Schneider Electric Security Notification

EcoStruxure™ Power Monitoring Expert and EcoStruxure™ Power Operation or EcoStruxure™ Power SCADA Operation with Advanced Reporting and Dashboards

10 September 2024

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) 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 remediations provided below could result in execution of malicious web code, or unintended software operation.

Affected Products and Versions

Product	Version
EcoStruxure™ Power Monitoring Expert (PME) 2021	EcoStruxure™ Power Monitoring Expert 2021 CU1 and prior
EcoStruxure™ Power Monitoring Expert (PME) 2020	EcoStruxure™ Power Monitoring Expert 2020 CU3 and prior
EcoStruxure™ Power Operation (EPO) 2022	EcoStruxure™ Power Operation 2022 CU4 and prior
EcoStruxure™ Power Operation (EPO) 2022 – Advanced Reporting and Dashboards Module	EcoStruxure™ Power Operation 2022 CU4 and prior NOTE: EcoStruxure™ Power Operation 2022 with Advanced Reporting AND EcoStruxure™ Power Operation 2021 with Advanced Reporting utilizes EcoStruxure™ Power Monitoring Expert.

Schneider Electric Security Notification

	You will need to update the version of EcoStruxure™ Power Monitoring Expert installed independently of the EcoStruxure™ Power Operation patch level installed and apply the appropriate EcoStruxure™ Power Monitoring Expert update as outlined above. For assistance in determining the version of PME installed, contact the Schneider Electric Customer Care Center.
EcoStruxure™ Power Operation (EPO) 2021	EcoStruxure™ Power Operation 2021 CU3 with Hotfix 2 and prior
EcoStruxure™ Power Operation (EPO) 2021 – Advanced Reporting and Dashboards Module	EcoStruxure™ Power Operation 2021 CU3 with Hotfix 2 and prior NOTE: EcoStruxure™ Power Operation 2022 with Advanced Reporting AND EcoStruxure™ Power Operation 2021 with Advanced Reporting utilizes EcoStruxure™ Power Monitoring Expert. You will need to update the version of EcoStruxure™ Power Monitoring Expert installed independently of the EcoStruxure™ Power Operation patch level installed and apply the appropriate EcoStruxure™ Power Monitoring Expert update as outlined above. For assistance in determining the version of PME installed, contact the Schneider Electric Customer Care Center.
EcoStruxure™ Power SCADA Operation 2020 (PSO) - Advanced Reporting and Dashboards Module	All versions

Schneider Electric Security Notification

Vulnerability Details

CVE ID: **CVE-2024-8401**

CVSS v3.1 Base Score 5.4 | Medium | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists when an authenticated attacker modifies folder names within the context of the product.

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 *2021 CU1 and prior*	EcoStruxure™ Power Monitoring Expert 2021 CU2 includes a fix for this vulnerability and is available for download here: https://ecoxpert.se.com/software-center/power-monitoring-expert/power-monitoring-expert-2021 OR EcoStruxure™ Power Monitoring Expert 2022 includes a fix for this vulnerability and is available for download here: https://ecoxpert.se.com/software-center/power-monitoring-expert/power-monitoring-expert-2022 OR Upgrade to the latest version of EcoStruxure™ Power Monitoring Expert. Contact the customer care center for more information.
EcoStruxure™ Power Operation (EPO) 2022 *CU4 and prior*	EcoStruxure™ Power Operations 2022 CU5 includes a fix for this vulnerability and is available for download here: https://community.se.com/t5/EcoStruxure-Power-Operation/v2022-Release-amp-Updates-Install-Procedure/m-p/416561/thread-id/6058 OR

	Upgrade to latest version of EcoStruxure™ Power Operations. Contact the customer care center for more information. Additionally, EcoStruxure™ Power operation 2022 with Advanced Reporting utilizes EcoStruxure™ Power Monitoring Expert. You will need to update the version of EcoStruxure™ Power Monitoring Expert installed independently of the EcoStruxure™ Power Operation patch level installed and apply the appropriate EcoStruxure™ Power Monitoring Expert update as outlined above.
EcoStruxure™ Power Operation (EPO) 2021 *CU3 Hotfix 2 and prior*	EcoStruxure™ Power Operations 2021 CU3 Hotfix 3 includes a fix for this vulnerability and is available for download here: https://community.se.com/t5/EcoStruxure-Power-Operation/v2021-Release-amp-Updates-Install-Procedure/td-p/358628 OR Upgrade to latest version of EcoStruxure™ Power Operations. Contact the customer care center for more information. Additionally, EcoStruxure™ Power Operation 2021 with Advanced Reporting utilizes EcoStruxure™ Power Monitoring Expert. You will need to update the version of EcoStruxure™ Power Monitoring Expert installed independently of the EcoStruxure™ Power Operation patch level installed and apply the appropriate EcoStruxure™ Power Monitoring Expert update as outlined above.

Mitigation

Affected Product & Version	Mitigations
EcoStruxure™ Power Monitoring Expert *2020*	EcoStruxure™ Power Monitoring Expert 2020 is at its end-of-life support. Customers should consider upgrading to the latest version offering of PME to resolve this issue. Please contact Schneider Electric Customer Care Center for more details.
EcoStruxure™ Power SCADA Operation 2020 (PSO) - Advanced Reporting and Dashboards Module	EcoStruxure™ Power SCADA Operation 2020 (PSO) - Advanced Reporting and Dashboards Module is at its end-of-life support. Customers should consider upgrading to the latest version offering of EPO to resolve this issue. Please contact Schneider Electric Customer Care Center for more details.

Schneider Electric Security Notification

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.

If customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit:

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:

Schneider Electric Security Notification

CVE	Researcher
CVE-2024-8401	McKade Umbenhower, Sandia National Labs

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.

Schneider Electric Security Notification

www.se.com

Revision Control:

Version 1.0.0 *10 September 2024*	Original Release

CPCERT

Digitally signed by CPCERT
Date: 2024.09.09 12:21:43 -04'00'