

Schneider Electric Security Notification

EcoStruxure™ Power Monitoring Expert Software & EcoStruxure™ Power Operation (EPO) and EcoStruxure™ Power SCADA Operation (PSO)

12 August 2025 (11 November 2025)

Overview

Schneider Electric is aware of multiple vulnerabilities in its EcoStruxure™ Power Monitoring Expert (PME) and EcoStruxure™ Power Operation (EPO) and EcoStruxure™ Power SCADA Operation (PSO) 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. Note: There are some instances of PME being deployed in a Managed Service model.

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

Failure to apply the remediation and/or mitigations provided below may risk deserialization of untrusted data, server-side request forgery and/or path traversal that could result in remote code execution, and/or unauthorized access to sensitive data.

November 2025 Update: Updated Affected Products and Version section to include PME 2023 R2. Updated the impacting CVEs for PME 2022, 2023, and 2023 R2. There have been remediation updates made for PME 2023, and 2023 R2.

Affected Products and Versions

Product	Version	Impacting CVEs
EcoStruxure™ Power Monitoring Expert (PME)	Version 2024 Version 2024 R2	CVE-2025-54924 CVE-2025-54925 CVE-2025-54926 CVE-2025-54927 CVE-2025-54923
EcoStruxure™ Power Monitoring Expert (PME)	Version 2022 Version 2023 Version 2023 R2	CVE-2025-54924 CVE-2025-54925 CVE-2025-54927
EcoStruxure™ Power Operation (EPO) Advanced Reporting and Dashboards Module	Version 2022 w/ Advanced Reporting Module Version 2024 w/ Advanced Reporting Module	CVEs impacting EPO dependent on version of Advance Dashboard running

Schneider Electric Security Notification

Vulnerability Details

CVE ID: **CVE-2025-54923**

CVSS v3.1 Base Score 8.8 | High | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Base Score 8.7 | High | CVSS:4.0/AV:N/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 remote code execution and compromise of system integrity when authenticated users send crafted data to a network-exposed service that performs unsafe deserialization.

CVE ID: **CVE-2025-54924**

CVSS v3.1 Base Score 7.5 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v4.0 Base Score 8.7 | High | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

CWE-918: Server-Side Request Forgery (SSRF) vulnerability exists that could cause unauthorized access to sensitive data when an attacker sends a specially crafted document to a vulnerable endpoint.

CVE ID: **CVE-2025-54925**

CVSS v3.1 Base Score 7.5 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v4.0 Base Score 8.7 | High | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

CWE-918: Server-Side Request Forgery (SSRF) vulnerability exists that could cause unauthorized access to sensitive data when an attacker configures the application to access a malicious url.

CVE ID: **CVE-2025-54926**

CVSS v3.1 Base Score 7.2 | High | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Base Score 8.6 | High | CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could cause remote code execution when an authenticated attacker with admin privileges uploads a malicious file over HTTP which then gets executed.

CVE ID: **CVE-2025-54927**

CVSS v3.1 Base Score 4.9 | Medium | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

CVSS v4.0 Base Score 6.9 | High | CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could cause unauthorized access to sensitive files when an authenticated attackers uses a crafted path input that is processed by the system.

Schneider Electric Security Notification

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 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.

