

# Schneider Electric Security Notification

## Deserialization of Untrusted Data vulnerability on Multiple Products

10 March 2026

### Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure™ Power Monitoring Expert (PME) and EcoStruxure™ Power Operation (EPO) 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 \(EPO\)](#) are on-premises software offers that provides a single platform to monitor and control medium and lower power systems.

Failure to apply the fix provided below may risk local arbitrary code execution, which could result in the local system being compromised, a disruption of operations, and/or unauthorized administrative control of the system.

### Affected Products and Versions

Product	Version
EcoStruxure™ Power Monitoring Expert (PME)	Version 2022 Version 2023 Version 2023 R2 Version 2024 Version 2024 R2
EcoStruxure™ Power Operation (EPO) Advanced Reporting and Dashboards Module	Version 2022 Version 2024

### Vulnerability Details

CVE ID: **CVE-2025-11739**

CVSS v3.1 Base Score 7.8 | High | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Base Score 8.5 | High | CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

*CWE-502: Deserialization of Untrusted Data* vulnerability exists that could cause arbitrary code execution with administrative privileges when a locally authenticated attacker sends a crafted data stream, triggering unsafe deserialization.

*The severity of vulnerabilities was calculated using the CVSS Base metrics for 4.0 ([CVSS v4.0](#)). CVSS v3.1 will be still evaluated until the adoption of CVSS v4.0 by the industry. The severity was calculated 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*

## Schneider Electric Security Notification

*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
<b>EcoStruxure™ Power Monitoring Expert 2024</b> <i>Versions PME 2024 R2</i>	Hotfix_279338_Release_2024R2 is available for EcoStruxure™ Power Monitoring Expert (PME) that includes a fix for this vulnerability.  Contact Schneider Electric's Customer Care Center to download this hotfix  No reboot required.
<b>EcoStruxure™ Power Monitoring Expert 2024</b> <i>Versions PME 2024</i>	Customers should upgrade to EcoStruxure™ Power Monitoring Expert (PME) 2024 R3.  Contact Schneider Electric's Customer Care Center for assistance.
<b>EcoStruxure™ Power Monitoring Expert 2023</b> <i>Versions PME 2023 R2</i>	Hotfix_282807 - for 2023R2 is available for EcoStruxure™ Power Monitoring Expert (PME) that includes a fix for this vulnerability.  Contact Schneider Electric's Customer Care Center to download this hotfix  No reboot required.
<b>EcoStruxure™ Power Monitoring Expert 2024</b> <i>Versions PME 2023</i>	Customers should upgrade to EcoStruxure™ Power Monitoring Expert (PME) 2023 R2. Once upgraded, Hotfix_282807 - for 2023R2 is available for EcoStruxure™ Power Monitoring Expert (PME) that includes a fix for this vulnerability.  Contact Schneider Electric's Customer Care Center for assistance.
<b>EcoStruxure™ Power Operation (EPO) 2024 with Advanced Reporting and Dashboards Module</b> <i>Version 2024</i>	Customers should upgrade to EcoStruxure™ Power Monitoring Expert (PME) 2023 R2. Once upgraded, Hotfix_282807 - for 2023R2 is available for EcoStruxure™ Power Monitoring Expert (PME) that includes a fix for this vulnerability.  Contact Schneider Electric's Customer Care Center for assistance.

NOTE: EcoStruxure™ Power Operation 2022 with Advanced Reporting AND EcoStruxure™ Power Operation 2024 with Advanced Reporting utilizes EcoStruxure™ Power Monitoring Expert. You must update EcoStruxure™ Power Monitoring Expert separately from EcoStruxure™ Power Operation and apply the appropriate update for Power Monitoring Expert as described above.

## Schneider Electric Security Notification

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:

### Mitigations

Affected Product & Version	Mitigations
<b>EcoStruxure™ Power Monitoring Expert 2022</b> <i>Versions PME 2022 and prior</i>	<p>EcoStruxure™ Power Monitoring Expert (PME) 2022 version has reached its end of life and is no longer supported.</p> <ul style="list-style-type: none"><li>• Ensure your deployment of PME has followed the cybersecurity hardening guidelines provided with the product: <a href="https://product-help.schneider-electric.com/EcoStruxure/Power-Monitoring-Expert-2024/content/2_planning/cybersecurity/cyber-planningrecactions.htm">https://product-help.schneider-electric.com/EcoStruxure/Power-Monitoring-Expert-2024/content/2_planning/cybersecurity/cyber-planningrecactions.htm</a></li><li>• Ensure PME is running in an isolated network • Deploy and configure the Windows firewall to limit access to appropriate network segments</li><li>• Enforce complex password policies.<ul style="list-style-type: none"><li>○ Review Server Access Permissions</li><li>○ Conduct an audit of all Windows-authenticated users who currently have access to PME. Repeat this audit of your system periodically.</li><li>○ Identify all accounts with access rights, especially those with elevated privileges or remote access.</li><li>○ Limit access to essential users only.</li><li>○ Revoke access for any user accounts that are not critical for system functionality or daily operations.</li><li>○ Apply the principle of least privilege to ensure users have only the access necessary for their role(s).</li></ul></li></ul> <p>Customers should also consider upgrading to the latest product offering EcoStruxure™ Power Monitoring Expert (PME) 2024 R3 to resolve this issue.</p>

## Schneider Electric Security Notification

<p><b>EcoStruxure™ Power Operation (EPO) 2022 with Advanced Reporting and Dashboards Module</b> Version 2022 and prior</p>	<p>EcoStruxure™ Power Operation (EPO) 2022 version and EcoStruxure™ Power Monitoring Expert (PME) 2022 has reached its end of life and is no longer supported.</p> <ul style="list-style-type: none"> <li>• Ensure your deployment of PME has followed the cybersecurity hardening guidelines provided with the product: <a href="https://product-help.schneider-electric.com/EcoStruxure/Power-Monitoring-Expert-2024/content/2_planning/cybersecurity/cyber-planningrecactions.htm">https://product-help.schneider-electric.com/EcoStruxure/Power-Monitoring-Expert-2024/content/2_planning/cybersecurity/cyber-planningrecactions.htm</a></li> <li>• Ensure PME is running in an isolated network • Deploy and configure the Windows firewall to limit access to appropriate network segments</li> <li>• Enforce complex password policies. <ul style="list-style-type: none"> <li>○ Review Server Access Permissions</li> <li>○ Conduct an audit of all Windows-authenticated users who currently have access to PME. Repeat this audit of your system periodically.</li> <li>○ Identify all accounts with access rights, especially those with elevated privileges or remote access.</li> <li>○ Limit access to essential users only.</li> <li>○ Revoke access for any user accounts that are not critical for system functionality or daily operations.</li> <li>○ Apply the principle of least privilege to ensure users have only the access necessary for their role(s).</li> </ul> </li> </ul> <p>Customers should also consider upgrading to the latest product offering EcoStruxure™ Power Monitoring Expert (PME) 2024 R3 to resolve this issue.</p>
--	---

To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric's security notification service here:

<https://www.se.com/en/work/support/cybersecurity/notification-contact.jsp>

## 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.

## Schneider Electric Security Notification

- 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 researchers for identifying and helping to coordinate a response to this vulnerability:

CVE	Researchers
CVE-2025-11739	CNCERT

### 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

## Schneider Electric Security Notification

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](http://www.se.com)

Revision Control:

<b>Version 1.0.0</b> 10 March 2026	Original Release
---------------------------------------	------------------