Schneider Electric Security Notification

EcoStruxure™ Power Operation 2021, EcoStruxure™ Power SCADA Operation 2020 and EcoStruxure™ Power SCADA Operation 2020 R2

11 October 2022 (14 October 2022)

Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure™ Power Operation and Power SCADA Operation software.

[EcoStruxure™ Power Operation and EcoStructure™ Power SCADA Operation](#) are on-premises software offers that provides a single platform to monitor and control medium and lower power systems.

Failure to apply the remediation provided below may risk result in a loss of data confidentiality, data integrity issues, or a loss of access to the server.

14 October 2022 Update: There is an update to the EcoStruxure™ Power SCADA Operation 2020 remediation advising customers to move to 2020 R2 instead of 2020 CU2.

Affected Product and Versions

Product	Version
EcoStruxure™ Power SCADA Operation 2020	Version 2020 and 2020 CU1
EcoStruxure™ Power SCADA Operation 2020 R2	Version 2020 R2 Prior to CU1
EcoStruxure™ Power Operation 2021	Version 2021, 2021 CU1 and 2021 CU2

Vulnerability Details

CVE ID: **CVE-2022-22727**

CVSS v3.1 Base Score 7.1 | High | CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:H/A:H

A *CWE-20: Improper Input Validation* vulnerability exists that could allow an unauthenticated attacker to view data, change settings, impact availability of the software, or potentially impact a user's local machine when the user clicks a specially crafted link.

Remediations

Affected Product & Version	Remediation
EcoStruxure™ Power SCADA Operation 2020 *Version 2020 and 2020 CU1*	Power SCADA Operation 2020 R2 Cumulative Update 1 (CU1) or newer, if available, includes a fix for this vulnerability and is available for download here: https://community.exchange.se.com/t5/EcoStruxure-Power-Operation/Downloads-Installers-Cumulative-Updates-and-Drivers/td-p/152169 **Please note**: these updates are made available through the Schneider Electric Exchange community. If you are unable to access this service, please contact Schneider Electric Customer Care Center for assistance in accessing these updates.
EcoStruxure™ Power SCADA Operation 2020 R2 *Version 2020 R2 Prior to CU1*	Power SCADA Operation 2020 R2 Cumulative Update 1 (CU1) or newer, if available, includes a fix for this vulnerability and is available for download here: https://community.exchange.se.com/t5/EcoStruxure-Power-Operation/Downloads-Installers-Cumulative-Updates-and-Drivers/td-p/152169 **Please note**: these updates are made available through the Schneider Electric Exchange community. If you are unable to access this service, please contact Schneider Electric Customer Care Center for assistance in accessing these updates.
EcoStruxure™ Power Operation 2021 *Version 2021, 2021 CU1 and 2021 CU2*	Power Operation 2021 Cumulative Update 3 (CU3) or newer, if available, includes a fix for this vulnerability and is available for download here: https://community.exchange.se.com/t5/EcoStruxure-Power-Operation/Downloads-Installers-Cumulative-Updates-and-Drivers/td-p/152169 **Please note**: these updates are made available through the Schneider Electric Exchange community. If you are unable to access this service, please contact Schneider Electric Customer Care Center for assistance in accessing these updates.

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.

Schneider Electric Security Notification

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 this vulnerability:

CVE	Researcher
CVE-2022-22727	U.S. Department of Energy CyTRICS researcher Robert Erbes – INL

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

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 *11 October 2022*	Original Release
Version 1.1 *14 October 2022*	There is an update to the EcoStruxure™ Power SCADA Operation 2020 remediation advising customers to move to 2020 R2 instead of 2020 CU2.