Remediations

Affected Product & Version	Remediations
EcoStruxure™ Power Monitoring Expert (PME) 2024 R2	<p>Hotfix_279338_Release_2024R2 is available for EcoStruxure™ Power Monitoring Expert (PME) 2024 R2 that includes a fix for the vulnerabilities CVE-2025-54924, CVE-2025-54925, CVE-2025-54926, CVE-2025-54927 and CVE-2025-54923.</p> <p>Contact Schneider Electric's Customer Care Center for assistance applying this hotfix.</p> <p>In addition to applying the hotfixes noted above, you are encouraged to review the mitigations listed below.</p>
EcoStruxure™ Power Monitoring Expert (PME) 2024	<p>Customers should upgrade to the latest product offering EcoStruxure™ Power Monitoring Expert (PME) 2024 R2 and apply Hotfix_279338_Release_2024R2 that includes a fix for the vulnerabilities CVE-2025-54924, CVE-2025-54925, CVE-2025-54926, CVE-2025-54927 and CVE-2025-54923.</p> <p>Contact Schneider Electric's Customer Care Center for assistance with obtaining EcoStruxure™ Power Monitoring Expert (PME) 2024 R2 and help applying this hotfix.</p> <p>In addition to applying the hotfix noted above, you are encouraged to review the mitigations listed below.</p>
EcoStruxure™ Power Monitoring Expert (PME) 2023 R2	<p>Hotfix_199767_release and Hotfix_273686_release.12.0 are available for EcoStruxure™ Power Monitoring Expert (PME) that includes a fix for the vulnerabilities CVE-2025-54924, CVE-2025-54925, and CVE-2025-54927.</p> <p>Contact Schneider Electric's Customer Care Center for assistance applying these hotfixes.</p> <p>In addition to applying the hotfixes noted above, you are encouraged to review the mitigations listed below.</p>

Schneider Electric Security Notification

EcoStruxure™ Power Monitoring Expert (PME) 2023	<p>Customers should upgrade to EcoStruxure™ Power Monitoring Expert (PME) 2023 R2 and apply Hotfix_199767_release and Hotfix_273686_release.12.0 that includes a fix for the vulnerabilities CVE-2025-54924, CVE-2025-54925, and CVE-2025-54927.</p> <p>Contact Schneider Electric's Customer Care Center for assistance applying these hotfixes.</p> <p>In addition to applying the hotfixes noted above, you are encouraged to review the mitigations listed below.</p>
EcoStruxure™ Power Operation (EPO) 2024 w/ Advanced Reporting and Dashboards Module	<p>Hotfix_279338_Release_2024R2 is available for EcoStruxure™ Power Monitoring Expert (PME) 2024 R2 that includes a fix for the vulnerabilities CVE-2025-54924, CVE-2025-54925, CVE-2025-54926, CVE-2025-54927 and CVE-2025-54923.</p> <p>Contact Schneider Electric's Customer Care Center to determine if you are running EcoStruxure™ Power Monitoring Expert (PME) 2024 R2 as part of your solution. Customers running this version of PME can work with Schneider Electric's Customer Care Center for assistance applying this hotfix.</p> <p>OR</p> <p>Contact Schneider Electric's Customer Care Center to determine if you are running EcoStruxure™ Power Monitoring Expert (PME) 2024 as part of your solution. Customers running this version of PME can work with Schneider Electric's Customer Care Center for assistance upgrading to EcoStruxure™ Power Monitoring Expert (PME) 2024 R2 and then help applying the hotfix.</p>
EcoStruxure™ Power Operation (EPO) 2022 w/ Advanced Reporting and Dashboards Module	<p>Hotfix_279338_Release_2024R2 is available for EcoStruxure™ Power Monitoring Expert (PME) 2024 R2 that includes a fix for the vulnerabilities CVE-2025-54924, CVE-2025-54925, CVE-2025-54926, CVE-2025-54927 and CVE-2025-54923.</p> <p>Contact Schneider Electric's Customer Care Center to determine if you are running EcoStruxure™ Power Monitoring Expert (PME) 2024 R2 as part of your solution. Customers running this version of PME can work with Schneider Electric's Customer Care Center for assistance applying this hotfix.</p> <p>OR</p> <p>Contact Schneider Electric's Customer Care Center to determine if you are running EcoStruxure™ Power Monitoring Expert (PME) 2024 as part of your solution. Customers running this version of PME can work with Schneider Electric's Customer Care Center for assistance upgrading to EcoStruxure™ Power Monitoring Expert (PME) 2024 R2 and then help applying the hotfix.</p>

