

# Schneider Electric Security Notification

## EcoStruxure™ Power Monitoring Expert

14 December 2021

### Overview

Schneider Electric is aware of multiple vulnerabilities in its EcoStruxure™ Power Monitoring Expert product.

[EcoStruxure Power Monitoring Expert](#) (PME) is on-premise software used to help power-critical and energy-intensive facilities maximize uptime and operational efficiency.

Failure to apply the mitigation provided below may risk arbitrary code execution, which could result in an attacker having the victim's browser carry out work on the attacker's behalf.

### Affected Product and Versions

EcoStruxure™ Power Monitoring Expert 9.0 and prior versions

### Vulnerability Details

CVE ID: **CVE-2021-22826**

CVSS v3.1 Base Score 6.7 | Medium | CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:H/A:H

A CWE-20: Improper Input Validation vulnerability exists that could cause arbitrary code execution when the user visits a page containing the injected payload. This CVE is unique from CVE-2021-22827.

CVE ID: **CVE-2021-22827**

CVSS v3.1 Base Score 6.7 | Medium | CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:H/A:H

A CWE-20: Improper Input Validation vulnerability exists that could cause arbitrary code execution when the user visits a page containing the injected payload. This CVE is unique from CVE-2021-22826.

### Remediation

A fix for these two vulnerabilities is included in EcoStruxure™ Power Monitoring Expert 2020 or later version, and available for download:

[https://www.se.com/ww/en/download/document/PME\\_10.0.iso/](https://www.se.com/ww/en/download/document/PME_10.0.iso/)

Contact your Schneider Electric representative for details on how to upgrade your system.

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.

# Schneider Electric Security Notification

## 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 vulnerabilities:

CVE	Researcher
CVE-2021-22826, CVE-2021-22827	Ed Stewart, Microsoft

## 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.

## Schneider Electric Security Notification

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

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability**. We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

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

Revision Control:

<p><b>Version 1.0</b> 14 December 2021</p>	<p>Original Release</p>
--	-------------------------