# Schneider Electric Security Notification

## EcoStruxure Power Monitoring Expert and EcoStruxure™ Power Operation with Advanced Reports

**10 October 2023**

## Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure™ Power Monitoring Expert (PME) and EcoStruxure™ Power Operation products.

EcoStruxure™ Power Monitoring Expert (PME) is an on-premises software used to help power critical and energy-intensive facilities maximize uptime and operational efficiency.

EcoStruxure™ Power Operation and EcoStruxure™ Power SCADA Operation with Advanced Reports are on-premises software offers that provides a single platform to monitor and control medium and lower power systems.

Failure to apply the remediations provided below may risk a remote code execution attack, which could result in an attacker gaining access and/or control of the targeted system.

## Affected Products and Versions

| Product | Version |
|---|---|
| EcoStruxure™ Power Monitoring Expert (PME) | *All versions – prior to application of Hotfix-145271* |
| EcoStruxure™ Power Operation (EPO) with Advanced Reports<br><br>EcoStruxure™ Power SCADA Operation with Advanced Reports | *All versions – prior to application of Hotfix-145271*<br><br>Note: Power SCADA Operation and Power Operation without Advanced Reports are not affected. |

## Vulnerability Details

CVE ID: **CVE-2023-5391**

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-502: Deserialization of untrusted data* vulnerability exists that could allow an attacker to execute arbitrary code on the targeted system by sending a specifically crafted packet to the application.

*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.*

## Remediation

| Affected Product & Version | Remediation |
|---|---|
| **EcoStruxure™ Power Monitoring Expert (PME)** *All versions prior to the application of Hotfix-145271* | A Hotfix for this vulnerability is available by contacting Contact Schneider Electric's Customer Care Center. The Hotfix can be applied to versions PME 2023, 2022, and 2021, the versions currently in support on the date of this disclosure. Previous versions, please contact customer care to inquire about upgrade paths. |
| **EcoStruxure™ Power Operation (EPO) with Advanced Reports and EcoStruxure™ Power SCADA Operation with Advanced Reports** *All versions prior to the application of Hotfix-145271* | A Hotfix for this vulnerability is available by contacting Contact Schneider Electric's Customer Care Center. The Hotfix can be applied to versions EPO 2022, and 2021, the versions currently in support on the date of this disclosure. Previous versions, please contact customer care to inquire about upgrade paths. |

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:

- Deploy allowlisting/whitelisting strategies to ensure only approved IP addresses can communicate with your PME or EPO system.

## 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-2023-5391 | Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam) working with Trend Micro Zero Day Initiative |

## 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

"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**<br>*10 October 2023* | Original Release |

Product Security Office

Digitally signed by Product Security Office
Date: 2023.10.09 08:39:24 -04'00'