Schneider Electric Security Notification

<p>EcoStruxure™ Power Operation (EPO) 2022 w/ Advanced Reporting and Dashboards Module</p>	<p>Hotfix_199767_release and Hotfix_273686_release.12.0 is available for EcoStruxure™ Power Monitoring Expert (PME) 2023R2 that includes a fix for the vulnerabilities CVE-2025-54924, CVE-2025-54925, and CVE-2025-54927.</p> <p>Contact Schneider Electric's Customer Care Center to determine if you are running EcoStruxure™ Power Monitoring Expert (PME) 2023R2 as part of your solution. Customers running this version of PME can work with Schneider Electric's Customer Care Center for assistance applying this hotfix.</p> <p>OR</p> <p>Contact Schneider Electric's Customer Care Center to determine if you are running EcoStruxure™ Power Monitoring Expert (PME) 2023 as part of your solution. Customers running this version of PME can work with Schneider Electric's Customer Care Center for assistance upgrading to EcoStruxure™ Power Monitoring Expert (PME) 2023 R2 and then help applying the hotfix.</p>
---	---

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

Contact Schneider Electric's Customer Care Center for assistance applying these hotfixes.

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:

- Ensure your deployment of PME has followed the cybersecurity hardening guidelines provided with the product. https://product-help.schneider-electric.com/EcoStruxure/Power-Monitoring-Expert-2024/content/2_planning/cybersecurity/cyber-planningrecactions.htm
- Ensure PME is running in an isolated network.
- Deploy and configure the Windows firewall to limit access to appropriate network segments.
- Enforce complex password policies.
- Review Server Access Permissions:
 - Conduct an audit of all Windows-authenticated users who currently have access to PME. Repeat this audit of your system periodically.
 - Identify all accounts with access rights, especially those with elevated privileges or remote access.

Schneider Electric Security Notification

- Limit access to essential users.
- Revoke access for any user accounts that are not critical for system functionality or day-to-day operations.
- Apply the principle of least privilege to ensure users have only the access needed for their role.

Mitigations

Affected Product & Version	Mitigations
EcoStruxure™ Power Monitoring Expert (PME) 2022	<p>EcoStruxure™ Power Monitoring Expert (PME) 2022 version has reached its end of life and is no longer supported. Customers should immediately apply the following mitigations to reduce the risk of exploit for CVE-2025-54924, CVE-2025-54925, and CVE-2025-54927:</p> <ul style="list-style-type: none"> • Ensure your deployment of PME has followed the cybersecurity hardening guidelines provided with the product. https://product-help.schneider-electric.com/EcoStruxure/Power-Monitoring-Expert-2024/content/2_planning/cybersecurity/cyber-planningrecactions.htm • Ensure PME is running in an isolated network • Deploy and configure the Windows firewall to limit access to appropriate network segments. • Enforce complex password policies. • Review Server Access Permissions <ul style="list-style-type: none"> • Conduct an audit of all Windows-authenticated users who currently have access to PME. Repeat this audit of your system periodically. • Identify all accounts with access rights, especially those with elevated privileges or remote access. • Limit access to essential users only. • Revoke access for any user accounts that are not critical for system functionality or daily operations. • Apply the principle of least privilege to ensure users have only the access necessary for their role(s). <p>Customers should also consider upgrading to the latest product offering EcoStruxure™ Power Monitoring Expert (PME) 2024 R2 to resolve this issue.</p>

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

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/security-notifications.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.
- 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-2025-54923 CVE-2025-54924 CVE-2025-54925 CVE-2025-54926 CVE-2025-54927	ZDI - Trend Micro Initiative

Schneider Electric Security Notification

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 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

Schneider Electric Security Notification

Revision Control:

Version 1.0.0 <i>12 August 2025</i>	Original Release
Version 2.0.0 <i>14 October 2025</i>	Remediations are now available for all impacting CVEs listed below for EcoStruxure™ Power Monitoring Expert (PME) 2023 & 2024 & 2024R2 and EcoStruxure™ Power Operation (EPO) 2022 & 2024 w/ Advanced Reporting and Dashboards Module. After further investigation, CVE-2025-54923 and CVE-2025-54925 do not impact EcoStruxure™ Power Monitoring Expert (PME) 2023 and prior.
Version 3.0.0 <i>11 November 2025</i>	Updated Affected Products and Version section to include PME 2023 R2. Updated the impacting CVEs for PME 2022, 2023, and 2023 R2. There have been remediation updates made for PME 2023, and 2023 R2.