Schneider Electric Security Notification

EcoStruxure™ Power Monitoring Expert

11 January 2022

Overview

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

EcoStruxure Power Monitoring Expert is on-premise software used to help power-critical and energy-intensive facilities maximize uptime and operational efficiency.

Failure to apply the remediation provided below may risk loss of data confidentiality, data integrity issues, or a loss of access to the server.

Affected Product and Versions

Product	Version
EcoStruxure Power Monitoring Expert	Versions 2020 and prior

Vulnerability Details

CVE ID: **CVE-2022-22726**

CVSS v3.1 Base Score 5.0 | Medium | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N

A *CWE-20: Improper Input Validation* vulnerability exists that could allow arbitrary files on the server to be read by authenticated users through a limited operating system service account.

CVE ID: **CVE-2019-8963**

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

A *Denial of Service* vulnerability exists in FlexNet Publisher's lmadmin tool, when doing a crafted POST request on lmadmin using web-based tool. This tool is deployed with PME and an attacker leveraging this vulnerability may be able, with a sustained attack, to stop PME from operating.

CVE ID: **CVE-2022-22727**

CVSS v3.1 Base Score 7.1 | High | CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:H/A:H

A *CWE-20: Improper Input Validation* vulnerability exists that could allow an unauthenticated attacker to view data, change settings, impact availability of the software, or potentially impact a user's local machine when the user clicks a specially crafted link.

Schneider Electric Security Notification

CVE ID: **CVE-2022-22804**

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-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')* vulnerability exists that could allow an authenticated attacker to view data, change settings, or impact availability of the software when the user visits a page containing the injected payload.

Remediations

Affected Product & Version	Remediation
EcoStruxure Power Monitoring Expert 2020	Remediation Steps: 1. Install Version 2020 CU3 of EcoStruxure Power Monitoring Expert which includes a fix for **CVE-2022-22726, CVE-2022-22727,** and **CVE-2022-22804.** 2. Install Floating License Manager 2.7 after PME 2020 CU3 installation to address **CVE-2019-8963.** Both updates can be downloaded here: https://schneider-electric.app.box.com/folder/152201039971?s=dwbjm0bp3850ek95zyinv6g7nqjj86fm
EcoStruxure Power Monitoring Expert 9.0 or older	Contact your Schneider Electric representative for details on how to upgrade to PME 2021.

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.

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

CVE	Researcher
CVE-2022-22726, CVE-2022-22727, CVE-2022-22804	U.S. Department of Energy CyTRICS researcher Robert Erbes – INL

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

Schneider Electric Security Notification

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

Revision Control:

Version 1.0 *11 January 2022*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2022.01.09 14:20:51 -05'00'