Life Is On | Schneider Electric

Schneider Electric Security Notification

EcoStruxure Power Monitoring Expert and EcoStruxure™ Power Operation with Advanced Reporting and Dashboards Module

14 November 2023

Overview

Schneider Electric is aware of multiple vulnerabilities in its EcoStruxure™ Power Monitoring Expert (PME) product, EcoStruxure™ Power Operation (EPO) and EcoStruxure™ Power SCADA Operation (PSO) - Advanced Reporting and Dashboards Module.

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 remediation provided below may risk a Cross Site Scripting or an open redirect attack which could result in an account takeover scenario or the execution of code in the user browser.

Affected Products and Versions

Product	Version
EcoStruxure™ Power Monitoring Expert (PME)	EcoStruxure™ Power Monitoring Expert (PME) 2021 prior to CU2 EcoStruxure™ Power Monitoring Expert (PME) 2020 prior to CU3
EcoStruxure™ Power Operation (EPO) – Advanced Reporting and Dashboards Module EcoStruxure™ Power SCADA Operation (PSO) - Advanced Reporting and Dashboards Module	Advanced Reporting and Dashboards Module 2021 prior to CU2 for EcoStruxure™ Power Operation 2021 Advanced Reporting and Dashboards Module 2020 prior to CU3 EcoStruxure™ Power SCADA Operation (PSO) 2020 or 2020 R2 ***Note 1:*** *Power SCADA Operation and Power Operation without the Advanced Reporting and Dashboards Module are not affected.* ***Note 2:*** *Advanced Reporting and Dashboards Module is equivalent to EcoStruxure™ Power Monitoring Expert.*

Vulnerability Details

CVE ID: **CVE-2023-5986**

CVSS v3.1 Base Score 8.2 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N

A *CWE-601 URL Redirection to Untrusted Site* vulnerability exists that could cause an open-redirect vulnerability leading to a cross site scripting attack. By providing a URL-encoded input attackers can cause the software's web application to redirect to the chosen domain after a successful login is performed.

CVE ID: **CVE-2023-5987**

CVSS v3.1 Base Score 6.1 | Medium | CVSS:3.1 AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

A *CWE-79 Improper Neutralization of Input During Web Page Generation* (Cross-site Scripting) vulnerability that could cause a vulnerability leading to a cross site scripting condition where attackers can have a victim's browser run arbitrary JavaScript when they visit a page containing the injected payload.

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) *Version 2020 CU2 and prior*	Version 2020 CU3 of EcoStruxure™ Power Monitoring Expert (PME) includes a fix for these vulnerabilities and is available for download here: https://ecoxpert.se.com/software-center/power-monitoring-expert/power-monitoring-expert-2020
EcoStruxure™ Power Monitoring Expert (PME) *Version 2021 CU1 and prior*	Version 2021 CU2 of EcoStruxure™ Power Monitoring Expert (PME) includes a fix for these vulnerabilities and is available for download here: https://ecoxpert.se.com/software-center/power-monitoring-expert/power-monitoring-expert-2021

EcoStruxure™ Power Operation (EPO) - Advanced Reporting and Dashboards Module *2020* **EcoStruxure™ Power SCADA Operation (PSO) - Advanced Reporting and Dashboards Module** *2020*	Version 2020 CU3 of EcoStruxure™ Power Monitoring Expert (PME) includes a fix for these vulnerabilities and is available for download here: https://ecoxpert.se.com/software-center/power-monitoring-expert/power-monitoring-expert-2020 NOTE: Advanced Reporting and Dashboards Module is the commercial name for PME which is why, in this case, you are asked to download and install PME 2020 CU3.
EcoStruxure™ Power Operation (EPO) - Advanced Reporting and Dashboards Module *2021*	Version 2021 CU2 of EcoStruxure™ Power Monitoring Expert (PME) includes a fix for these vulnerabilities and is available for download here: https://ecoxpert.se.com/software-center/power-monitoring-expert/power-monitoring-expert-2021 NOTE: Advanced Reporting and Dashboards Module is the commercial name for PME which is why, in this case, you are asked to download and install PME 2021 CU2.

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

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:

- Follow the PME and EPO security guidelines on securing web communications by reviewing Cybersecurity Recommendations in the respective user manuals.

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.

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 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 *14 November 2023*	Original Release

Product Security Office Digitally signed by Product Security Office
Date: 2023.11.14 07:48:59 -05'00'