities in its Wiser Smart products.

Wiser Smart is a home automation system which reports your energy consumption and controls the most energy consuming devices.

Failure to apply the mitigations provided below may risk root level access attack, which could result in execution of arbitrary code.

Affected Products and Versions

Product	Version
Wiser Smart, EER21000	V4.5 and prior
Wiser Smart, EER21001	V4.5 and prior

Vulnerability Details

CVE ID: **CVE-2022-30234**

CVSS v3.1 Base Score 9.4 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

A *CWE-798: Use of Hard-coded Credentials* vulnerability exists that could allow arbitrary code to be executed when root level access is obtained.

CVE ID: **CVE-2022-30235**

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 unauthorized access when an attacker uses brute force.

CVE ID: **CVE-2022-30238**

CVSS v3.1 Base Score 8.3 | High | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L

A *CWE-287: Improper Authentication* vulnerability exists that could allow an attacker to take over the admin account when an attacker hijacks a session.

Schneider Electric Security Notification

CVE ID: **CVE-2022-30236**

CVSS v3.1 Base Score 8.2 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

A *CWE-669: Incorrect Resource Transfer Between Spheres* vulnerability exists that could allow unauthorized access when an attacker uses cross-domain attacks.

CVE ID: **CVE-2022-30237**

CVSS v3.1 Base Score 8.2 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

A *CWE-311: Missing Encryption of Sensitive Data* vulnerability exists that could allow authentication credentials to be recovered when an attacker breaks the encoding.

CVE ID: **CVE-2022-30233**

CVSS v3.1 Base Score 6.5| Medium | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

A *CWE-20: Improper Input Validation* vulnerability exists that could allow the product to be maliciously manipulated when the user is tricked into performing certain actions on a webpage.

Mitigations

<table>
<tr><th>Affected Product & Version</th><th>Mitigation</th></tr>
<tr><td>Wiser Smart, EER21000

V4.5 and prior</td><td rowspan="2">Wiser Smart EER21000 and EER21001 have reached end of life and are no longer supported. Customers should immediately apply the following mitigations to reduce the risk of exploit:
These controller products should not have a publicly or Internet 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 VLAN, it is preferable to locate the controller there.
Use the strongest Wi-Fi encryption available.
Never re-use passwords.
Use HTTPS in local network.
Only visit trusted websites.</td></tr>
<tr><td>Wiser Smart, EER21001

V4.5 and prior</td></tr>
</table>

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.

Acknowledgements

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

CVE	Researcher
CVE-2022-30234, CVE-2022-30235, CVE-2022-30236, CVE-2022-30237, CVE-2022-30238, CVE-2022-30233	Tony 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

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

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 *10 May 2022*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2022.05.08 13:36:37 -07'00'